



# Casper Suite Administrator's Guide

Version 8.6

JAMF Software, LLC  
© 2012 JAMF Software, LLC. All rights reserved.

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

JAMF Software  
301 4th Ave S Suite 1075  
Minneapolis, MN 55415-1039  
(612) 605-6625

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of JAMF Software, LLC.

Active Directory, Office, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

ADmitMac is a registered trademark of Thursby Software Systems, Inc.

Adobe and Adobe Creative Suite are trademarks of Adobe Systems Incorporated.

Apache Directory LDAP Studio and Tomcat are trademarks of the Apache Software Foundation.

Apple, the Apple logo, Apple Remote Desktop, Finder, FileVault, FireWire, iPhone, iTunes, Mac OS, MacBook, and Safari are trademarks of Apple Inc., registered in the United States and other countries. iPad is a trademark of Apple Inc. App Store is a service mark of Apple Inc., registered in the United States and other countries.

Casper Admin, Casper Imaging, Casper Remote, the Casper Suite logo, Composer, jamf, the JAMF Software logo, the JAMF Software Server, Recon, Recon.exe, and Self Service are trademarks of JAMF Software, LLC in the United States and other countries.

Centrify is a registered trademark of Centrify Corporation in the United States and/or other countries.

eDirectory is a trademark of Novell, Inc. in the United States and other countries.

iOS is a trademark or registered trademark of Cisco in the United States and other countries.

Likewise is a trademark of Likewise Software.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

Maker's Mark is a registered trademark of Beam Global Spirits & Wine, Inc.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

UNIX is a registered trademark of the Open Group.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

All other product and service names mentioned are the trademarks of their respective companies.



# Contents

## **7 Chapter 1: Administering the JSS**

### **8 Overview of Technologies**

8 Applications and Utilities

12 Ports

14 Security

17 Requirements

### **21 Installing and Managing the JSS**

21 Required Components

22 Installing the JSS on Mac OS X Server

25 Allocating Additional Memory to Tomcat

27 Setting Up the JSS

31 Upgrading the JSS

32 Changing the Activation Code

33 Backing Up the Database

36 Restoring Database Backups

37 Deleting Logs from the Database

39 Migrating to Another Server

40 Managing Distribution Points

44 Enabling Email Notifications

46 Enabling Change Management

48 Integrating with GSX

50 Generating a Web Server Certificate

51 Enabling Clustering

53 Configuring Tomcat to Work with a Load Balancer

54 Changing the Limited Access Setting

56 Frequently Asked Questions

58 Troubleshooting the JSS

## **61 Chapter 2: Client Management**

### **62 Building Packages**

62 Introduction to Composer

63 Creating Package Sources

71 Managing Package Manifests

74 Editing Package Sources

82 Building Packages from Package Sources

84 Building OS Packages

87 Managing Composer Preferences

<b>91</b>	<b>Building Your Client Management Framework</b>
91	Integrating with LDAP Servers
99	Managing JSS User Accounts
104	Adding Software Update Servers
106	Adding NetBoot Servers
110	Managing Buildings and Departments
112	Managing Network Segments
114	Managing Packages
134	Managing Scripts
141	Managing Printers
146	Managing Dock Items
147	Creating Directory Bindings
152	Creating Disk Encryption Configurations
155	Configuring the Computer Management Framework
167	Managing Removable MAC Addresses
169	Policies
<b>180</b>	<b>Inventory</b>
180	Managing Inventory Preferences
189	Managing Peripheral Types
191	Acquiring Mac OS X Computers
195	Enrolling Mac OS X Computers with the JSS
209	Acquiring Windows Computers
213	Acquiring Mobile Devices
214	Searching Computers
227	Searching Peripherals
232	Searching Software Inventory
237	Performing Mass Actions on Computer Search Results
242	Editing Computer Records
244	Deleting Computers from the JSS
245	Creating Computer Groups
248	Suppressing Software from Reports
249	Viewing Receipts
250	Managing Custom Reports
<b>253</b>	<b>Imaging</b>
253	Overview of the Imaging Process
255	Managing Configurations
264	Imaging Drives
266	Customizing the Imaging Process
273	Managing Autorun Preferences
274	Using the Autorun Feature
277	PreStage Imaging
281	Target Mode Imaging

<b>284</b>	<b>Patch Management</b>
284	Running Software Update
287	Installing Adobe CS3/CS4 Updaters
<b>290</b>	<b>Software Distribution</b>
290	Installing Packages
294	Caching Packages
298	Installing Cached Packages
303	Uninstalling Packages
307	Using the Self Healing Feature
<b>309</b>	<b>Remote Control</b>
309	Overview of Remote Control
310	Requirements
311	Using Screen Sharing
312	How Screen Sharing Works
<b>313</b>	<b>Settings and Security Management</b>
313	Managed Preferences
324	Managing Mac OS X Configuration Profiles
331	Running Remote Commands for Mac OS X Computers
334	Running Scripts
338	Managing Printers
341	Managing Dock Items
343	Managing Local Accounts
351	Binding to Directory Services
353	Deploying Disk Encryption Configurations
357	Managing Open Firmware/EFI Passwords
<b>360</b>	<b>License Management</b>
360	Creating Licensed Software Records
367	Reporting on Licensed Software
373	Sending Notifications on Licensed Software Violations
374	Reclaiming Unused Licensed Software
<b>375</b>	<b>Usage Management</b>
375	Application Usage
378	Computer Usage
380	Restricted Software
<b>384</b>	<b>Self Service</b>
384	Overview of Self Service
385	Managing User Authentication Preferences
386	Installing Self Service
387	Making Policies Available in Self Service
391	Managing Self Service Plug-ins
395	Installing Items from Self Service

## **398 Chapter 3: Mobile Device Management**

### **399 Building Your MDM Framework**

399 Configuring the Mobile Device Management Framework

### **408 Enrollment**

408 About Mobile Device Enrollment

409 Enrolling Mobile Devices OTA

413 The OTA Enrollment User Experience

419 Enrolling Connected Mobile Devices

423 Unenrolling Mobile Devices

### **424 Inventory**

424 Searching Mobile Devices

432 Searching Mobile Device Apps

437 Performing Mass Actions on Mobile Device Search Results

440 Editing Mobile Device Records

443 Deleting Mobile Devices from the JSS

444 Creating Mobile Device Groups

### **447 Configuration**

447 Creating and Distributing iOS Configuration Profiles

451 Distributing iOS Configuration Profiles Created with Apple's Tools

454 Updating iOS Configuration Profiles

455 Removing iOS Configuration Profiles

456 Deleting iOS Configuration Profiles

### **457 Security Management**

457 Running Remote Commands for Mobile Devices

459 Viewing the Status of Remote Commands for Mobile Devices

460 Canceling Remote Commands for Mobile Devices

### **461 Distribution**

461 Apps

475 eBooks



# Chapter 1: Administering the JSS

# Overview of Technologies

## Applications and Utilities

This section describes the applications and utilities that make up the Casper Suite.

### JSS Installers

JSS Installers provide a quick, easy way to install and upgrade the JAMF Software Server (JSS). JSS Installers are available for the following platforms:

- Mac
- Linux
- Windows

#### JSS Installer for Mac

The JSS Installer for Mac is an installation package that allows you to install and upgrade the JSS on Mac OS X Server. It also allows you to create your initial distribution point during a fresh installation.

**Note:** The JSS Installer for Mac included in the product DMG (JSS\_Installer.mpkg) is unsigned. To obtain a signed version of the JSS Installer for Mac (JSS\_Installer.pkg), contact JAMF Software Support. The signed version allows you to install or upgrade the JSS when Apple's Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

#### JSS Installers for Linux and Windows

The JSS Installers for Linux and Windows allow you to install and upgrade the JSS on supported Linux and Windows operating systems.

To obtain these installers and their documentation, see the introductory email that you received from JAMF Software or contact your JAMF Software Representative.

# Mac OS X Applications

## Casper Admin

The Casper Admin application is a repository for packages, scripts, printers, and Dock items. Casper Admin allows you to create and maintain configurations (similar to images) using these items and manually replicate distribution points.

The JSS also has an implementation of Casper Admin that is almost identical to the application with a few exceptions. The JSS implementation of Casper Admin does not allow you to perform the following actions:

- Copy packages to distribution points.
- Delete files from distribution points.
- Replicate distribution points or FireWire drives.
- Add new printers.
- Add and manage Dock items.
- Identify Adobe Installers and Adobe Updaters.
- Index packages.

Conversely, the following actions can only be performed using the JSS implementation of Casper Admin:

- Specify Self Healing data for packages.
- View the contents of an indexed package.
- Create directory bindings.

## Casper Imaging

The Casper Imaging application is used to image local drives. It provides two options for automating the imaging process: Autorun and PreStage imaging.

Casper Imaging can also be used to run scripts, map printers, create local user accounts, bind to Active Directory, and automate other common postfix tasks.

## Casper Remote

The Casper Remote application allows you to perform the following tasks on remote computers:

- Distribute software.
- Run Apple's Software Update.
- Run scripts.
- Map printers.
- Create local user accounts.
- Bind to Active Directory.
- Automate other management tasks.

Casper Remote allows you to perform the same management tasks as a policy, but the actions take place immediately over a Secure Shell (SSH) connection instead of waiting for clients to check in to the JSS.

## Composer

The Composer application is used to build packages from software, applications, preference files, documents, and other installable items. Building packages allows you to break down images into smaller, deployable components that facilitate a modular approach to the imaging process.

## JAMF Software Server

The JSS is a web application that serves as the administrative core of the Casper Suite. All other JAMF Software administrative applications communicate with the JSS.

The JSS allows you to perform remote management tasks on enrolled computers, such as deploying policies or restricting software. It also allows you to perform over-the-air management tasks on enrolled mobile devices, such as installing configuration profiles or distributing apps.

In addition, you can use the JSS to collect and view inventory for computers and mobile devices regardless of their enrollment status.

## Recon

The Recon application allows you to acquire Mac OS X computers to create your inventory and collect data, such as hardware, applications, fonts, and plug-ins.

## Self Service

The Self Service application allows users to run pre-configured management tasks (policies) on their computers. Using an interface similar to iTunes, users can point-and-click their way through management tasks, such as installing software, running Software Update, and mapping printers.

Plug-ins can also be added to Self Service for additional functionality. They can be a web page or an actual plug-in file that is written for Self Service. Plug-ins are stored in the following location on client computers:

```
/Library/Application Support/JAMF/Self Service/
```

## iOS Applications

### Self Service Web Clip

The Self Service web clip is added to enrolled devices by default. It allows you to distribute configuration profiles, apps, eBooks, and updated MDM profiles to devices for users to install. Users tap the web clip to browse and install items using an interface similar to the App Store.

You can configure settings for the Self Service web clip using the Mobile Device Management Framework settings in the JSS.



# Windows Applications

## Recon.exe

The Recon.exe application allows you to acquire Windows computers to create your inventory and collect data, such as hardware, applications, fonts, and plug-ins.

## Utilities

### JAMF Helper

The JAMF Helper displays messages to users. It is stored in the following location on client computers:

```
/Library/Application Support/JAMF/bin/
```

### JSS Database Utility

The JSS Database Utility allows you to back up and restore the jamfsoftware database. It also allows you to restart Apache Tomcat and MySQL and modify their settings.

### **/usr/sbin/jamf (jamf binary)**

Most tasks in the Casper Suite are executed using the “jamf” command-line application (also known as the jamf binary). Although you are free to use this application at will, the Casper Suite automatically installs, updates, and runs it.

# Ports

The following table describes the main ports used to host communication among client computers, distribution points, and the JAMF Software Server (JSS):

Port	Used for
22	The standard port for SSH (known as remote login in Mac OS X).
80	The standard port for HTTP. If you use HTTP to deploy packages or scripts, they are downloaded on this port.
443	The standard port for HTTPS. If you use HTTPS to deploy packages or scripts, they are downloaded on this port.
548	The standard port for Apple File Protocol (AFP). If you use an AFP share to deploy packages or scripts, clients mount the AFP share on this port.
3306	The default port for MySQL.
8443	The SSL port for the JSS. Default port used by applications and enrolled computers and mobile devices to connect to the JSS.

The following table describes other commonly used ports:

Port	Used for
25	The standard port for SMTP. The JSS connects to an SMTP server to send email notifications to administrators.
139	If you use an SMB share to deploy packages or scripts, clients mount the SMB share on this port.
389	The standard port for LDAP. Any LDAP connections—even those coming from other applications—go through the JSS. This means that only the JSS connects to your LDAP server.
445	If you have an SMB client, such as “DAVE”, installed on your client computers, they may mount the SMB share on this port.
514	The default port for Syslog servers.
2195	The port used to send messages from the JSS to Apple Push Notification service (APNs).
2196	The port used for feedback from APNs.
5223	The port used to send messages from APNs to the mobile devices and computers in your network.
8080	The HTTP port for the JSS on Linux and Windows platforms. Although it is available, applications do not connect to this port unless the defaults are overridden.
9006	The HTTP port for the JSS on the Mac platform. Although it is available, applications do not connect to this port unless the defaults are overridden.

On the Mac platform, the JSS runs on ports 8443 and 9006 by default. On Linux and Windows platforms, the JSS runs on 8443 and 8080 by default. If you decide to change these ports, you must change the port information in Tomcat's `server.xml` file and in the Preferences window for each Casper Suite application.

You cannot change the default ports for SSH or SMB with the Casper Suite.

# Security

This section explains the primary security measures in the Casper Suite:

- Passwords
- Communication protocols
- Public key infrastructure
- Signed applications

## Passwords

The Casper Suite allows you to store individual accounts for client computers and reset the passwords if necessary.

Passwords stored in the database are encrypted using a standard 128-bit RSA encryption with a 1024-bit key.

## Communication Protocols

The Casper Suite has security built into its design. Connections between the JAMF Software Server (JSS), the other applications in the Casper Suite, and mobile devices take place over Secure Sockets Layer (SSL). The Casper Remote application and the network scanner in the Recon application connect to clients over Secure Shell (SSH), or remote login.

### Secure Shell (SSH)

SSH is a network security protocol built into Mac OS X. For more information, go to:

<http://openssh.org/>

### Secure Sockets Layer (SSL)

SSL is a security protocol for Internet communication. For more information, go to:

<https://www.openssl.org/>

## Public Key Infrastructure

A public key infrastructure (PKI) is the design by which digital certificates are obtained, managed, stored, and distributed to ensure a secure exchange of data over a public network. For more information on PKI, go to:

[https://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](https://en.wikipedia.org/wiki/Public_key_infrastructure)

## Certificate Authority

A certificate authority (CA) is a trusted entity that signs and issues the certificates required for certificate-based authentication. It is the central component of the PKI.

The JSS has a built-in CA that is enabled by default, but you can integrate it with third-party CA if you prefer.

For more information on CAs, go to:

[https://en.wikipedia.org/wiki/Certificate\\_authority](https://en.wikipedia.org/wiki/Certificate_authority)

## Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol (SCEP) obtains certificates from the CA and distributes them to enrolled mobile devices, allowing over-the-air management tasks to take place.

The CA hosted by the JSS is SCEP-enabled by default. If you plan to use a third-party CA, it must be SCEP-enabled.

## Certificates

Certificates are electronic documents that validate the identity of a public key to ensure the encryption of data and establish trust.

### Web Server Certificate

This certificate validates the identity of the JSS and establishes trust between the JSS and clients. Choosing to install this certificate prevents possible man-in-the-middle attacks by allowing clients to validate the certificate when connecting to the JSS. Clock skew can also be reduced to prevent the replay of messages from the JSS to client computers.

If you are using the Casper Suite for mobile device management, you need a web server certificate to ensure that the devices are communicating with a valid JSS.

### CA Certificate

This certificate establishes trust between the CA and Mac OS X clients, and between the CA and enrolled mobile devices.

### Signing Certificate

This certificate is used to sign messages passed between the between the JSS and Mac OS X clients, and between the JSS and enrolled mobile devices.

### Apple Push Notification Service Certificate

This certificate authenticates the JSS to Apple Push Notification service (APNs).

### Device Certificate

This certificate validates the identity of Mac OS X clients and enrolled mobile devices each time they communicate with the JSS.

## Signed Applications

The following applications are signed by JAMF Software:

- Casper Admin
- Casper Imaging
- Casper Remote
- Composer
- JAMF Helper
- JSS Installer for Windows (JSS\_Installer.msi)
- Recon
- Recon.exe
- Self Service
- /usr/sbin/jamf (jamf binary)

A signed version of the JSS Installer for Mac (JSS\_Installer.pkg) is also available. You can obtain it by contacting JAMF Software Support.

# Requirements

This section lists the requirements for the following components and functions of the Casper Suite:

- JAMF Software Server
- JSS Installers
- JSS Database Utility
- Package building
- Inventory
- Imaging
- Remote management
- Self Service
- Mobile device management

## JAMF Software Server

You can host the JAMF Software Server (JSS) on any server that meets the following minimum requirements:

- Java 1.6
- MySQL 5.1 or later
- Apache Tomcat 6.0 or later

Tested operating systems include:

- OS X Server v10.6
- OS X Server v10.7
- OS X Server v10.8
- Ubuntu 10.04 LTS Server
- Ubuntu 12.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6
- Windows Server 2008

Although you can install the JSS on any server that meets the minimum requirements, the JSS Installers for Mac, Linux, and Windows have additional requirements. (See the “JSS Installers” section for detailed information.)

## JSS Installers

### JSS Installer for Mac

The JSS Installer for Mac requires a Mac computer with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- OS X Server v10.6 or later
- Java 1.6
- MySQL Enterprise Edition 5.5 or later (recommended) or MySQL Community Server 5.5 or later, available at:  
<https://www.mysql.com/downloads/>
- Ports 8443 and 9006 available

### JSS Installers for Linux and Windows

Requirements for the JSS Installers for Linux and Windows are available in the JAMF Software Server Installation Guides for Linux and Windows. To obtain the JSS Installer for Linux or Windows along with its installation guide, contact your JAMF Software Representative, or visit the following website and log in with a valid JAMF Nation account:

<https://jamfnation.jamfsoftware.com/myAssets.html>

## JSS Database Utility

The JSS Database Utility requires a server with MySQL Server 5.1 or later.

## Package Building

Composer can run on the following operating systems:

- OS X v10.5.x
- OS X v10.6.x
- OS X v10.7.x
- OS X v10.8.x

## Inventory

Recon can run locally on the following operating systems:

- OS X v10.5.x
- OS X v10.6.x



- OS X v10.7.x
- OS X v10.8.x
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Recon can remotely acquire computers with the following operating systems:

- OS X v10.5.x
- OS X v10.6.x
- OS X v10.7.x
- OS X v10.8.x

Older versions of Recon (available by contacting JAMF Software Support) can remotely acquire computers with the following operating systems:

- Mac OS v8.6
- Mac OS v9.x
- OS X v10.1.x
- OS X v10.2.x
- OS X v10.3.x
- OS X v10.4.x
- Windows NT4
- Windows ME

Recon can acquire synced mobile devices with iOS 4 or later.

## Imaging

Casper Imaging can image computers with OS X v10.5.x, OS X v10.6.x, OS X v10.7.x, or OS X v10.8.x that do not have PowerPC processors.

## Remote Management

Policies can be used to manage computers with the following operating systems:

- OS X v10.5.x
- OS X v10.6.x
- OS X v10.7.x
- OS X v10.8.x

Casper Remote can be used to manage computers with OS X v10.5.x, OS X v10.6.x, OS X v10.7.x, or OS X v10.8.x that do not have PowerPC processors.

## Self Service

Self Service can run on the following operating systems:

- OS X v10.5.x
- OS X v10.6.x
- OS X v10.7.x
- OS X v10.8.x

## Mobile Device Management

The Casper Suite can be used to enroll and manage mobile devices with iOS 4 or later.

# Installing and Managing the JSS

## Required Components

This section describes the components that run the JSS.

### Java

Java 1.6 is required to start the Tomcat web application server that runs the JSS.

### MySQL

The JSS stores information in a MySQL database. For more information about MySQL, go to:

<https://www.mysql.com/>

### Apache Tomcat

The JSS runs on Tomcat, a web application server similar to Microsoft's Internet Information Server (IIS). For more information about Tomcat, go to:

<https://tomcat.apache.org/>

# Installing the JSS on Mac OS X Server

Installing the JAMF Software Server (JSS) involves the following steps:

1. Install the required software (if you haven't already).
2. Create the jamfsoftware database.
3. Run the JSS Installer.

This section includes details for each step.

Before you begin, review the "Requirements" section and make sure that your server meets the JSS Installer requirements.

**Note:** The instructions in this guide are for the Mac platform only. To obtain the JSS Installer for Windows or Linux along with its installation guide, contact your JAMF Software Representative, or visit the following website and log in with a valid JAMF Nation account:

<https://jamfnation.jamfsoftware.com/myAssets.html>

For instructions on how to manually install the JSS on Linux and Windows, download the "Manually Installing the JAMF Software Server" technical paper from:

[http://jamfsoftware.com/libraries/pdf/white\\_papers/Manually\\_Installing\\_the\\_JAMF\\_Software\\_Server.pdf](http://jamfsoftware.com/libraries/pdf/white_papers/Manually_Installing_the_JAMF_Software_Server.pdf)

## Step 1: Install the Required Software

Java and MySQL must be installed on the server before you can create the jamfsoftware database and run the JSS Installer. For instructions on how to install and configure Java and MySQL, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=28>

## Step 2: Create the jamfsoftware Database

Create a MySQL database in which the JSS can store its data, and a MySQL user can access it. Name the database "jamfsoftware" and give the MySQL user the following credentials:

- Username: jamfsoftware
- Password: jamfsw03

**Note:** If you customize the database name, username, or password, you will be prompted to enter the custom settings when you run the JSS Installer.

### To create the jamfsoftware database:

1. Open Terminal and access the MySQL command line as "root" by typing:

```
mysql -u root -p
```

If MySQL is not in the path or it is installed in a custom location, access the MySQL command line by updating the path or by typing:

```
/path/to/mysql -u root -p
```

**Note:** On OS X v10.7 or later, the default path for MySQL is `/usr/local/mysql/bin/`.

2. When prompted, enter the password for the MySQL "root" user.  
If you did not create a root password, press the Return key.
3. Create a database named "jamfsoftware" by executing:

```
CREATE DATABASE jamfsoftware;
```

4. Grant permissions to a MySQL user named "jamfsoftware" so that it can access the new database:

```
GRANT ALL ON jamfsoftware.* TO 'jamfsoftware'@localhost IDENTIFIED BY  
'jamfsw03';
```

**Note:** If you choose to enter a username other than "jamfsoftware", it is recommended that you do not use "root".

## Step 3: Run the JSS Installer

Run the JSS Installer to install Apache Tomcat and the JSS web application, and create your initial distribution point.

### To run the JSS Installer:

1. Copy the JSS Installer for Mac to the server.

**Note:** The JSS Installer for Mac included in the product DMG (`JSS_Installer.mpkg`) is unsigned. To obtain a signed version of the JSS Installer for Mac (`JSS_Installer.pkg`), contact JAMF Software Support. The signed version allows you to install or upgrade the JSS when Apple's Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

2. Double-click the installer and click **Continue** to proceed.
3. When the Introduction pane appears, click **Continue**.
4. Read the information on the Read Me pane, and then click **Continue**.

5. Select a drive on which to install the software, and then click **Continue**.
6. Modify the information on the Database pane to reflect any custom settings if needed, and then click **Continue**.
7. Click **Install**.
8. Enter your administrator password when prompted, and then click **OK** or **Install Software**.
9. When the installation is complete, follow the instructions on the Summary pane to access the JSS. Then, click **Close**.

# Allocating Additional Memory to Tomcat

This section explains how to:

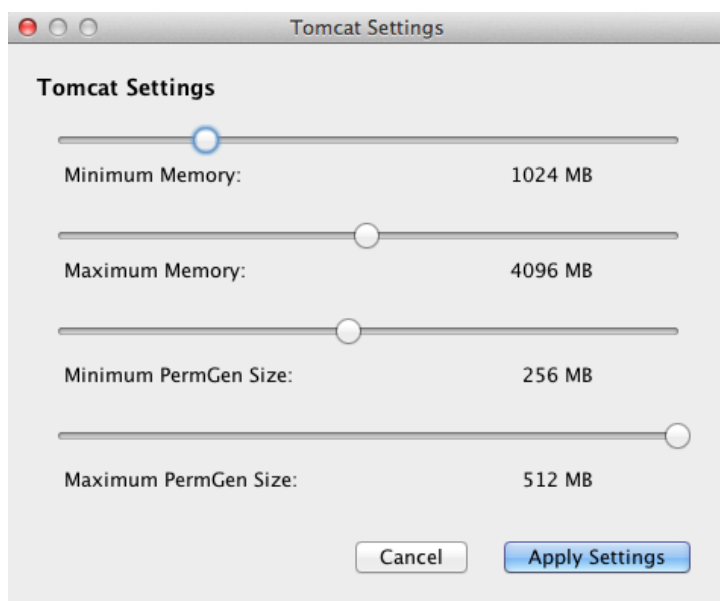
- View the amount of memory being used by the web application
- Allocate additional memory to Tomcat

**To view web application memory usage:**

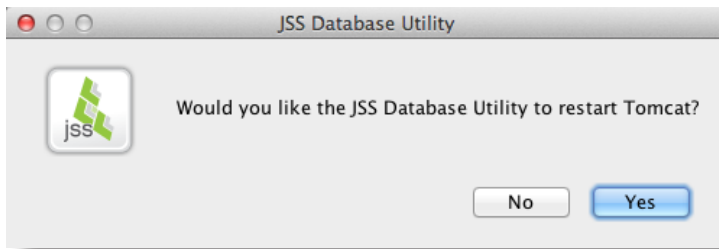
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Web App Memory** link.

**To allocate additional memory to Tomcat using the JSS Database Utility:**

1. Open the JSS Database Utility on the server running the JSS.  
The JSS Database Utility is located in:  
`/Library/JSS/bin/JSSDatabaseUtil.jar`
2. Enter the username and password for an administrator account to the server, and then click **OK**.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the location of the binary.
4. From the menu bar, choose **Utilities > Change Tomcat settings**.
5. Modify the minimum and maximum memory and PermGen sizes as needed.



6. Click **Apply Settings**.
7. When prompted to restart Tomcat, click **Yes**.





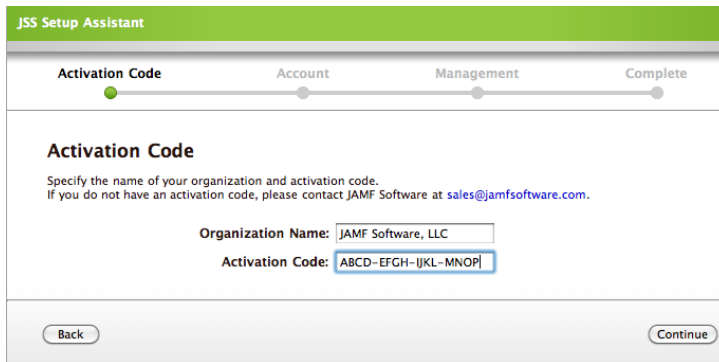
# Setting Up the JSS

The first time you connect to the JAMF Software Server (JSS), the JSS Setup Assistant guides you through creating your first account and configuring the basic computer management framework.

## To set up the JSS:

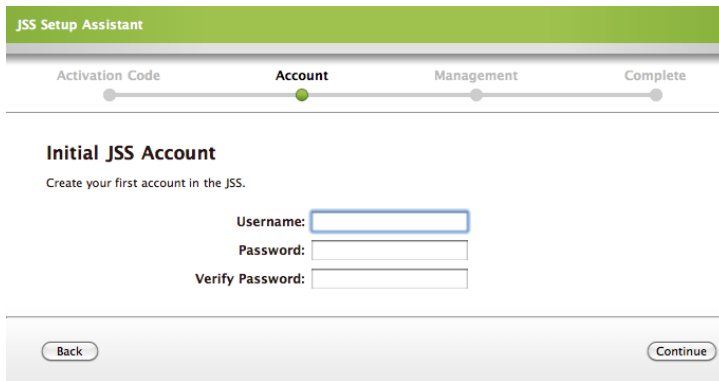
1. Log in to the JSS with a web browser.
2. Read the License Agreement and click **Agree**.
3. Enter the name of your organization and the activation code you received from your JAMF Software Representative, and then click **Continue**.

If you did not receive an activation code, send an email to [sales@jamfsoftware.com](mailto:sales@jamfsoftware.com).



The screenshot shows the 'JSS Setup Assistant' interface. At the top, a progress bar indicates four steps: 'Activation Code' (current), 'Account', 'Management', and 'Complete'. The 'Activation Code' step is highlighted with a green dot. Below the progress bar, the title 'Activation Code' is displayed. The instructions state: 'Specify the name of your organization and activation code. If you do not have an activation code, please contact JAMF Software at [sales@jamfsoftware.com](mailto:sales@jamfsoftware.com).' There are two input fields: 'Organization Name' with the value 'JAMF Software, LLC' and 'Activation Code' with the value 'ABCD-EFGH-IJKL-MNOP'. At the bottom, there are 'Back' and 'Continue' buttons.

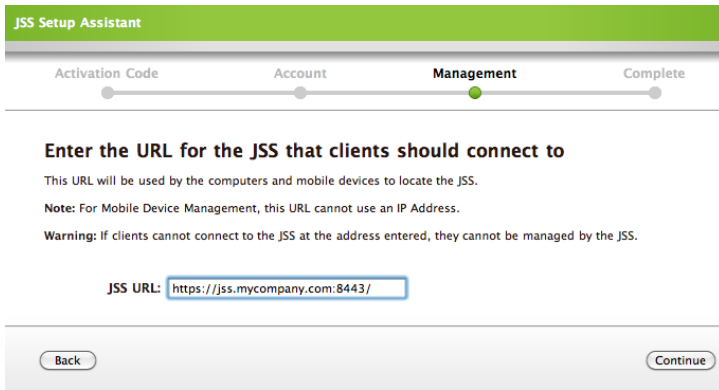
4. Enter a username and password to create your first administrator account in the JSS.



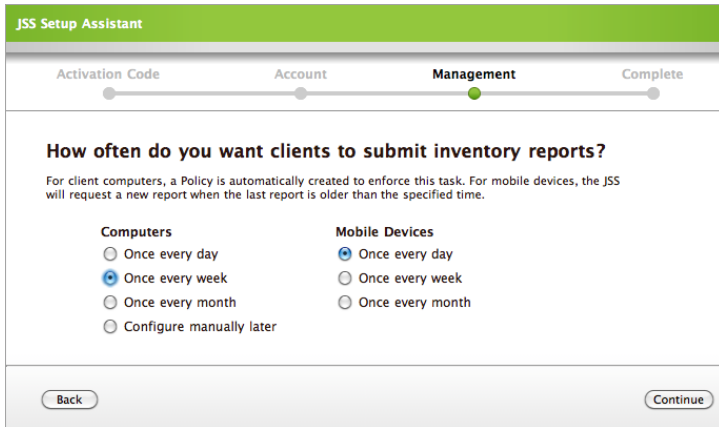
The screenshot shows the 'JSS Setup Assistant' interface. The progress bar now shows 'Account' as the current step, highlighted with a green dot. The title 'Initial JSS Account' is displayed. The instructions state: 'Create your first account in the JSS.' There are three input fields: 'Username', 'Password', and 'Verify Password'. At the bottom, there are 'Back' and 'Continue' buttons.

5. Enter the password again to verify it, and then click **Continue**.

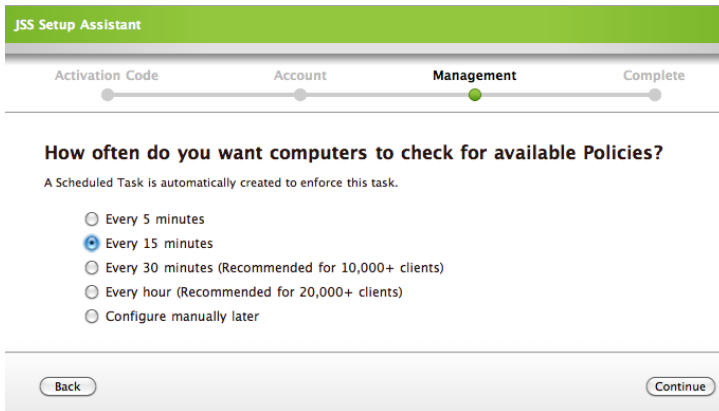
6. Verify the URL for your JSS, and then click **Continue**.  
The URL must include the correct protocol, domain, and port. For example:  
`https://jss.mycompany.corp:8443/`



7. Choose how often you want computers and mobile devices to submit inventory reports to the JSS, and then click **Continue**.  
For computers, this automatically creates a policy to enforce the inventory schedule. For more information on policies, see the "Policies" section.

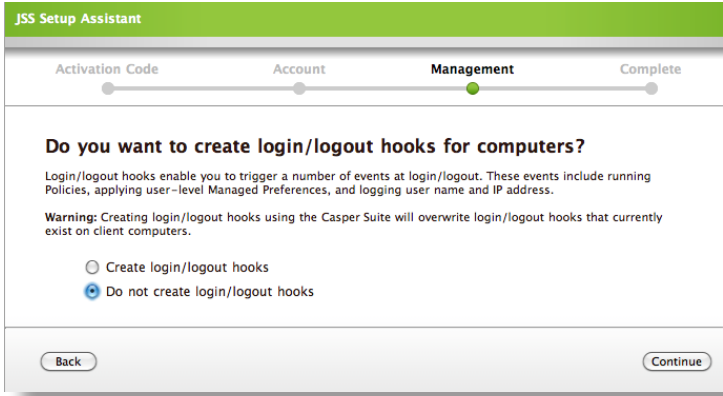


8. Choose how often you want computers to check in for policies, and then click **Continue**.



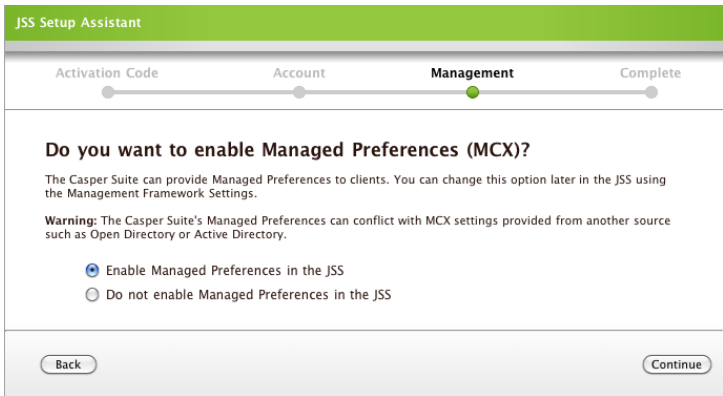
9. Choose whether or not to create login/logout hooks, and then click **Continue**.  
Login/logout hooks enable you to schedule management tasks to take place automatically when users log in or out of a computer. For more information on login/logout hooks, see the “Configuring the Computer Management Framework” section.

**Warning:** Creating login/logout hooks with the Casper Suite overwrites existing login/logout hooks.

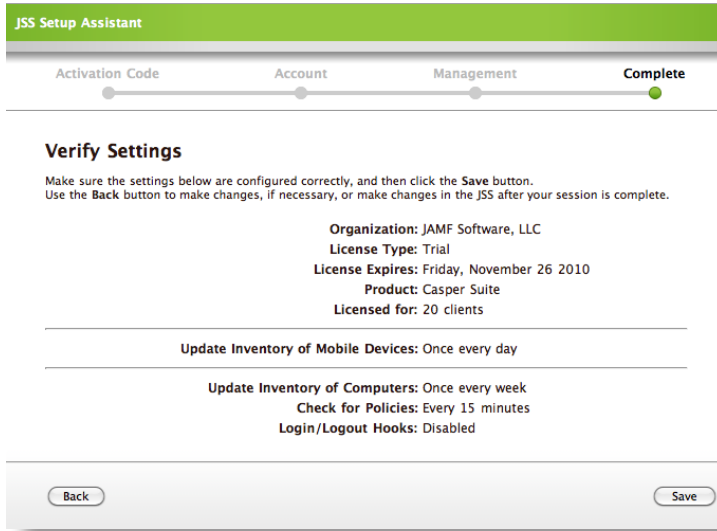


10. If you chose to create login/logout hooks in the previous step, choose whether or not to enable Managed Preferences and click the **Continue** button.  
Enabling Managed Preferences allows you to set locked preferences for groups of users across your network. You may be familiar with these preferences as MCX settings. For more information on Managed Preferences, see the “Managed Preferences” section.

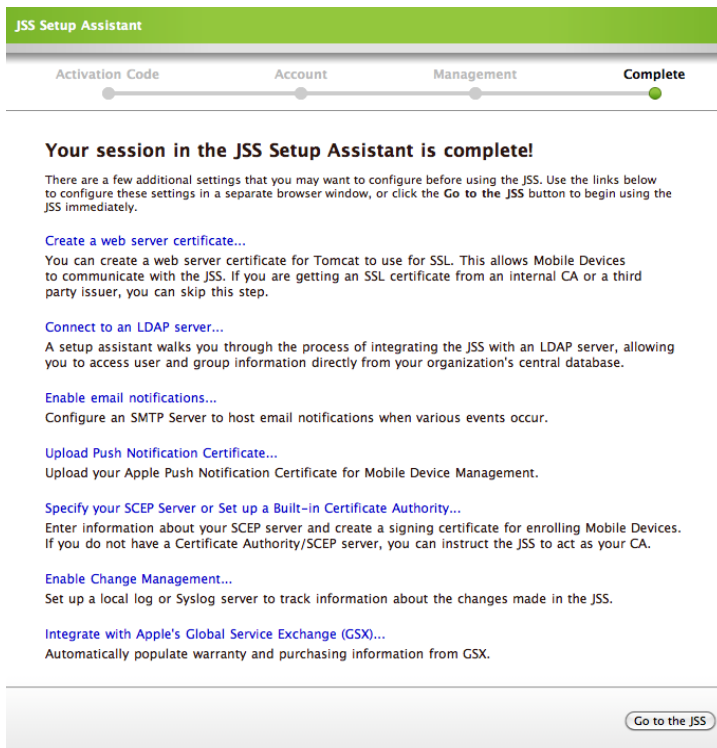
**Warning:** The Casper Suite’s Managed Preferences may conflict with MCX settings provided from another source, such as Open Directory or Active Directory.



11. Verify your settings, and then click the **Save** button.  
If you need to make changes, click the **Back** button or make changes in the JSS.



12. Click the **Go to the JSS** button to start using the JSS immediately, or use the links to configure additional settings for client and mobile device management in a separate browser window.



# Upgrading the JSS

This section explains how to upgrade the JAMF Software Server (JSS) on Mac OS X Server.

## To upgrade the JSS:

1. Back up the current database using the JSS Database Utility. (See “Backing Up the Database” for complete instructions.)

2. Back up custom reports.

If you used the JSS Installer to install the JSS on Mac OS X Server, custom reports are located in `/Library/JSS/Tomcat/webapps/ROOT/WEB-INF/reporting/`.

If you did not use the JSS Installer to install the JSS on Mac OS X Server, custom reports are located in `/Library/Tomcat/webapps/ROOT/WEB-INF/reporting/`.

3. Copy the most current version of the JSS Installer for Mac to the server.

**Note:** The JSS Installer for Mac included in the product DMG (`JSS_Installer.mpkg`) is unsigned. To obtain a signed version of the JSS Installer for Mac (`JSS_Installer.pkg`), contact JAMF Software Support. The signed version allows you to install or upgrade the JSS when Apple’s Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

4. Double-click the installer and click **Continue**.
5. When the Introduction pane appears, click **Continue**.
6. Read the information on the Read Me pane, and then click **Continue**.
7. Select a drive on which to install the software, and then click **Continue**.
8. If the Database pane appears, enter information about your MySQL database. Then, click **Continue**. The JSS Installer uses this information to connect to the existing database.

**Note:** This pane is only displayed if the `database.xml` file is in a custom location or contains invalid information.

9. Click **Install**.
10. Enter your administrator password when prompted, and then click **OK**.
11. When the upgrade is complete, follow the instructions on the Summary pane to access the JSS. Then, click **Close**.

# Changing the Activation Code

Every time you receive a new activation code, it must be updated in the JAMF Software Server (JSS).

When you update the activation code, you can also update your company name and view the following licensing information:

- **Product**—Product you are licensed for
- **Licenses**—Current number of licenses
- **License Renewal Date**—Date the maintenance contract expires
- **License Type**—Commercial, education, trial, etc.

**To change the activation code:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Enter the new activation code in the **Activation Code** field and click **Save**.

# Backing Up the Database

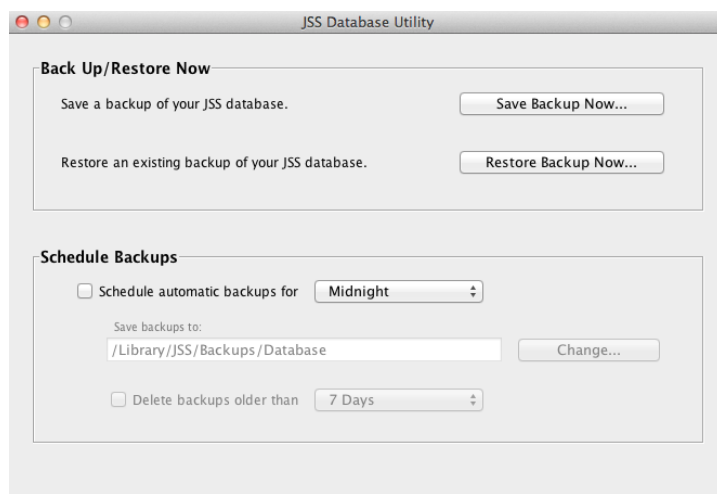
The JSS Database Utility allows you to create backups of the jamfsoftware database, schedule database backups, and stop scheduled database backups.

## Creating Database Backups

Use the JSS Database Utility to create a backup of the jamfsoftware database. The time it takes to create the backup depends on the size of the database.

### To create a database backup:

1. Open the JSS Database Utility, located in:  
`/Library/JSS/bin/JSSDatabaseUtil.jar`
2. Enter the username and password for an administrator account to the server, and then click **OK**.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the location of the binary.
4. If the Database Connection Setup pane appears, edit the settings to match your database configuration and click **Apply Settings**.
5. Click **Save Backup Now**.



6. Select the location where you want to save the backup, and then click **Choose**.

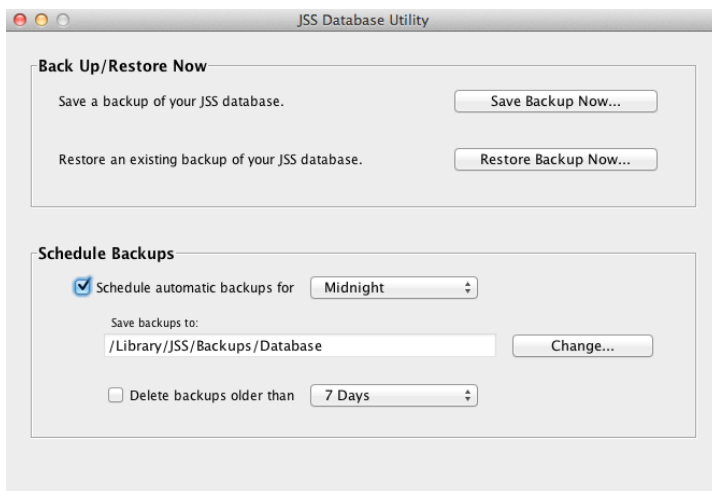
The JSS Database Utility creates the backup and saves it as a .sql.gz file.

## Scheduling Database Backups

Use the JSS Database Utility to schedule daily backups of the jamfsoftware database. You can also automate the deletion of scheduled backups that are older than a certain number of days.

**To schedule database backups:**

1. Open the JSS Database Utility, located in:  
`/Library/JSS/bin/JSSDatabaseUtil.jar`
2. Enter the username and password for an administrator account to the server, and then click **OK**.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to specify the path. Click **Continue** and specify the location of the binary.
4. If the Database Connection Setup pane appears, edit the settings to match your database configuration and click **Apply Settings**.
5. Select the **Schedule automatic backups for** checkbox and choose the hour of the day that you want backups to occur.
6. To change the location where backups are saved, click the **Change** button and select a new location.



7. To automate the deletion of scheduled backups, select the **Delete backups older than** checkbox. Then, choose the number of days after which backups should be deleted.

The JSS Database Utility saves daily backups at the hour that you specified. It also deletes scheduled backups older than the number of days that you specified.

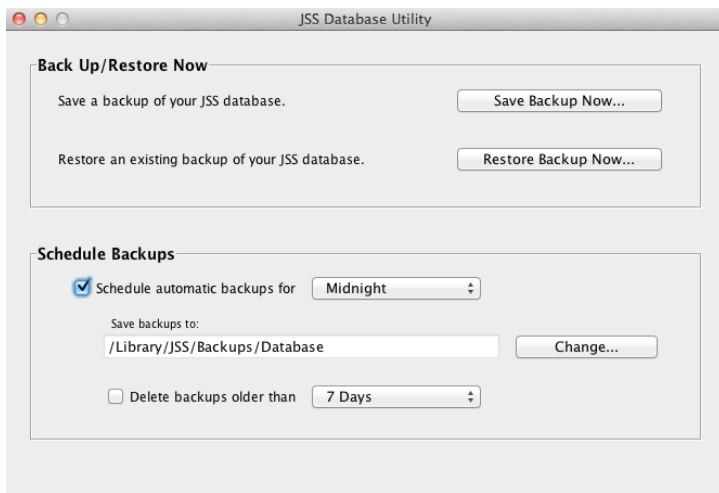
## Stopping Scheduled Database Backups

Use the JSS Database Utility to stop scheduled backups of the jamfsoftware database.



### To stop scheduled database backups:

1. Open the JSS Database Utility, located in:  
`/Library/JSS/bin/JSSDatabaseUtil.jar`
2. Enter the username and password for an administrator account to the server, and then click **OK**.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the location of the binary.
4. If the Database Connection Setup pane appears, edit the settings to match your database configuration and click **Apply Settings**.
5. Deselect the **Schedule automatic backups for** checkbox.



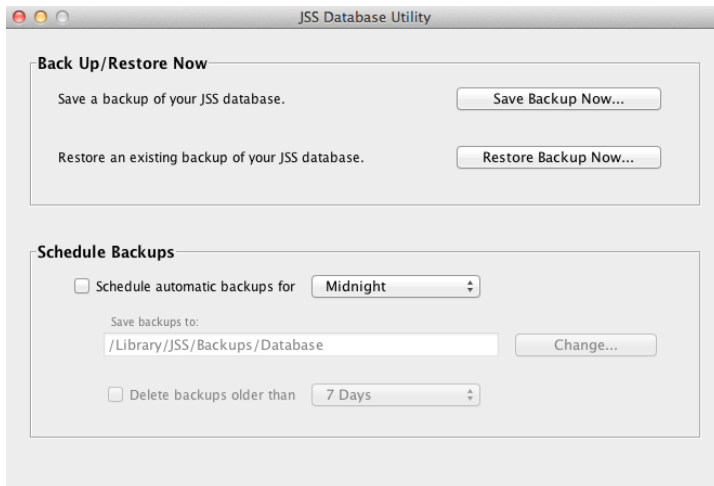
The JSS Database Utility stops scheduled backups immediately.

# Restoring Database Backups

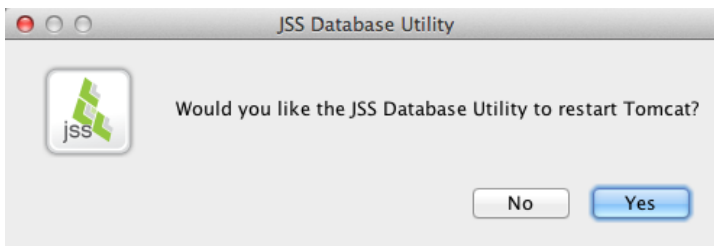
If you need to revert to an earlier version of your database, you can use the JSS Database Utility to restore a database backup.

## To restore a database backup:

1. Open the JSS Database Utility, located in:  
`/Library/JSS/bin/JSSDatabaseUtil.jar`
2. Enter the username and password for an administrator account to the server, and then click **OK**.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the location of the binary.
4. If the Database Connection Setup pane appears, edit the settings to match your database configuration and click **Apply Settings**.
5. Click **Restore Backup Now**.



6. Select the backup that you want to restore (.sql or .sql.gz), and then click **Choose**.
7. When prompted to restart Tomcat, click **Yes**.



The JSS Database Utility restarts Tomcat and replaces the current database with the one that you restored.

# Deleting Logs from the Database

Over time, the JAMF Software Server (JSS) accumulates a large number of logs. Deleting these logs can reduce the size of the database and can speed up searches.

You can schedule log deletion to take place automatically or manually delete logs as needed.

## To schedule automatic log deletion:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Flush Database Logs** link.
4. Use the pop-up menus to specify the period of time after which logs will be deleted.

For example, to delete Policy logs that are six months old or older, choose “Six Months” from the pop-up menu next to **Policy Logs**.

To stop deleting a type of log, choose “Do not delete” from the pop-up menu next to it.

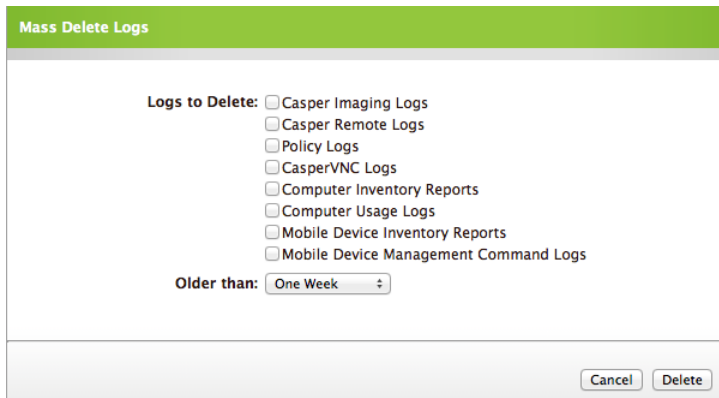
The screenshot shows a dialog box titled "Flush Database Logs" with a green header. Below the header, there is a sub-header "Flush Database Logs" and a paragraph of text: "Logs that are older than the times specified will be automatically deleted from the JSS at the time specified. The JSS will not delete the last inventory report for a computer or mobile device even if it is older than the time specified." Below this text, there are several log types, each with a dropdown menu: "Casper Imaging Logs: Do not delete", "Casper Remote Logs: Do not delete", "Policy Logs: Do not delete", "CasperVNC Logs: Do not delete", "Computer Inventory Reports: Do not delete", "Computer Usage Logs: Do not delete", "Mobile Device Inventory Reports: Do not delete", and "Mobile Device Management Command Logs: Do not delete". At the bottom, there is a "Time of Day:" label with a dropdown menu set to "Midnight". At the very bottom of the dialog, there are three buttons: "Flush Manually", "Cancel", and "Save".

5. Use the **Time of Day** pop-up menu to schedule a time for the deletion. For example, to delete logs every morning at 2 a.m., choose “2 AM” from the pop-up menu.
6. Click **Save**.
7. Click **Continue** to confirm the schedule.

## To delete logs manually:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Flush Database Logs** link.

4. Click the **Flush Manually** button.
5. Select the types of logs you want to delete.



6. Use the **Older than** pop-up menu to specify the period of time after which logs will be deleted. For example, to delete logs that are six months old or older, choose "Six Months" from the pop-up menu.
7. Click **Delete**.
8. Click **Continue** to confirm the results.

# Migrating to Another Server

The instructions in this section explain how to migrate the JAMF Software Server (JSS) to another server.

## To migrate the JSS:

1. Back up the existing jamfsoftware database using the JSS Database Utility. (See “Backing Up the Database” for detailed instructions.)
2. Ensure that the new server meets the requirements for the JSS Installer. Then, follow the instructions in “Installing the JSS” to install the required software (if needed) and create the jamfsoftware database.
3. Copy the JSS Installer to the new server.
4. Install the JSS by launching the installer and following the onscreen instructions. (See “Installing the JSS” for detailed instructions.)
5. Copy the database backup to the new server, and then use the JSS Database Utility to restore the backup. (See “Restoring a Database Backup” for detailed instructions.)
6. Regenerate the web server certificate. (See “Generating a Web Server Certificate” for detailed instructions.)
7. Update the DNS entry to point to the new server’s IP address.

**Note:** If you can’t change the DNS entry, you must change the JSS URL and re-enroll all mobile devices and computers.

# Managing Distribution Points

A key feature of the Casper Suite is the ability to deploy packages from multiple distribution points. This allows you to deploy packages to computers in other locations using servers that are geographically close to each destination. It reduces the need for bandwidth between locations and allows you to deploy packages across a widespread network.

Distribution points can share files over Apple Filing Protocol (AFP) or Server Message Block (SMB).

This section explains how to:

- Add distribution points
- Replicate distribution points
- Replicate FireWire or USB drives

## Adding Distribution Points

Servers running any platform can function as distribution points.

Adding a distribution point involves the following steps:

1. Set up the distribution point.
2. Add a record of the distribution point to the JAMF Software Server (JSS).

### Step 1: Set Up a New Distribution Point

1. Create a share point (AFP or SMB) on the server you want to utilize as the distribution point.
2. Create an account that has read-only access to the share.
3. Create an account that has read/write access to the share.
4. Make sure "Everyone" has read-only access to the share.
5. (Optional) Enable HTTP or HTTPS on the share point.

### Step 2: Add a Record of the Distribution Point to the JSS

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Add Server** button in the toolbar.
5. Select the **Distribution Point** option and click **Continue**.
6. Enter a display name for the server.

7. Enter the DNS name or IP address for the server.
8. To use this server as the default distribution point, select the **Use this server as the Master** option.
9. To assign a backup distribution point, choose a server from the **Failover Distribution Point** pop-up menu.
10. Click the **File Sharing** tab and enter information about the AFP or SMB share point.  
Casper Imaging uses the read-only account to mount the share.  
Casper Admin uses the read/write account.

Edit Distribution Point: NYC

General | File Sharing | HTTP

Connection Type:

Share Name:

Workgroup or Domain (SMB only):

Port:

---

Read-Only Username:

Read-Only Password:

Verify Read-Only Password:

---

Read/Write Username:

Read/Write Password:

Verify Read/Write Password:

11. (Optional) Configure the distribution point to use HTTP downloads.  
This requires HTTP or HTTPS access to be enabled on the distribution point server.
  - a. Click the **HTTP** tab.

Edit Distribution Point: NYC

General | File Sharing | HTTP

HTTP Downloads are enabled for this Distribution Point

---

Protocol:

Port:

Context:

---

No Authentication is Required

---

Username & Password Authentication is Required

Username:

Password:

Verify Password:

---

Certificate Authentication is Required

Certificate:  [Choose File...](#)

- b. Select the **HTTP Downloads are enabled for this Distribution Point** checkbox.
  - c. Choose “HTTP” or “HTTPS” from the **Protocol** pop-up menu.
  - d. Enter the port in the **Port** field.
  - e. In the **Context** field, enter the path to the share point (following the DNS name or port) that exists in the URL. For example, you would type “CasperShare” if the share is accessible at:  
`http://192.168.10.10/CasperShare/`
  - f. If the share requires a username and password to access files, select the **Username & Password Authentication is Required** option. Enter the username and password, and then enter the password again to verify it.
  - g. If the share requires a certificate, select **Certificate Authentication is Required** and click **Choose File** to upload the certificate.  
The certificate that you upload must be trusted.
12. Click the **Save** button.

## Replicating Distribution Points

You can replicate distribution points that are running on any platform.

To ensure distribution points have the same deployable items, synchronize them manually using the Casper Admin application.

### To replicate distribution points:

1. Open Casper Admin.
2. Select the distribution point(s) you want to replicate and click the **Replicate** button.

## Replicating FireWire or USB Drives

To make packages, scripts, printers, and configurations available for Casper Imaging offline, replicate to an external drive and place a copy of Casper Imaging at the root of the drive.

**Note:** Casper Imaging cannot create a management account when imaging offline.

Replicating a FireWire or USB drive involves the following steps:

1. Replicate to an external drive.
2. Use the replicated drive offline.

### Step 1: Replicate to an External Drive

1. Open Casper Admin.
2. Drag the hard drive icon from the Finder to the sidebar in Casper Admin.



3. If the external drive is already under the Local Drives heading in the sidebar, it is already replicated and is mounted automatically when you open Casper Admin.
4. Select the drive in the sidebar and click the **Replicate** button.

### **Step 2: Use the Replicated Drive Offline**

1. Make a copy of the Casper Imaging application.
2. Put the copy at the root of the replicated drive at the same level as the Packages, Scripts, and Casper Data folders.
3. Open Casper Imaging.

# Enabling Email Notifications

In order for the JAMF Software Server (JSS) to send email notifications, you must specify the SMTP server from which the notifications will be sent.

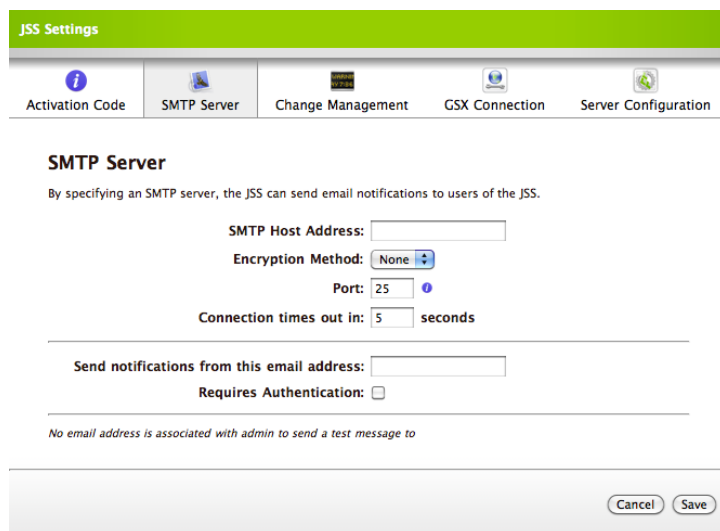
Email notifications can be sent when the following events occur:

- A computer is acquired using a PreStage.
- An error occurs during the imaging or Autorun process.
- An error occurs while a policy is being executed.
- A Self Healing event takes place.
- Restricted software is found.
- A licensing violation occurs.
- A smart computer group changes.
- There is a JSS service restart.
- A database is backed up successfully.
- A database backup fails.

This section explains how to set up and modify an SMTP server.

## To set up or modify an SMTP Server:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **SMTP Server** tab.
5. Enter the DNS name or IP address for the SMTP server in the **SMTP Host Address** field.



The screenshot shows the 'JSS Settings' interface with the 'SMTP Server' tab selected. The page title is 'JSS Settings'. The navigation bar includes 'Activation Code', 'SMTP Server', 'Change Management', 'GSX Connection', and 'Server Configuration'. The main content area is titled 'SMTP Server' and contains the following fields and options:

- SMTP Host Address:** A text input field.
- Encryption Method:** A dropdown menu with 'None' selected.
- Port:** A text input field with '25' entered.
- Connection times out in:** A text input field with '5' entered, followed by the word 'seconds'.
- Send notifications from this email address:** A text input field.
- Requires Authentication:** A checkbox that is currently unchecked.

At the bottom of the form, there is a note: 'No email address is associated with admin to send a test message to'. At the very bottom, there are 'Cancel' and 'Save' buttons.

6. Use the **Encryption Method** pop-up menu to specify the protocol used for data encryption.
7. In the **Port** field, enter the port over which the connection is made.  
The default port is 25.
8. Enter the number of seconds you want to wait before the connection times out.  
By default, this is 5 seconds.
9. Enter the email address from which notifications will be sent.
10. If the SMTP server requires authentication, select the **Requires Authentication** checkbox and enter credentials for a valid account to the server.

The screenshot shows the 'JSS Settings' dialog box with the 'SMTP Server' tab selected. The dialog has a green header bar with the title 'JSS Settings' and a navigation bar with icons for 'Activation Code', 'SMTP Server', 'Change Management', 'GSX Connection', and 'Server Configuration'. The 'SMTP Server' section is titled 'SMTP Server' and includes a sub-header: 'By specifying an SMTP server, the JSS can send email notifications to users of the JSS.' The form contains the following fields and controls:

- SMTP Host Address:** A text input field.
- Encryption Method:** A dropdown menu currently set to 'None'.
- Port:** A text input field with the value '25' and a small blue circle icon to its right.
- Connection times out in:** A text input field with the value '5' followed by the text 'seconds'.
- Send notifications from this email address:** A text input field.
- Requires Authentication:** A checked checkbox.
- Username:** A text input field.
- Password:** A text input field.
- Verify Password:** A text input field.

At the bottom of the dialog, there is a note: 'No email address is associated with admin to send a test message to'. At the very bottom right, there are 'Cancel' and 'Save' buttons.

11. If you want to send a test message, click the **Send Test message to <email address>** link.  
The JSS sends this message to the email address for the account currently logged in to the JSS.
12. Click **Save**.

# Enabling Change Management

Change management logs allow you to track the following information:

- Changes made to the client computers on your network
- Computers from which the changes were made
- Accounts that initiated the changes

You can choose to write these logs to a local log on the server running the JAMF Software Server (JSS) or a Syslog server.

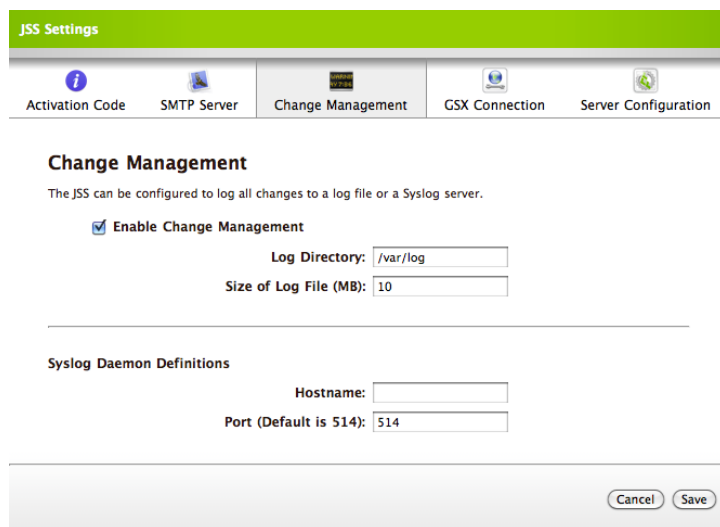
The header for each logged event includes the following information:

- Timestamp (when the event took place)
- Username of the account that initiated the change
- IP address of the client computer that triggered the event
- JSS identifier (com.jamfsoftware.jss)

This section explains how to set up and modify change management to a log file and a Syslog server.

## To set up or modify change management to a log file:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **Change Management** tab.
5. Select the **Enable Change Management** checkbox if it is not already selected, and enter a directory location for the log file.



The screenshot shows the 'JSS Settings' web interface. At the top, there is a green header with the title 'JSS Settings'. Below the header is a navigation bar with five tabs: 'Activation Code', 'SMTP Server', 'Change Management', 'GSX Connection', and 'Server Configuration'. The 'Change Management' tab is currently selected. The main content area is titled 'Change Management' and contains the following information:

The JSS can be configured to log all changes to a log file or a Syslog server.

**Enable Change Management**

Log Directory:

Size of Log File (MB):

---

Syslog Daemon Definitions

Hostname:

Port (Default is 514):

At the bottom right of the form, there are two buttons: 'Cancel' and 'Save'.

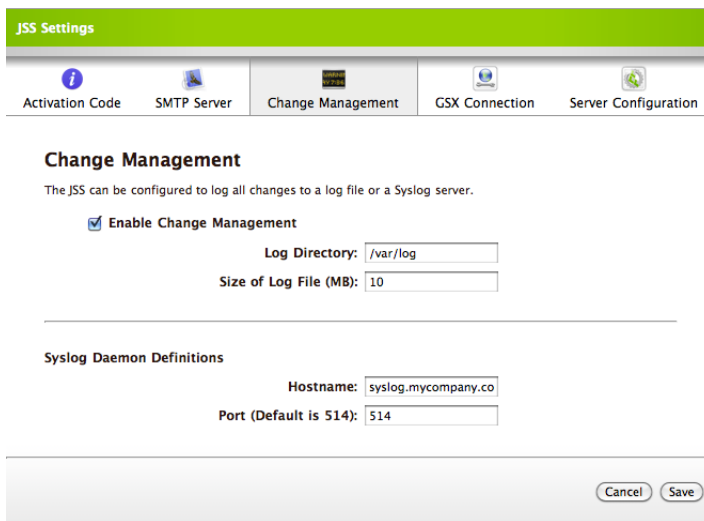
6. Click **Save**.

Change Management logs are written to the file specified in the **Log Directory** field. They have the filename `jamfChangeManagement.log` and can be viewed using the Console application.

**To set up or modify change management to a Syslog server:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **Change Management** tab.
5. Select the **Enable Change Management** checkbox.
6. In the **Hostname** field, enter the DNS name or IP address for the Syslog server.
7. Enter the UDP port that the Syslog server is using.

The port is entered as 514 by default.



The screenshot shows the 'JSS Settings' window with the 'Change Management' tab selected. The 'Enable Change Management' checkbox is checked. The 'Log Directory' field contains '/var/log' and the 'Size of Log File (MB)' field contains '10'. Under 'Syslog Daemon Definitions', the 'Hostname' field contains 'syslog.mycompany.co' and the 'Port (Default is 514)' field contains '514'. 'Cancel' and 'Save' buttons are at the bottom right.

8. Click **Save**.

# Integrating with GSX

The JAMF Software Server (JSS) can access the following purchasing information from Apple's Global Service Exchange (GSX) for computers in the JSS:

- Purchase date
- Warranty expiration date
- Apple Care ID (Warranty reference number)

To set up a GSX connection, you must have a GSX account and be signed up for Apple's Self-Servicing Account (SSA) Program. Information on this program is currently available at:

<https://www.apple.com/support/programs/ssa/>

For information on setting up a GSX account for integration with the JSS, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=26>

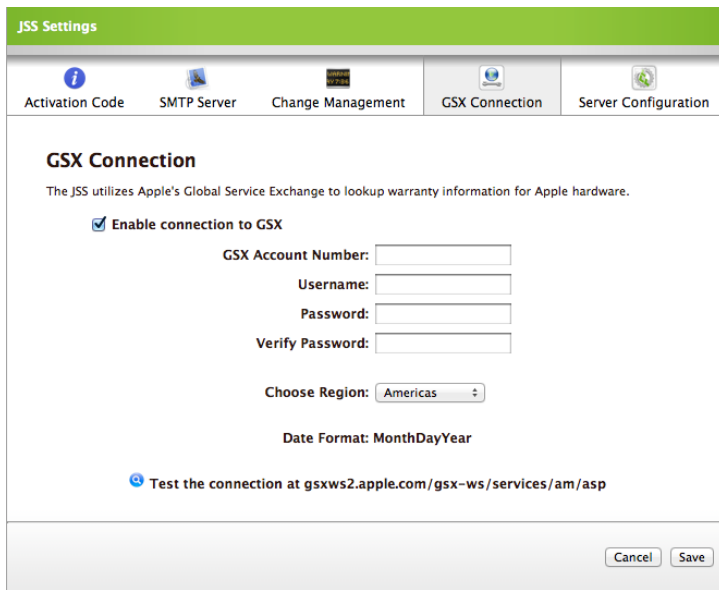
**Note:** GSX may not always return complete purchasing information for a computer. The JSS displays any information that is returned.

This section explains how to set up and modify the GSX connection.


## To set up or modify the GSX connection:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **GSX Connection** tab.
5. Select the **Enable connection to GSX** checkbox.

6. Enter your GSX account number in the **GSX Account Number** field.



The screenshot shows the 'JSS Settings' window with the 'GSX Connection' tab selected. The window has a green header bar with the title 'JSS Settings'. Below the header is a navigation bar with five tabs: 'Activation Code', 'SMTP Server', 'Change Management', 'GSX Connection', and 'Server Configuration'. The 'GSX Connection' tab is active. The main content area is titled 'GSX Connection' and contains the following text: 'The JSS utilizes Apple's Global Service Exchange to lookup warranty information for Apple hardware.' Below this is a checked checkbox labeled 'Enable connection to GSX'. There are four text input fields: 'GSX Account Number:', 'Username:', 'Password:', and 'Verify Password:'. Below these is a 'Choose Region:' dropdown menu currently set to 'Americas'. At the bottom of the form area, it says 'Date Format: MonthDayYear'. A blue search icon is followed by the text 'Test the connection at gsxws2.apple.com/gsx-ws/services/am/asp'. At the bottom right of the window are 'Cancel' and 'Save' buttons.

7. Enter the username and password for your GSX account, and then enter the password again to verify it.
8. Choose your region from the **Choose Region** pop-up menu.  
The date format automatically updates to reflect the region you choose.
9. To test the GSX connection, click the **Search**  icon.  
The JSS attempts to connect to GSX with the account number and credentials that you provided. A message displays confirming the success or failure of the connection.
10. Click **Save**.

# Generating a Web Server Certificate

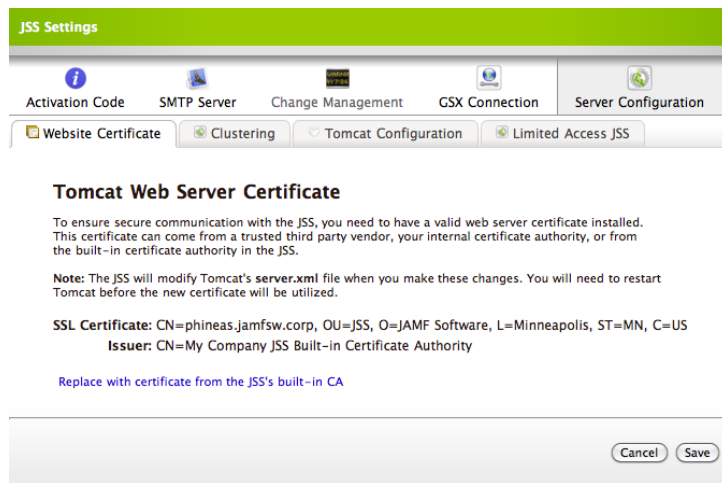
The JAMF Software Server (JSS) requires a valid web server certificate to ensure that computers and mobile devices communicate with the JSS and not an imposter server.

If you already have a web server certificate from an internal certificate authority (CA) or a trusted third-party vendor, follow the vendor's instructions for using the certificate with Tomcat.

If you do not have a valid web server certificate, you can generate one from the CA that is built into the JSS. To do this, the JSS must be installed as the "ROOT" web application and the user running the Tomcat process must have read/write access to Tomcat's `server.xml` file.

## To generate a web server certificate from the built-in CA:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **Server Configuration** tab.
5. Click the **Replace with certificate from the JSS's built-in CA** link.



6. Click **Save**.
  7. Restart Tomcat to begin utilizing the certificate.
- For instructions on how to restart Tomcat, see the Knowledge Base article at: <https://jamfnation.jamfsoftware.com/article.html?id=117>



# Enabling Clustering

Clustering allows you to point multiple instances of the JAMF Software Server (JSS) web application to the same database. This requires a load balancer with the address of the JSS. For example:

`https://jss.mycompany.com:8443/`

The load balancer should route traffic to the servers running the web application.

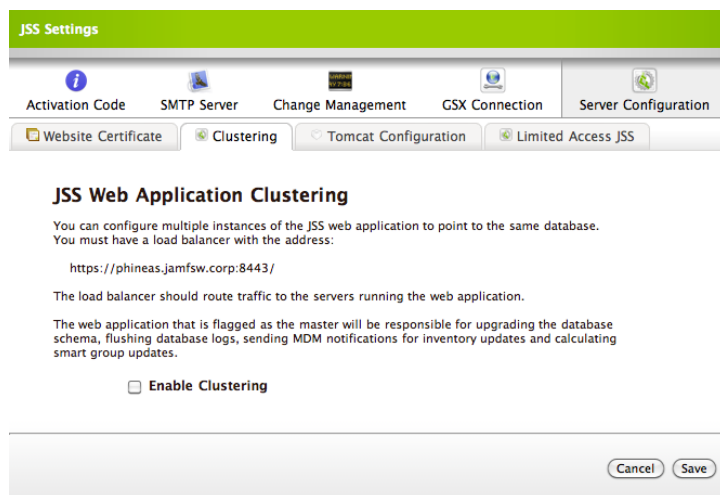
The web application that functions as the master handles the following tasks:

- Upgrading the database schema
- Flushing database logs

For more information on setting up a clustered environment, contact your JAMF Software Representative.

## To enable clustering:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Generals Settings** link.
4. Click the **Server Configuration** tab.
5. Click the **Clustering** tab.
6. Select the **Enable Clustering** checkbox.



7. To add web applications to the cluster, click the **Add To Cluster** links.
8. To make a web application the master, click the **Master** link.
9. Click **Save**.

10. Restart Tomcat for the changes to take effect.

For instructions on how to restart Tomcat, see the Knowledge Base article at:

<https://jamfnation.jamfsoftware.com/article.html?id=117>

# Configuring Tomcat to Work with a Load Balancer

When working with a load balancer, you may need to enable a few attributes in Tomcat's `server.xml` file to ensure that Tomcat and the load balancer communicate properly.

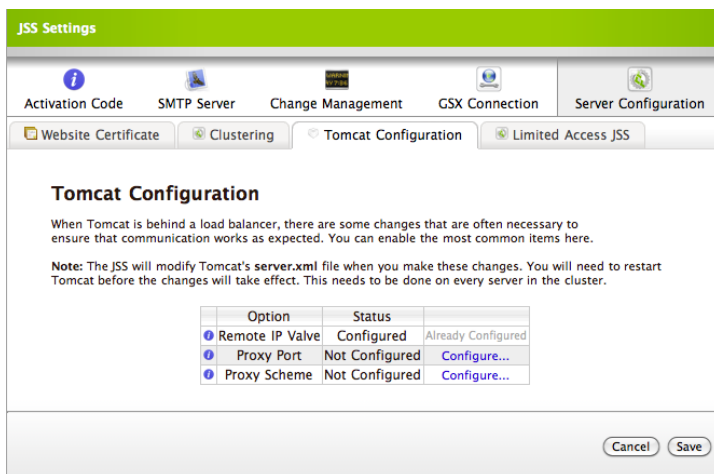
The JAMF Software Server (JSS) allows you to enable the following attributes without requiring you to access the `server.xml` file manually:

- Remote IP valve
- Proxy port
- Proxy scheme

To enable these attributes, the JSS must be installed as the "ROOT" web application and the user running the Tomcat process must have read/write access to Tomcat's `server.xml` file.

**To configure Tomcat to work with a load balancer:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **Server Configuration** tab.
5. Click the **Tomcat Configuration** tab.
6. Click the **Configure** link across from an attribute to enable it.



7. Click **Save**.
  8. Restart Tomcat for the changes to take effect.
- For instructions on how to restart Tomcat, see the Knowledge Base article at: <https://jamfnation.jamfsoftware.com/article.html?id=117>

# Changing the Limited Access Setting

When working in a clustered environment, you may have a JAMF Software Server (JSS) that computers and mobile devices can access from outside of the network. If you have a second JSS web application that resides in your DMZ, you can make the administrative interface unavailable by changing the Limited Access setting. Changing this setting also limits the types of devices that can check in and enroll with the JSS.

The Limited Access setting has four options:

- **Full JSS**—This is the default option for every JSS. It allows computers and mobile devices to check in and enroll with the JSS and use Self Service. It also makes the JSS interface available from anywhere.
- **Computer and Mobile Device Management**—This option allows computers and mobile devices to check in and enroll with the JSS and use Self Service. It also disables the JSS interface.
- **Computer Management Only**—This option allows computers to check in with the JSS and use Self Service. It also disables the JSS interface.
- **Mobile Device Management Only**—This option allows mobile devices to check in and enroll with the JSS and use Self Service. It also disables the JSS interface.

**Warning:** Do not change the Limited Access setting while connecting through a load balancer. Connect directly to the instance of Tomcat that is inside of your DMZ.

After you change the Limited Access setting, the JSS interface is inaccessible. To make additional changes, you need to manually modify the `web.xml` file. If you need to revert the JSS to the default setting (Full JSS), delete the `web.xml` file in `/Library/JSS/Tomcat/webapps/ROOT/WEB-INF/` and rename the `web.xml.original` file to `web.xml`.

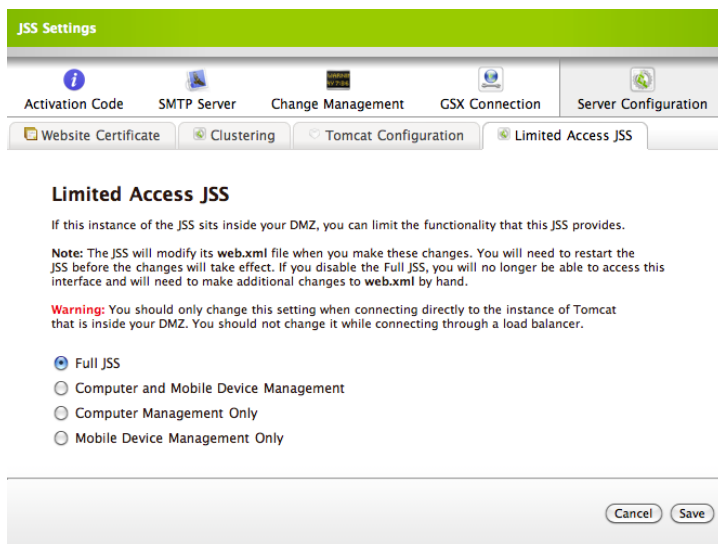
**Note:** If you upgraded from v8.1 or earlier, the `web.xml` and `web.xml.original` files are located in `/Library/Tomcat/webapps/ROOT/WEB-INF/`.

Upgrading the JSS automatically resets the Limited Access setting to Full JSS. You will need to change this setting every time you upgrade.

## To change the Limited Access setting:

1. Use a web browser to log in to the desired instance of the JSS.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **Server Configuration** tab.
5. Click the **Limited Access JSS** tab.

6. Select a limited access option.



7. Click **Save**.
8. Restart the JSS for any changes to take effect.

# Frequently Asked Questions

## Q. What is installed on Mac OS X Server when I install the JSS?

A. The following files and folders are installed on Mac OS X Server:

### **Apache Tomcat**

Tomcat is the web application server that runs the JSS web application. A directory named Tomcat is installed in:

```
/Library/JSS/Tomcat/
```

### **CasperShare**

The distribution point created by default for a fresh installation. The JSS Installer creates a directory named CasperShare in:

```
/Shared Items/CasperShare/
```

### **com.jamfsoftware.tomcat.plist**

This is the launchd item that controls Tomcat. It is installed and loaded in the following location:

```
/Library/LaunchDaemons/com.jamfsoftware.tomcat.plist
```

### **Database backup location**

The JSS Database Utility stores database backups in the following location by default:

```
/Library/JSS/Backups/Database/
```

### **JSS Database Utility**

The JSS Database Utility is installed in the following location:

```
/Library/JSS/bin/JSSDatabaseUtil.jar
```

### **JSS web application**

The JSS is a web application that runs on Tomcat. A directory named ROOT is installed in:

```
/Library/JSS/Tomcat/webapps/ROOT/
```

### **keystore**

Tomcat requires a .keystore file to provide connections over SSL. The JSS Installer creates a default .keystore file and stores it in the following location:

```
/Library/JSS/Tomcat/.keystore
```

### **Logs**

Logs for the installation and for the JSS are stored in the following directory:

```
/Library/JSS/Logs/
```

### server.xml

The JSS Installer installs a modified copy of Tomcat's `server.xml` file. This file enables SSL, ensures that the JSS appears in the root context, and enables database connection pooling. It is installed in the following location:

```
/Library/JSS/Tomcat/conf/server.xml
```

**Note:** The locations of these files and folders are different if you upgraded from v8.1 or earlier and your JSS is installed on OS X Server v10.6. Apache Tomcat and its related files are stored in `/Library/Tomcat/` and the JSS web application (previously known as the jamf web application) is stored in `/Library/Tomcat/webapps/ROOT/`.

## Q. Can I install the JSS on other platforms?

**A. Yes. You can install the JSS on any platform that supports the following software:**

- Java 1.6
- MySQL 5.1 or later
- Apache Tomcat 6.0 or later

Tested operating systems include:

- OS X Server v10.7
- OS X Server v10.6
- Ubuntu 10.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6
- Windows Server 2008

Although you can install the JSS on any server that meets the minimum requirements, JSS Installers are only available for Mac, Linux, and Windows.

To obtain the JSS Installers for Linux and Windows and their documentation, see the introductory email that you received from JAMF Software or contact your JAMF Software Representative.

# Troubleshooting the JSS

Most issues with the JSS have to do with the configuration of Apache Tomcat or MySQL. The JSS Database Utility allows you to troubleshoot most of the issues that you encounter.

This section explains how to troubleshoot the following issues:

- Connection issues
- Memory issues
- Database issues

## Connection Issues

If applications are not connecting to the JAMF Software Server (JSS), you can use a web browser to troubleshoot the issue. If you are able to connect to the JSS, the applications should be able to connect as well.

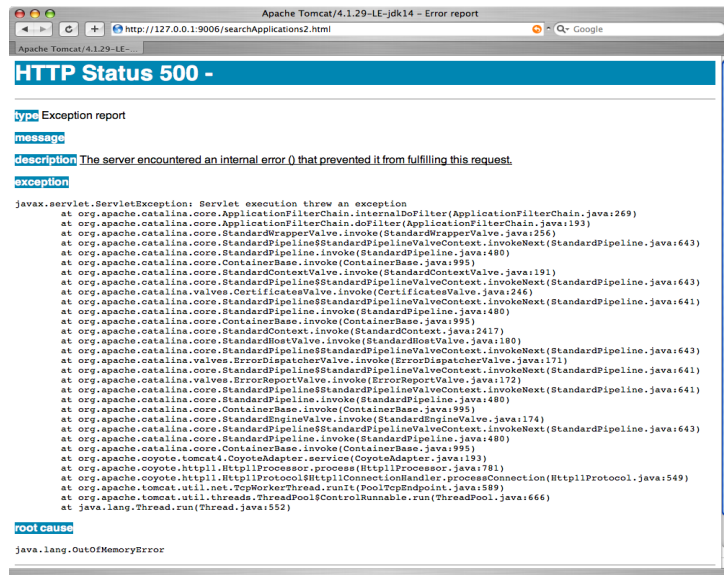
**To troubleshoot connection issues:**

1. Open a web browser and try connecting to the JSS on port 8443.  
For example, if the DNS name of the JSS is "jss.mycompany.com", try connecting to:  
<https://jss.mycompany.com:8443/>
2. If you are prompted to verify a certificate, accept the certificate.
3. If you are able to connect to the JSS, make sure that the application is pointing at the correct IP address.
  - a. Quit the application.
  - b. Hold down the Option key and re-open the application to bring up the Preferences pane.
  - c. On the Preferences pane, enter the DNS name or IP address for the JSS and then click **Save**.
  - d. Enter the username and password for an administrator account to the server, and then click **OK**.
4. If the application still fails to connect, restart Tomcat.  
For instructions on how to restart Tomcat, see the Knowledge Base article at:  
<https://jamfnation.jamfsoftware.com/article.html?id=117>



# Memory Issues

If there is a large amount of data in the JSS, you may need to allocate additional memory to Tomcat. Tomcat displays the following error page if more memory is required:



For instructions on viewing the amount of memory being used by the web application and allocating additional memory to Tomcat, see “Allocating Additional Memory to Tomcat”.

# Database Issues

MySQL database tables can become corrupt if the JSS is running on a very slow computer to which many clients are connected, or if the server running the JSS crashed and the database was not shut down properly.

When errors occur in the MySQL database, the JSS displays an alert similar to the following:

Got error 127 from table handler

This section explains how to:

- View the status of database tables
- Repair database tables
- Optimize database tables

## Viewing the Status of Database Tables

To view the status of database tables:

1. Log in to the JSS with a web browser.

2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Database Table Status** link.

## Repairing Database Tables

If you have a large database, it may take longer to verify the status of your database tables. Once the status of each table is returned, you may want to repair the tables that do not return an “OK” status.

**To repair database tables:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Repair Database Tables** link.

## Optimizing Database Tables

Optimizing database tables allows you to ensure that each table’s index is up to date so that you can perform database lookups as quickly as possible.

**To optimize database tables:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Optimize Database Tables** link.



## Chapter 2: Client Management

---

# Building Packages

## Introduction to Composer

A package is a self-contained group of files that can be deployed to remote computers or as part of the imaging process. A package consists of product or component files, such as an application and its required components, a set of fonts, a preference file, or a document. A package also contains instructions about how and where it should be installed once received by the user.

Depending on the files you want to package, Composer allows you to monitor the installation of your software or use files that already exist on your hard drive to create a package source.

You can create a package source using the following methods:

- Take before and after snapshots of your hard drive.
- Monitor the file system.
- Use pre-installed software.
- Use user environment settings.
- Drag contents from the Finder into Composer.
- Use an existing package.

After you verify the contents of a package source, Composer gives you the option to build a PKG or a DMG based on how you intend to use and deploy the package.

Composer also allows you to build a DMG of a pre-configured operating system.

# Creating Package Sources

A package source allows you to view and edit attributes of the package (such as files, scripts, permissions, and localizations) before it is built. Once a package source exists for a group of files, you can make modifications and build the package as many times as necessary.

You can create a package source using the following methods:

- **Snapshots**—Composer takes before and after snapshots of the file system and creates a package source based on the changes. This method allows you to monitor installations in all locations on the drive. If necessary, you can also quit Composer or log out/reboot during the installation process.
- **File system monitoring**—Composer uses the File System Events (FSEvents) framework to monitor any changes that are made to the file system during the installation process. Then, Composer creates a package source based on the changes. This method does not allow you to quit Composer or log in/reboot during the installation process. In addition, an excess of file system activity can cause FSEvents to miss changes.
- **Using pre-installed software**—You can use software that is pre-installed on your computer to create a package source based on package manifests. This method allows you to create package sources without monitoring the installation process.
- **Using user environment settings**—Package manifests can also be used to capture settings configured on your computer, such as Dashboard, Display, and Global Preference settings.
- **Dragging contents from the Finder**—A simple drag-and-drop process allows you to create a package source from files already installed on your computer.
- **Using an existing package**—Composer allows you to make modifications to an existing package or convert between the PKG and DMG package formats.

This section explains how to create package sources using these six methods.

## Taking Snapshots

If the files you want to package are not already installed on the drive, Composer can take a snapshot of the file system before and after the files have been installed and create a package source based on the changes.

Composer can take two kinds of snapshots:

- **Normal snapshots**—These snapshots capture any new files on the drive. These snapshots can take anywhere from ten seconds to several minutes depending on your hardware and the number of files on the drive.
- **New and modified snapshots**—These snapshots capture any new files on the drive, as well as any files that have been modified. These snapshots can take longer than normal snapshots, since Composer records the modifications date of each file while performing the snapshot.

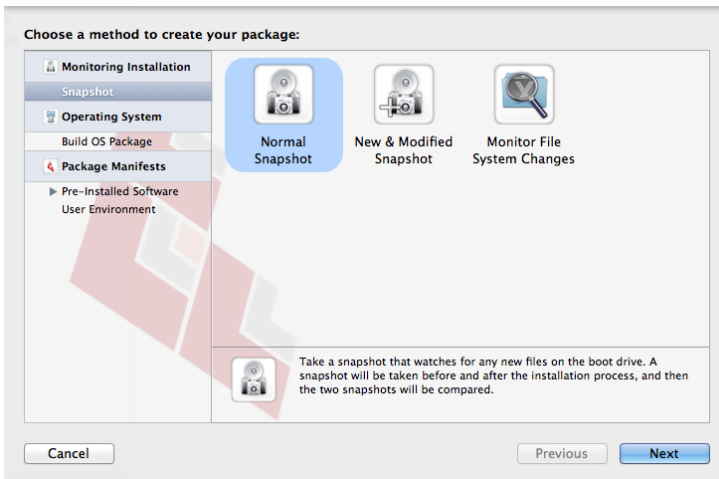
There are several benefits to using the snapshot approach:

- Composer monitors installations in all locations on the drive.
- You can quit Composer during the installation process.
- You can log out or reboot during the installation process.

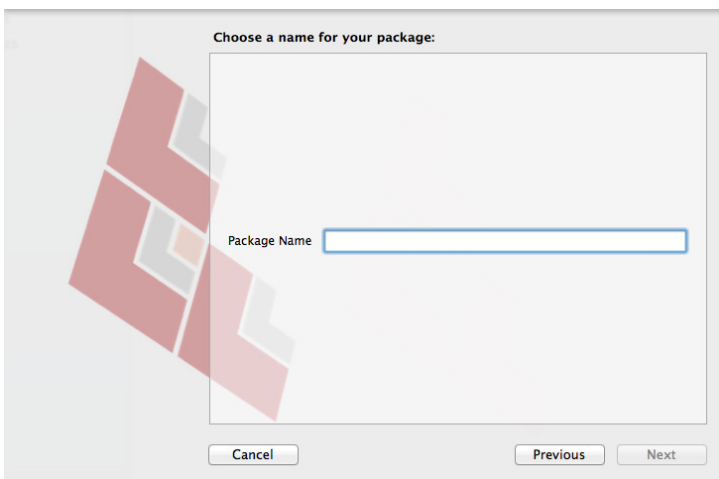
- If you delete a file while making modifications to a package source, it may be possible to restore the deleted file. For more information about restoring deleted files, see the “Editing a Package Source” section.

**To create a package source by taking snapshots:**

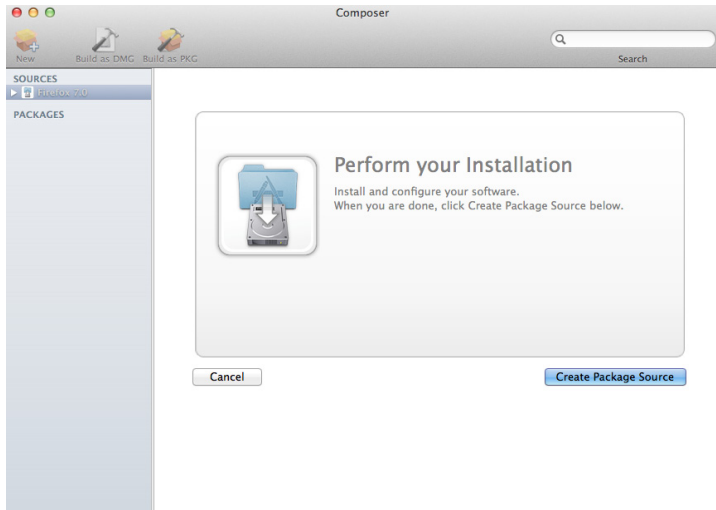
1. Open Composer and authenticate locally.
2. Click the **New** button in the toolbar.
3. Under the Monitor Installation heading in the sidebar, select **Snapshot**.
4. Select **Normal Snapshot** or **New & Modified Snapshot**, and then click **Next**.



5. Enter a name for the package and click **Next**.



6. Install and configure your software, and then click the **Create Package Source** button to initialize the “after” snapshot.



## Monitoring the File System

When creating a package source using file system monitoring, Composer uses the File System Events (FSEvents) framework that is built into Mac OS X to monitor any changes that are made to the file system. Each time a change is made, FSEvents receives a notification. After your software is installed, Composer analyzes the changes and creates a package source based on the results.

The following limitations should be taken into consideration when monitoring the file system to create a package source:

- You cannot quit Composer during the installation process.
- You cannot log in or restart during the installation process.
- It is possible for FSEvents to miss events if there is too much file system activity.

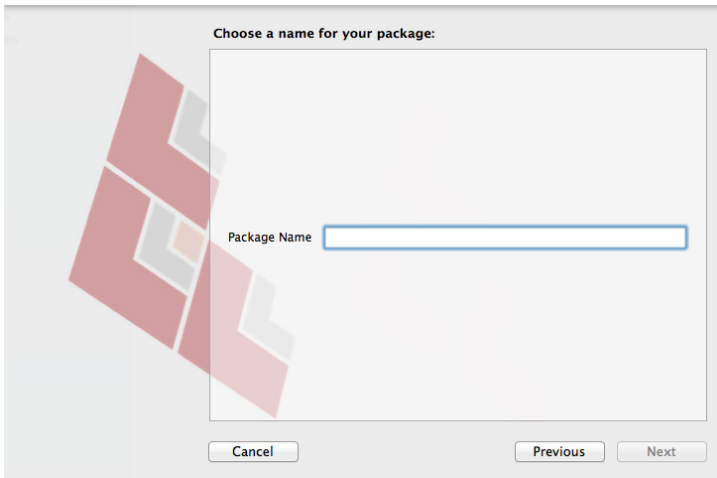
**To create a package source by monitoring the file system:**

1. Open Composer and authenticate locally.
2. Click the **New** button in the toolbar.
3. Under the Monitor Installation heading in the sidebar, select **Snapshot**.

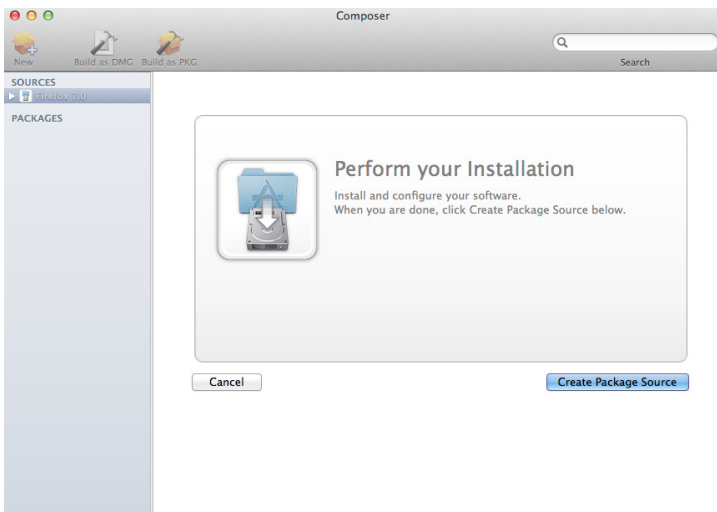
4. Select **Monitor File System Changes** and click **Next**.



5. Enter a name for the package and click **Next**.



6. Install and configure your software, and then click the **Create Package Source** button.





# Creating Package Sources from Pre-Installed Software

You can create a package source from software that is currently installed on your computer if Composer contains a package manifest for the software.

**Note:** If there is software you would like added to the package manifest options in Composer, email your recommendations to [diffs@jamfsoftware.com](mailto:diffs@jamfsoftware.com).

This section explains how to:

- View a list of available package manifests for pre-installed software
- Create a package source from pre-installed software

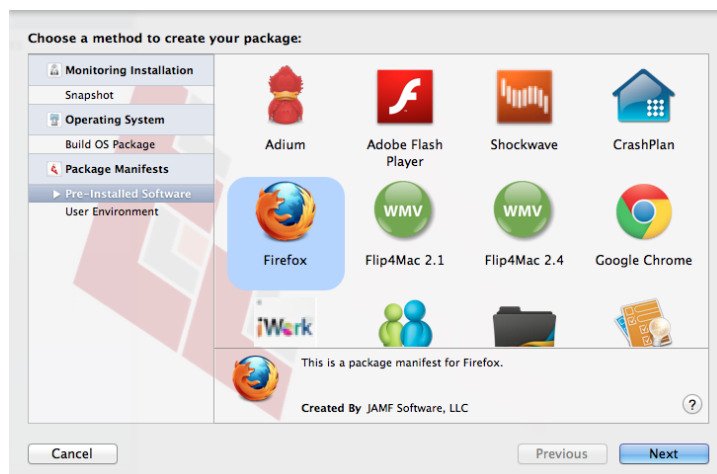
For instructions on creating package manifests, updating the package manifests available, and importing package manifests to Composer, see “Managing Package Manifests”.

## To view available package manifests for pre-installed software:

1. Open Composer and authenticate locally.
2. Click **New**.
3. To view package manifests for software installed on the computer, select **Pre-Installed Software**. Composer scans the file system and displays icons for the software it can package.
4. To view package manifests for software that is not installed on the computer, click the disclosure triangle next to **Pre-Installed Software** and select **Not Installed**.

## To create a package source from pre-installed software:

1. Open Composer and authenticate locally.
2. Click the **New** button in the toolbar.
3. Under the Package Manifests heading in the sidebar, select **Pre-Installed Software**.
4. Select the item(s) you want to create a package source from, and then click **Next**.



## Creating Package Sources from User Environment Settings

You can create a package source that captures the look-and-feel of your computer's interface, such as Dashboard, Display, and Global Preference settings. If Composer contains a package manifest for the setting you want to capture, you can create a package source from it.

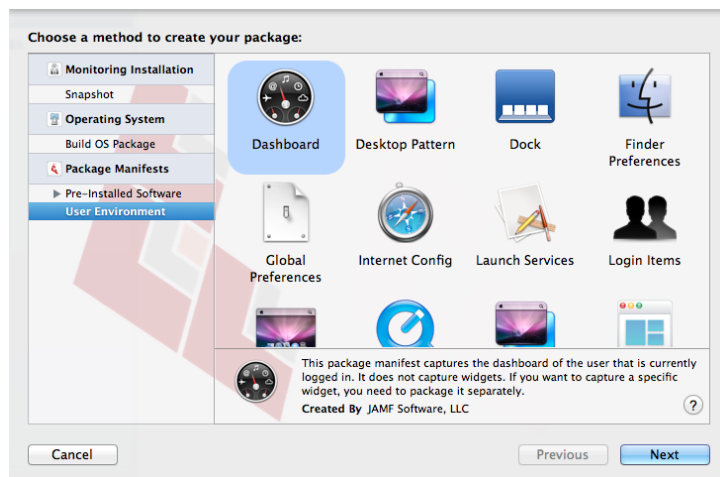
To determine which of your current settings Composer can package, select **User Environment** under the Package Manifests heading. Composer scans the file system and displays icons for the settings that it has package manifests for.

**Note:** If there is a setting you would like added to the package manifest options in Composer, email your recommendations to [diffs@jamfsoftware.com](mailto:diffs@jamfsoftware.com).

For instructions on creating package manifests, updating the package manifests available, and importing package manifests to Composer, see "Managing Package Manifests".

**To create a package source from user environment settings:**

1. Open Composer and authenticate locally.
2. Click the **New** button in the toolbar.
3. Under the Package Manifests heading in the sidebar, select **User Environment**.
4. Select the item(s) you want to create a package source from, and then click **Next**.



## Creating Package Sources by Dragging Contents from the Finder

If you already know which item you want to package, you can bypass the snapshot or monitoring process by dragging items from the Finder to the Sources list in Composer.

There are a few ways Composer handles these items:

- If the item is a package (DMG, PKG, or MPKG), it is listed in the sidebar under the Packages heading.
- If the item is a folder, the root of the folder is used as the root of the package if it is one of the following directories:

/Applications/

/Developer/

/Library/

/System/

/Users/

/bin/

/private/

/sbin/

/usr/

- Any other items are copied to their current location.

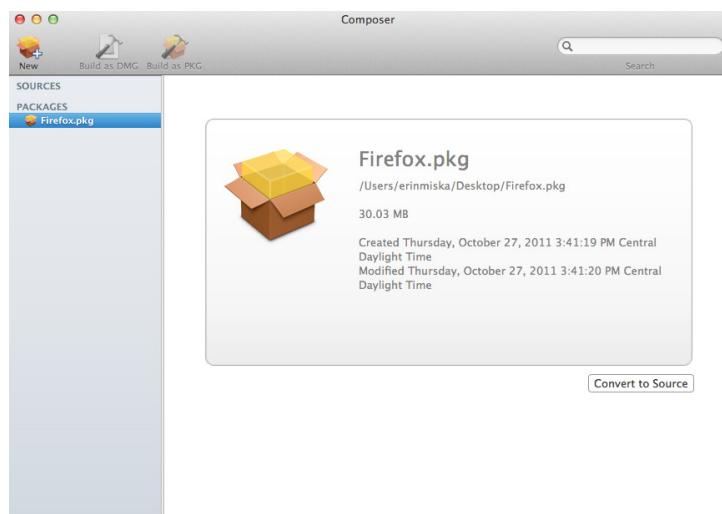
**Note:** This is the equivalent of a PreBuilt package in earlier versions of Composer.

## Creating Package Sources from Existing Packages

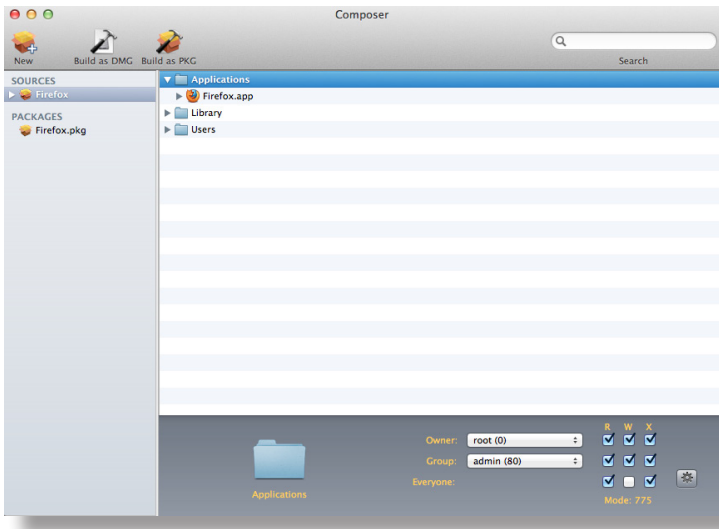
Composer allows you to rebuild an existing package (PKG, DMG, or MPKG) by converting it to a package source. After converting it to a package source, you can make changes to its contents and save a new copy of the package.

**To create a package source from an existing package:**

1. Open Composer and authenticate locally.
2. Drag the package you want to convert from the Finder to the sidebar in Composer. The package will appear under the Packages heading.
3. Select the package, and then click the **Convert to Source** button.



When the conversion is complete, a new package source is listed in the sidebar under the Sources heading.



# Managing Package Manifests

Package manifests are .composer files that can be used to create package sources from the software installed on your computer. They can also be used to capture settings configured on your computer, such as Dashboard, Display, and Global Preference settings.

Composer comes with over 100 package manifests. You can use the update feature in Composer to add new package manifests as they become available. You can also create your own package manifests and import package manifests that are stored on your computer.

This section explains how to:

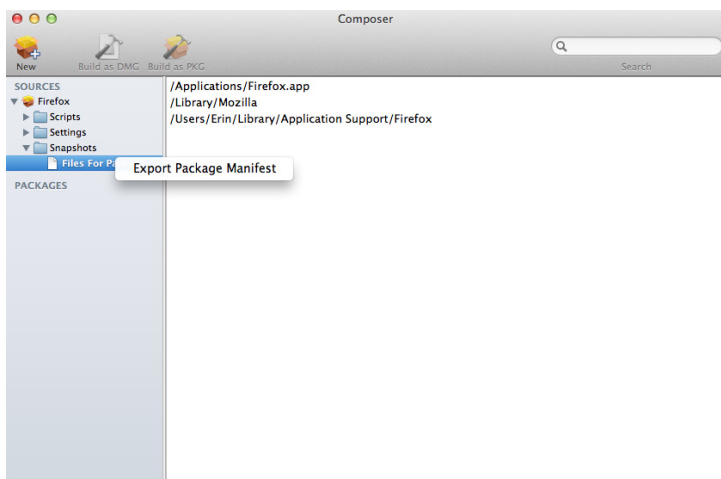
- Create package manifests
- Update the package manifests that are available in Composer
- Import package manifests

## Creating Package Manifests

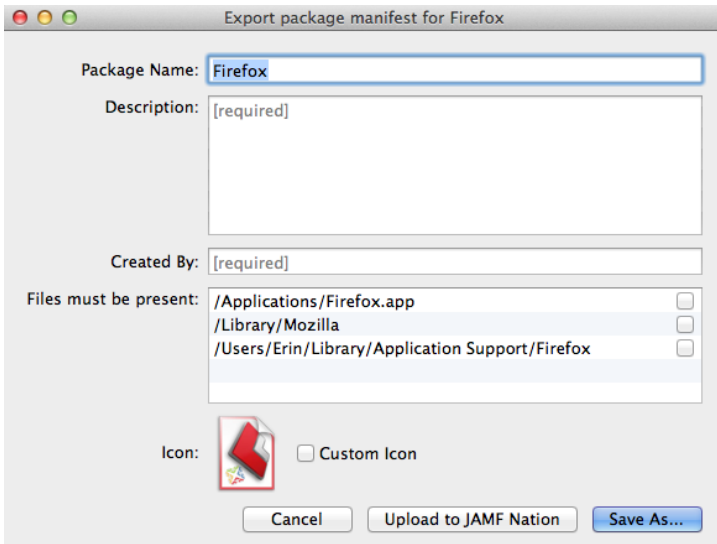
Composer allows you to create custom package manifests from existing package sources and save them on your computer.

**To create a package manifest:**

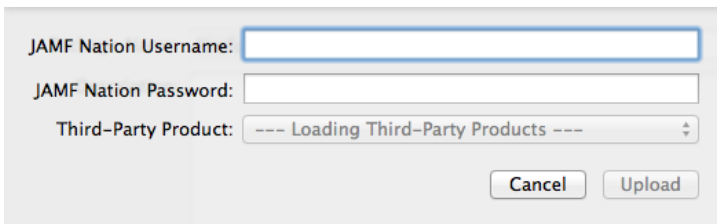
1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to an existing package source.
3. Click the disclosure triangle next to **Snapshots**.
4. Control-click (or right-click) **Files For Package** and select **Export Package Manifest**.



5. Enter a name for the package manifest.



6. Enter a description of the package manifest and the name of the person who is creating it.
7. Select the checkbox next to each file that must be present on a computer for the package manifest to appear under the Pre-Installed Software heading or the User Environment heading in Composer.
8. If desired, select the **Custom Icon** checkbox and choose an icon for the package manifest. The icon is displayed when viewing the package manifest in Composer.
9. If you want to upload the package manifest to JAMF Nation:
  - a. Click **Upload to JAMF Nation**.
  - b. Enter the username and password for your JAMF Nation account.



- c. Choose a third-party product to associate the package manifest with. For example, if you are creating a package manifest for Adobe Reader 10, associate it with the "Adobe Reader" third-party product.
  - d. Click **Upload**.
10. Click **Save As**.
  11. Choose a location to save the package manifest and click **Save**.

## Updating Package Manifests

Periodically, new package manifests become available for Composer. To ensure that you have the latest package manifests, choose **File > Update Package Manifests** from the menu bar in Composer.

Composer downloads the latest package manifests from JAMF Nation and any new package manifests that JAMF Software has added to the application, and stores them in the following location:

```
/Library/Application Support/JAMF/Composer/ImportedPackageManifests/
```

## Importing Package Manifests

If you do not want to add all package manifests from JAMF Nation to Composer, you can download one or more specific package manifests from JAMF Nation and import them to Composer. You can also import package manifests that you created.

To import package manifests that are saved to your computer, choose **File > Import Package Manifests** from the menu bar in Composer. Then, choose the package manifest you want to import.

Composer imports the package manifests and stores them in the following location:

```
/Library/Application Support/JAMF/Composer/ImportedPackageManifests/
```

# Editing Package Sources

If a file is listed in the sidebar under the Sources list in the sidebar, it exists as a package source and can be modified. If a file is not listed in the sidebar under the Sources list, a package source must be created before you can utilize the editing functions described in this section. See “Creating Package Sources” for more information about creating a package source.

**Note:** Composer does not allow you to create a package source from an OS package.

This section explains how to make the following modifications to a package source:

- View and edit the contents of the package source.
- Add scripts.
- Edit the `info.plist` and `description.plist` files.
- Add localizations.

## Viewing and Editing the Contents

Once a package source exists for the files you want to package, Composer allows you to:

- Delete files that should not be included in the package
- Add files by dragging them into Composer from the Finder
- Modify permissions on a file or folder
- Restore files that were deleted from the package source

In addition to viewing files or folders through the Composer interface, you can view this information in the Finder or using Quick Look.

## Deleting Files or Folders

In the Package Contents pane, select the item(s) you want to delete from your package source. Then, choose **Edit > Delete** from the menu bar.

## Adding Files

Drag the file(s) you want to add to your package source from the Finder into the Package Contents pane in Composer.

## Modifying Permissions on Files or Folders

Select a file or folder in the Package Contents pane in Composer to display its permissions in the bottom of the window. You can change the permissions using this display. Changes are saved automatically. If the selected item is a folder, you can apply the permissions that exist on the folder to each enclosed item by clicking the **Action** button (labeled with the gear icon) to the right of the X-column.



## Restoring Deleted Files or Folders

If you delete a file from the Package Contents pane, it may be possible to restore the file. The ability to restore a deleted file depends on the type of snapshot used to create the package source and the location of the file that was deleted. To restore a deleted file, Composer copies the file from its original location on the drive.

**Note:** A file can only be restored if a snapshot was used to create the package source.

**To restore a deleted file:**

1. Click the disclosure triangle next to the package source in the sidebar.
2. Click the disclosure triangle next to **Snapshots**.
3. Select **Files for Package** to display a list of files, folders, and directories from the snapshot.
4. Select the item you want to restore.
5. Control-click (or right-click) the selected item and choose **Restore**.

## Viewing Files or Folders Using the Finder

In the Package Contents pane, select the item(s) you want to preview. Then, choose **File > Reveal in Finder** from the menu bar.

## Viewing Files or Folders Using Quick Look

In the Package Contents pane, select the item(s) you want to preview. Then, choose **File > Quick Look** from the menu bar or press the Space bar.

**Note:** Quick Look is supported by OS X v10.5 or later.

## Adding Scripts

Composer allows you to manage scripts for PKGs. The following default scripts are available in shell and perl:

- InstallationCheck
- Postflight
- Postinstall
- Postupgrade
- Preflight
- Preinstall
- Preupgrade
- VolumeCheck

**Note:** Flat PKGs support `Preinstall` and `Postinstall` scripts only. To build a PKG that contains other scripts, you can deselect the **Build Flat PKGs** option in Composer preferences, or you can disable this preference for a single package. For information on how to disable this preference for a single package, see “Building PKGs”. For more information on flat PKGs, see “Managing Composer Preferences”.

These scripts read in the available parameters that are received from the installer and give descriptions for the supported exit codes.

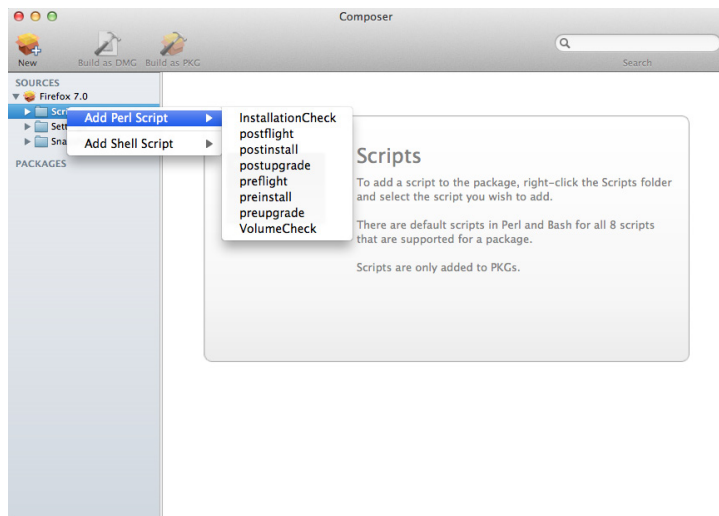
Composer also attempts to verify that the script syntax is valid. If a script appears to have invalid syntax, a warning icon appears.

To view the error that occurred while Composer was verifying the script, Control-click (or right-click) the script and choose **Compile Script**.

**Note:** `InstallationCheck` and `VolumeCheck` scripts have warning and failure messages that can be localized according to the needs of the user. To localize these messages, the corresponding `.strings` file (`InstallationCheck.strings` or `VolumeCheck.strings`) must be created for each localization.

### To add a script to a package source:

1. Click the disclosure triangle next to the package source in the sidebar.
2. Control-click (or right-click) **Scripts** and choose the script you want to add.



The script is displayed under the **Scripts** heading in the sidebar.

3. (Optional) Select the script in the sidebar to view or modify its contents.

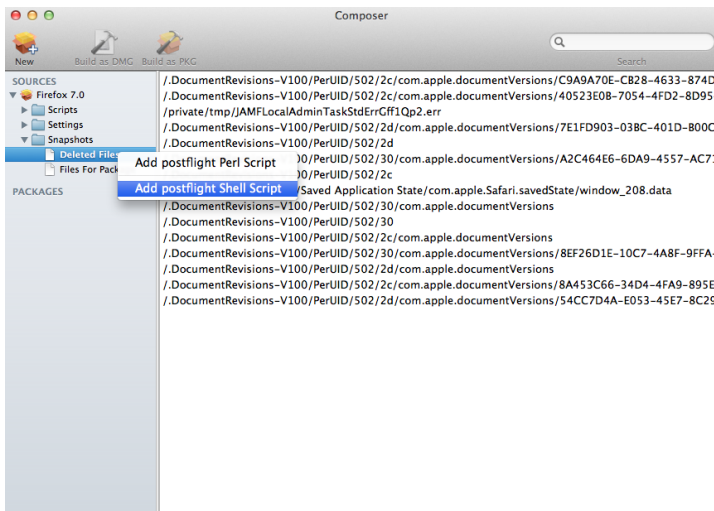
## Adding a Postflight Script that Removes Deleted Files from Clients

Adding a postflight script to a package source allows you to remove deprecated or unneeded files from client computers as clients install the package.

**Note:** This function is only available if a snapshot was used to create the package source.

To add a postflight script that removes deleted files from clients:

1. Click the disclosure triangle next to the package source in the sidebar.
2. Click the disclosure triangle next to **Snapshots**.
3. Select the Deleted Files heading to view the deleted files captured by the snapshot.
4. Control-click (or right-click) the Deleted Files heading and choose **Add postflight Shell Script**.



The script is displayed under the Scripts heading in the sidebar.

5. (Optional) Select the script in the sidebar to view or modify its contents.

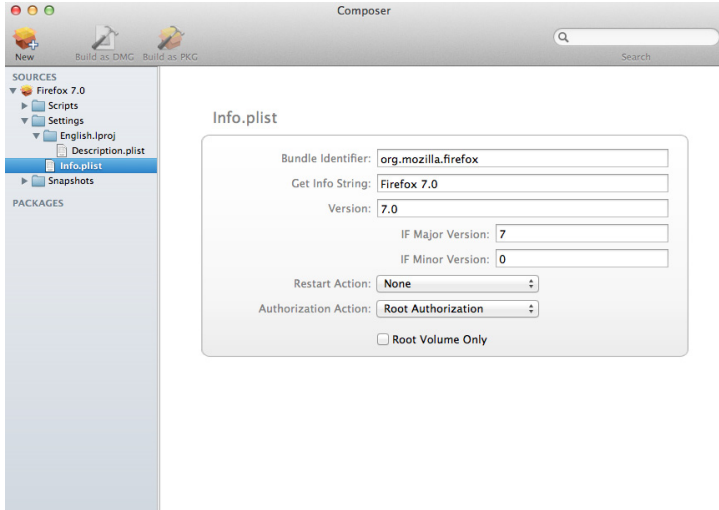
## Editing Info.plist and Description.plist Files

The Installer application uses information property list (`info.plist`) files and description property list (`description.plist`) files to display information about a package and determine how it is installed. Composer allows you to edit the most commonly used information in these files.

This section explains how to edit these files.

## Info.plist File

The `info.plist` file contains configuration information for a package. Composer allows you to define the `info.plist` keys and values shown in the screen shot below. After the screen shot, there is a list that further explains each key and value.



### Bundle Identifier

Identifies the package type. For example, `com.jamfsoftware.composer`

### Get Info String

Provides a description of the package. For example, `Composer 7.01 © 2009`

### Version

Identifies the iteration. For example, `7.01`

### IF Major Version

Identifies the major version number.

### IF Minor Version

Identifies the minor version number.

### Restart Action

Specifies reboot protocol for a package.

### Authorization Action

Specifies authorization requirements.

### Root Volume Only

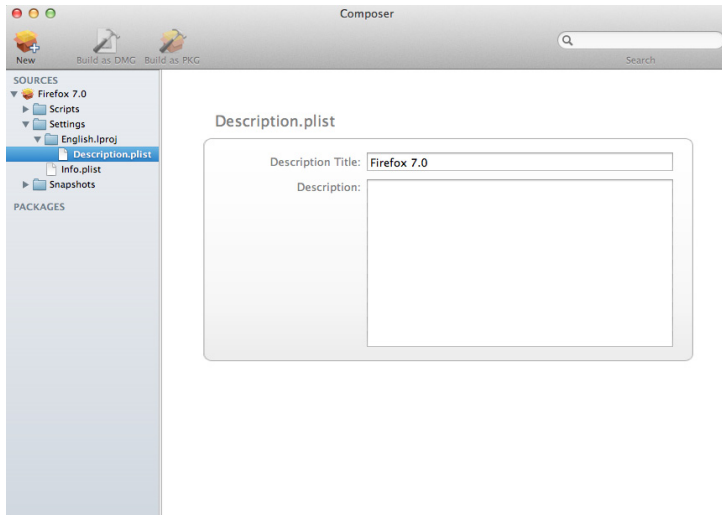
Indicates the package can only be installed to the root volume.

Less commonly used keys and values are also contained in the `info.plist` file. If you need to edit these items, Control-click (or right-click) **Info.plist** in the sidebar and select **Edit Manually**. This allows you to add or edit items in raw XML format.

## Description.plist File

The `description.plist` file allows you to define how a package presents itself in the Installer application.

Each localization includes its own `description.plist` file that allows you to define a description title and description for a package based on the target language.



There are other keys and values contained in the `description.plist` file. If you need to edit these items, Control-click (or right-click) **Description.plist** in the sidebar and select **Edit Manually**. This allows you to add or edit items in raw XML format.

## Adding Localizations

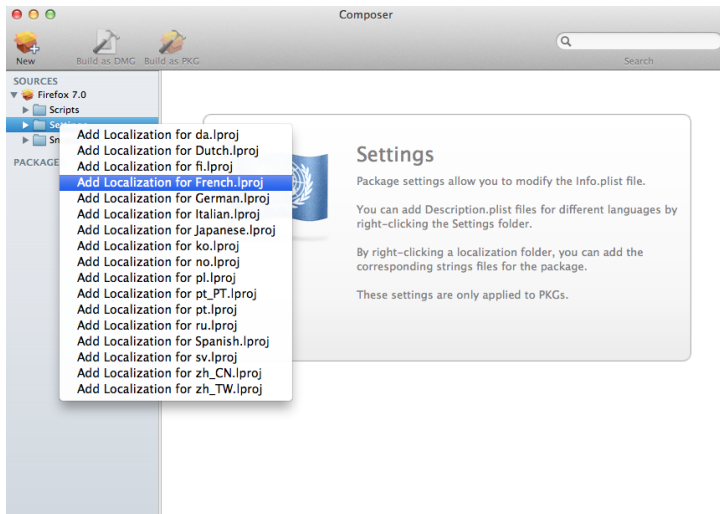
Localizations allow you to customize the language used when displaying package information to a user. By default, a package source only includes an English localization.

Composer includes defaults for the following localizations supported by the PKG format:

- `da.lproj`
- `Dutch.lproj`
- `English.lproj`
- `Fi.lproj`
- `French.lproj`
- `German.lproj`
- `Italian.lproj`
- `Japanese.lproj`
- `ko.lproj`
- `no.lproj`
- `pl.lproj`
- `pt_PT.lproj`
- `pt.lproj`
- `ru.lproj`
- `Spanish.lproj`
- `sv.lproj`
- `zh_CN.lproj`
- `zh_TW.lproj`

### To add a localization to a package source:

1. Click the disclosure triangle next to the package source in the sidebar.
2. Control-click (or right-click) **Settings** and choose the localization that you want to add.



## Adding and Editing Files for a Localization

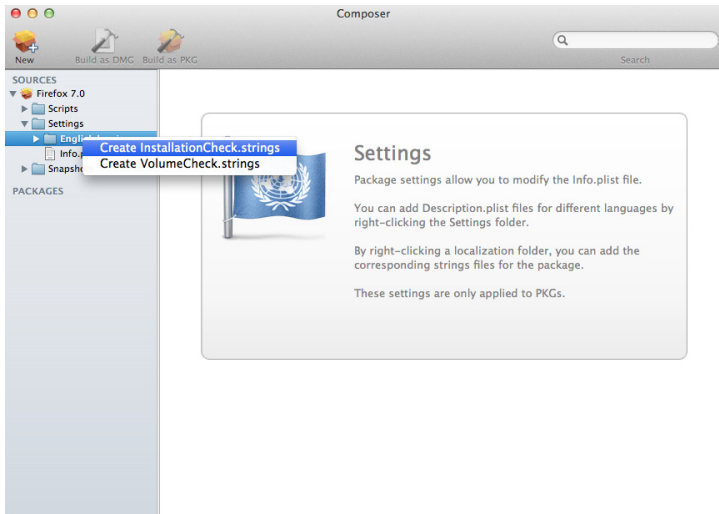
You can include two types of files in a localization:

- **Description.plist files**—These files display the title of a package and its description in the Installer application. Each localization contains a `description.plist` file by default. For instructions on how to edit these files, see “Editing Info.plist and Description.plist Files”.
- **Strings files**—`VolumeCheck.strings` and `InstallationCheck.strings` files are used to localize warning and error messages. These files are only effective when used in conjunction with their corresponding scripts (`VolumeCheck` and `InstallationCheck`). For instructions on how to add `VolumeCheck` and `InstallationCheck` scripts to a package source, see “Adding Scripts”.

### To add `InstallationCheck.strings` or `VolumeCheck.strings`:

1. Click the disclosure triangle next to the package source in the sidebar.
2. Click the disclosure triangle next to **Settings**.

- Control-click (or right-click) the language folder you want to add the .strings file to, and select **Create InstallationCheck.strings** or **Create VolumeCheck.strings**.



- Click the .strings file to modify its contents in the Package Contents pane.

# Building Packages from Package Sources

After you have verified the contents of a package source, Composer allows you to build two different types of packages: PKGs and DMGs. Each format has advantages depending on the intended use of the package and the tool you use to deploy it.

Once a package source exists in Composer, you can build a PKG or DMG package from the source at any time. You also have the ability to convert from one format to another after a package has been built. For more information about converting between the PKG and DMG formats, see “Creating Package Sources from Existing Packages”.

This section explains how to build PKGs and DMGs.

## Building PKGs

PKGs can be deployed using almost any deployment tool, such as Apple Remote Desktop (ARD), the Casper Suite, and other client management systems.

The PKG format allows for easy installation by the user. Double-clicking the package opens the Installer application and guides the user through the installation process.

**Note:** PKGs cannot dynamically deploy files in the user’s home directory to user templates when used with the Casper Suite.

By default, Composer builds flat PKGs. For more information on flat PKGs, see “Managing Composer Preferences”.

### To build a PKG:

1. Select the package source you want to build as a PKG from the Sources list in the sidebar.
2. Click the **Build as PKG** button in the toolbar.

**Note:** If the Build flat PKGs preference is enabled and the package source contains scripts that are not supported by flat PKGs, a dialog will appear. To disable this preference for this package only, click **Build as non-flat PKG**. To build a flat PKG that ignores unsupported scripts, click **Build as flat PKG**. For more information on which scripts are supported by flat PKGs, see “Adding Scripts”.

3. Select a location to save the package and click **Save**.



## Building DMGs

When used in conjunction with the Casper Suite, the DMG format allows you to dynamically deploy files and folders to each user that has an account on a computer, as well as the network home directories of currently logged-in users. There is also an option to deploy files and folders to the user template directories, ensuring that any new user receives the correct default environment.

### To build a DMG:

1. Select the package source you want to build as a DMG from the Sources list in the sidebar.
2. Click the **Build as DMG** button in the toolbar.
3. Select a location to save the package and click **Save**.

# Building OS Packages

In addition to building deployable packages of applications and other files, Composer allows you to build DMGs of pre-configured operating systems. OS packages can save you time and enhance consistency across your network.

While building an OS package with Composer is similar to building one with the Disk Utility application, Composer allows you to clean up the OS by removing unnecessary files before building the DMG.

Composer allows you to manage the following cleanup options for an OS package:

## **Compress Disk Image**

This option compresses the OS package DMG.

## **Delete Temp Files**

This option ensures the files in `/private/tmp` are deleted before building an OS package. These files are usually deleted during the startup process.

## **Delete Virtual Memory Files**

This option ensures that Virtual Memory files are deleted before building an OS package, including the potentially large `sleepfile`. These files are usually deleted and recreated during the startup process.

## **Delete Special Files**

Apple recommends deleting the following files before building an OS package:

```
/private/var/db/BootCache.playlist  
/private/var/db/volinfo.database
```

This option ensures that these files are deleted.

## **Delete Caches**

This option removes files in the `/Library/Caches` directory before building an OS package.

## **Remove Kerberos Certificate**

This option removes existing Kerberos certificates before building an OS package, preventing the “This computer already exists” error when attempting to bind a computer securely to Open Directory.

## **Ensure Trashes are Empty**

This option empties the Trash for any user with items in the `~/Trash` folder. It also updates a user’s `com.apple.dock.plist` file to reflect that the Trash is empty.

## Configuring the OS

Before building your OS package, consider performing the following tasks to ensure the OS is completely configured to your environment:

- Install a clean copy of Mac OS X.
- Create the main admin account.
- For security purposes, create a secondary admin account to be used with Secure Shell (SSH, or remote login in Mac OS X).
- Activate SSH.
- Secure SSH by allowing only a single user or group access.
- Perform any other system security fortification.
- Configure miscellaneous settings, such as:
  - Energy Saver settings
  - Keyboard and mouse settings
  - Network settings
  - QuickTime settings
  - Sharing settings
  - Login Window settings
  - Auto-login settings
  - Name and password or list of users
- Run all available software updates.
- Turn off the Software Update schedule.
- Confirm Universal Access settings.
- Confirm Directory Access settings.
- LDAPv3 bindings can often be built into your image.
- Active Directory bindings should not be built into the image. Each computer must join the domain.
- Make sure the Trash is empty.

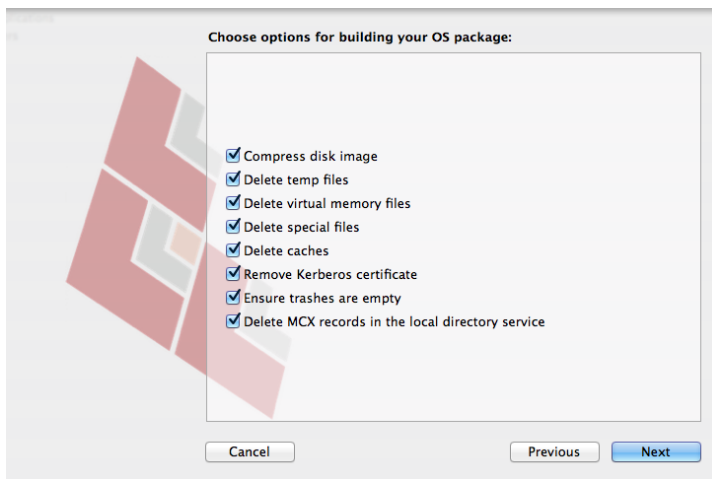
## Packaging the OS

When you're finished configuring the OS, boot to another startup disk to build the DMG.

**To build an OS package:**

1. Open Composer and authenticate locally.
2. Click the **New** button in the toolbar.
3. Under the Operating System heading in the sidebar, select **Build OS Package**.
4. Select the drive you want to package and click **Next**.

5. Choose options for removing unnecessary files from the package, and then click **Next**.



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

# Managing Composer Preferences

Composer allows you to manage the following settings:

- Toolbar preferences
- Package preferences
- Cleanup options for OS packages
- Excluded files
- Location of the work directory
- Default bundle identifier

You can access Composer preferences by choosing **Composer > Preferences** from the menu bar.

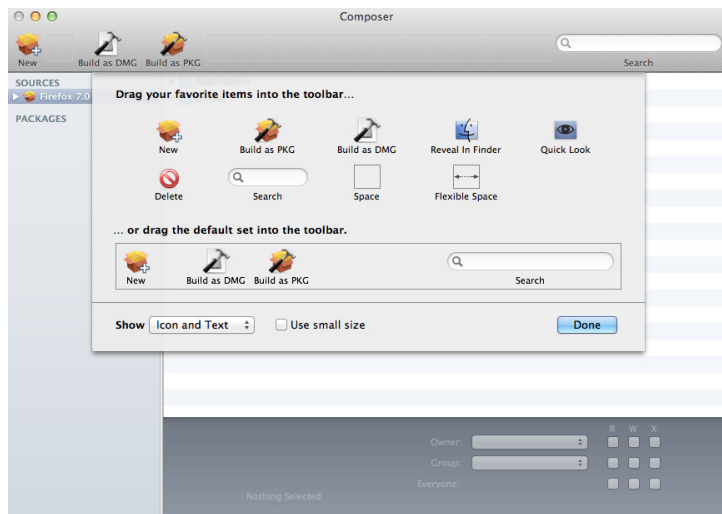
This section provides a detailed explanation of Composer preferences.

## Toolbar Preferences

Composer allows you to customize the toolbar by adding and removing items.

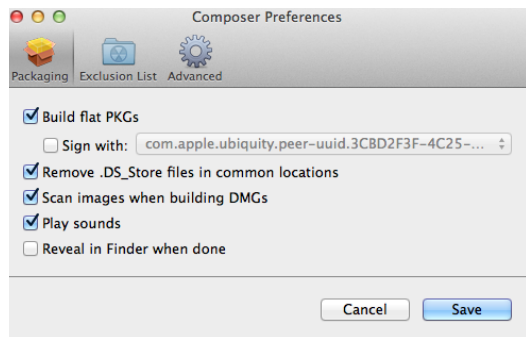
To add items to the toolbar, Control-click (or right-click) the toolbar and select **Customize toolbar**. Then drag desired items to the toolbar.

To remove an item from the toolbar, simply drag the item off of the toolbar.



# Package Preferences

Composer allows you to manage Package preferences from the pane in the screen shot below.



This pane includes the following preference settings:

## Build flat PKGs

By default, Composer builds flat PKGs. Flat PKGs consist of a single file and allow for easier and more reliable deployment than non-flat PKGs. You cannot view or modify the contents of a flat PKG after it is built.

## Sign flat PKGs

This option allows you to sign flat PKGs with an installer certificate (.p12) obtained from Apple's Developer Certificate Utility. Signing PKGs with an installer certificate makes it possible to verify that the PKG was created by an identified developer. It also allows users to install PKGs on computers that have Apple's Gatekeeper feature set to only allow applications downloaded from the Mac App Store and identified developers.

To sign flat PKGs, Composer must be running on OS X v10.7 or later.

Select the **Sign with** option and choose an installer certificate from the pop-up menu. Installer certificates that are located in the login keychain in Keychain Access are displayed in the pop-up menu.

**Note:** The pop-up menu also displays application certificates that are located in the login keychain in Keychain Access. It is important that you use an installer certificate, not an application certificate, to sign flat PKGs.

To obtain an installer certificate from Apple's Developer Certificate Utility, you must be a registered Apple Developer in the Mac Developer Program. To enroll in the Mac Developer Program, visit the following website:

<https://developer.apple.com/programs/mac/>

To install a signed QuickAdd package, the system keychain in Keychain Access must contain Apple's Developer ID Certification Authority intermediate certificate. For instructions on how to obtain this certificate and import it to the system keychain on client computers, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=294>

### **Remove .DS\_Store Files in Common Locations**

Enabling this option ensures the removal of any files that disturb the way Finder windows are presented on a user's computer. Any .DS\_Store files necessary to configure views of deployed files and folders will not be removed.

This feature removes .DS\_Store files in the following locations:

- / .DS\_Store
- /Applications/.DS\_Store
- /Applications/Utilities/.DS\_Store
- /Developer/.DS\_Store
- /Library/.DS\_Store
- /System/.DS\_Store
- /Users/.DS\_Store
- /Users/<username>/.DS\_Store
- /Users/<username>/<first\_level\_directory>/.DS\_Store

### **Scan Images When Building DMGs**

Scanning images when building a DMG calculates the checksum and stores it in the DMG.

The checksum is used to ensure proper installation of the DMG package.

### **Play Sounds**

Composer plays a sound each time a package source is created or deleted.

### **Reveal in Finder when done**

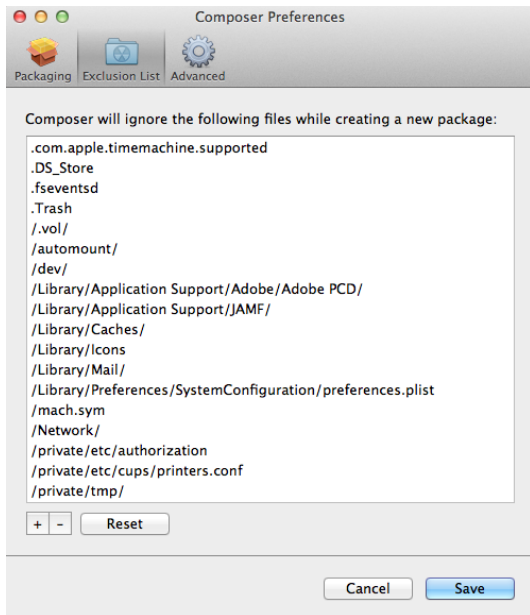
When this option is enabled, Composer reveals newly built packages in a Finder window.

## **Exclusion List**

The exclusion list allows you to specify files and folders that should be ignored when creating a package using a snapshot or file system monitoring.

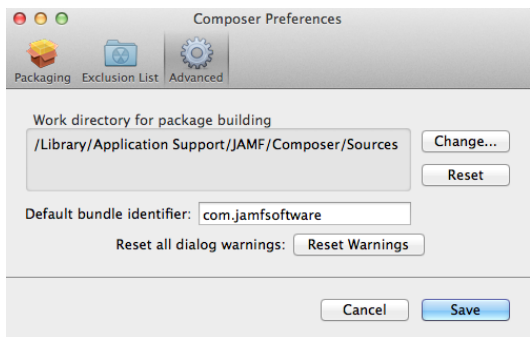
To view the exclusion list, click the **Exclusion List** button in the toolbar. A list of common files and folders is specified by default.

To add and remove files, use the **Add (+)** and **Delete (-)** buttons at the bottom of the list.



## Advanced Preferences

Composer allows you to manage some advanced preferences from the pane in the screen shot below.



This pane includes the following preference settings:

### Work Directory

When Composer creates a package source, it copies files to a work directory. This work directory must have permissions enabled.

To change this directory, click the **Change** button, or hold down the Option key when you open Composer.

### Default Bundle Identifier

The default bundle identifier is used when creating the `info.plist` file for a new package source. For example, if the default bundle identifier is "com.jamfsoftware", and you create a package source named "Composer", the bundle identifier for the package source is "com.jamfsoftware.composer".



# Building Your Client Management Framework

## Integrating with LDAP Servers

If you utilize one or more directory services to store information about the users in your organization, you can integrate the JAMF Software Server (JSS) with the directory service(s) to:

- Look up and populate user information for inventory purposes
- Authenticate users to the Casper Suite
- Authenticate users to Self Service
- Assign policies and Managed Preference profiles to user groups

**Note:** Integrating with Open Directory allows the JSS to access both user and computer list information. For details on accessing computer list information from Open Directory, see the “Adding LDAP Server Connections Manually” section.

This section explains how to:

- Add LDAP server connections using the LDAP Server Connection Assistant or manually
- Test LDAP server connections
- Edit and delete LDAP server connections
- Troubleshoot LDAP server connections

## Using the LDAP Server Connection Assistant

The LDAP Server Connection Assistant walks you through the process of adding an LDAP server connection to the JSS.

The assistant allows you to integrate with the following directory services:

- Apple’s Open Directory
- Microsoft’s Active Directory
- Novell’s eDirectory

**Note:** To integrate with other directory services or access computer list information from Open Directory, you must configure the connection manually.

### To use the LDAP Server Connection Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Server Connection** link.
4. Click the **Add LDAP Server Connection** button.
5. Choose the LDAP server you want to integrate with and click the **Continue** button.
6. Enter the host name (DNS name or IP address) for the LDAP server and click **Continue**.
7. Enter credentials for the LDAP service account and click **Continue**.
8. For testing purposes, enter the usernames for two different accounts in the LDAP server and click **Continue**.
9. Verify the returned attribute mappings are correct. If the attribute mappings are correct, click **Continue** and skip to step 11.

The screenshot shows the 'LDAP Server Connection Assistant' interface at the 'Mappings' step. A progress bar at the top indicates the current step. Below the title 'Verify Attribute Mappings', there is a brief instruction: 'Verify that the attributes from your LDAP server are mapped correctly to the JSS. To change an attribute mapping, click the ellipsis button across from it.' A table displays the mappings for two LDAP users: 'bcrocker\_OD' and 'dsmith\_OD'. Each row includes a JSS User Attribute, an LDAP User Attribute, and the corresponding values for the two LDAP users. Ellipsis buttons are present at the end of each row for editing. At the bottom, there are 'Back', 'Cancel', and 'Continue' buttons.

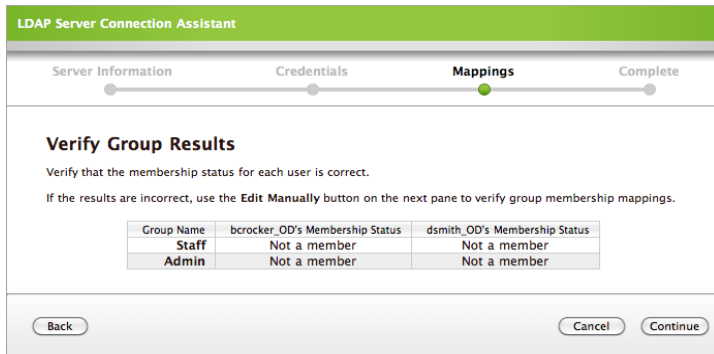
JSS User Attribute	LDAP User Attribute	Value for bcrocker_OD	Value for dsmith_OD	
Username:	uid	bcrocker_OD	dsmith_OD	⋮
Realname:	cn	Betty Crocker	Dave Smith	⋮
Email:	mail	bcrocker@jamfsoftware.com	dsmith@jamfsoftware.com	⋮
Phone:				⋮
Department:				⋮
Building:				⋮
Room:				⋮
Position:				⋮

10. If an attribute mapping is incorrect, change the mapping appropriately.
  - a. Click the **Ellipsis** button across from the mapping.
  - b. Choose the correct value for the attribute from one of the pop-up menus.

The screenshot shows the 'LDAP Server Connection Assistant' interface at the 'Edit Mappings for Email' step. A progress bar at the top indicates the current step. Below the title 'Edit Mappings for Email', there is a brief instruction: 'Choose the value for the attribute from one of the pop-up menus, and then click the Return to Verify Mappings button.' Three dropdown menus are shown, each with a selected value: 'LDAP Attribute: mail', 'Value for bcrocker\_OD: bcrocker@jamfsoftware.com', and 'Value for dsmith\_OD: dsmith@jamfsoftware.com'. At the bottom, there is a 'Return to Verify Mappings' button.

- c. Click the **Return to Attribute Mappings** button.

- d. Verify the changes are correct and click the **Continue** button.
11. For testing purposes, enter the names of two different user groups in the LDAP server and click **Continue**.
12. Verify the group membership status of each test user is correct and click **Continue**.



13. Click **Save** to save the LDAP server connection and continue using the JSS.  
If you want to make changes before you save the connection, click the **Edit Manually** button, make the necessary changes, and then click the **Save** button.

## Adding LDAP Server Connections Manually

Before adding an LDAP server connection manually, it is important that you are familiar with search bases, object classes, and attributes. If you are not familiar with these concepts, use the LDAP Server Connection Assistant to ensure attributes are mapped correctly.

Adding the connection manually allows you to:

- Integrate with directory services other than Open Directory, Active Directory, and Novell eDirectory
- Access computer list information from Open Directory

After adding the connection, test it to make sure it's working properly. See the "Testing LDAP Server Connections" section for testing instructions.

This section provides an overview of the Connection and Mappings panes you'll use to add the connection and step-by-step instructions on how to do so.

## Connection Pane

This pane allows you to configure how the JSS connects to an LDAP server.

**Edit LDAP Server Connection**

Connection | Mappings

Display Name:

Host name:

Encrypt using SSL

Use custom port

---

Use for:

Create Mappings Based On:

Domain:

---

Authentication Type:

---

Open/Close times out in:  seconds

Connection times out in:  seconds

Referrals:

Use wildcards when searching for objects

Cancel Save

### Display name

This field allows you to enter a display name for the LDAP server.

### Host name

This field allows you to enter the DNS name or IP address for the LDAP server.

### Encrypt Using SSL

You must select this checkbox if you want to connect to the LDAP server over SSL.

**Note:** For this to work, the LDAP server must have SSL enabled.

### Use custom port

If the LDAP server is not running on the standard port, you must select this checkbox and enter the port on which it is running.

### Use for

This pop-up menu allows you to specify the type of information you want to access from the LDAP server.

### Create Mappings Based On

This pop-up menu allows you to select the LDAP server you want to connect to.

### Domain

This field allows you to enter the domain for the LDAP server.

## Authentication Type

If the LDAP server requires authentication, specify the authentication type using this pop-up menu. After choosing an authentication type, two additional fields appear in which you can enter credentials for the LDAP service account.

Most LDAP servers require simple authentication.

## Open/Close times out in \_\_\_\_ seconds

This field allows you to enter the maximum number of seconds you want to wait for the server to open or close a connection before it times out.

## Connection times out in \_\_\_\_ seconds

This field allows you to enter the maximum number of seconds you want to wait for the server to return results before the connection times out.

## Referrals

This pop-up menu allows you to choose whether to ignore, follow, or utilize default LDAP referrals to locate information.

## Use wildcards when searching for objects

Select this checkbox if you want the JSS to return partial matches when searching the LDAP server for information.

## Mappings Pane

This pane allows you to map attributes and specify object class and search base data.

If you're not familiar with these concepts, use the LDAP Server Connection Assistant to add the connection.

**Edit LDAP Server Connection**

Connection | Mappings

**Users**

Map Users to: All ObjectClass values below

ObjectClass: (Comma separated)

Search Base:

all subtrees  first level only

Map User ID to:

Map Username to:

Map Real Name to:

Map Email Address to:

Append to email results:

Map Department to:

Map Building to:

Map Room to:

Map Phone to:

Map Position to:

Map User UUID to:

Bindable String Representation Needed

### To configure an LDAP server connection manually:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Server Connection** link.
4. Click the **Add LDAP Server Connection** button.
5. Select the **Configure manually** option and click the **Continue** button.
6. Configure the connection using the information on the Connection and Mappings panes.
7. Click the **Save** button.

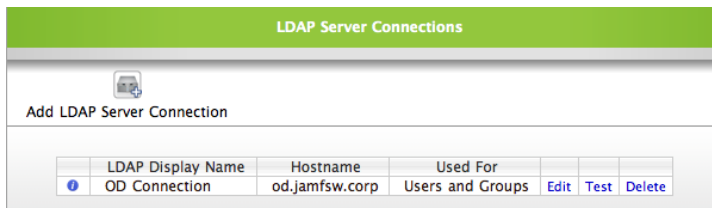
## Testing LDAP Server Connections

Before using an LDAP server connection as part of your framework, test the connection by looking up user (or computer list) information. If the results are returned correctly, the connection is working.

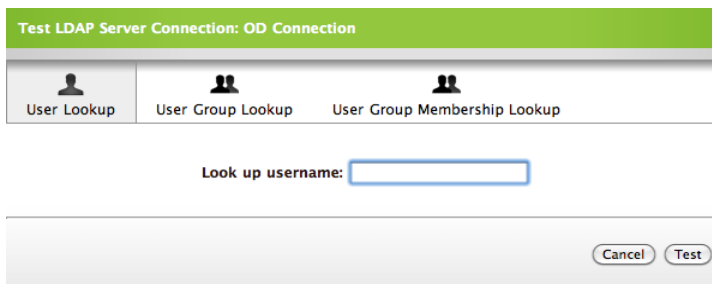
This section explains how to look up user and computer list information.

### To look up user information from an LDAP server:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Server Connection** link.
4. Click the **Test** link across from the connection you want to test.



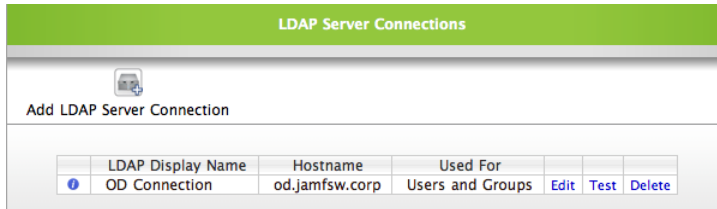
5. Click the **User Lookup**, **User Group Lookup**, or **User Group Membership Lookup** tab.
6. Enter information in the field(s) provided.



7. Click the **Test** button.

### To look up computer list information from Open Directory:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Servers Connection** link.
4. Click the **Test** link across from the Open Directory connection you want to test.



5. Click the **Computer Lookup**, **Computer Group Lookup**, or **Computer Group Membership Lookup** tab.
6. Enter information in the field(s) provided.
7. Click the **Test** button.

## Editing LDAP Server Connections

### To edit an LDAP server connection:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Servers Connection** link.
4. Click the **Edit** link across from the connection you want to edit and make changes manually. For more information about the Connection and Mappings panes, see the "Adding LDAP Server Connections Manually" section.
5. Click the **Save** button.

## Deleting LDAP Server Connections

### To delete an LDAP server connection from the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Servers Connection** link.
4. Click the **Delete** link across from the connection you want to delete.
5. Click the **Delete** button to confirm.

## Tools for Troubleshooting LDAP Server Connections

This section describes two tools you can use to troubleshoot the connection between the JSS and an LDAP server.

### Apache Directory LDAP Studio

The Apache Directory LDAP Studio allows you to connect to an LDAP server to pinpoint initial connections and find search bases and mappings. You can download Apache Directory LDAP Studio at:

<https://directory.apache.org/studio/>

### Workgroup Manager

Apple's Workgroup Manager allows you to view detailed information for individual LDAP server accounts.

**To view LDAP information using Workgroup Manager:**

1. Open Workgroup Manager.
2. Connect to your server.
3. From the menu bar, choose **Workgroup Manager > Preferences**.
4. Select the **Show "All Records" tab and inspector** checkbox, and then click **OK**.
5. Click the **All Records** tab (target icon) displayed in the sidebar to view the records.



# Managing JSS User Accounts

The JAMF Software Server (JSS) is a multi-user application. You can grant different levels of access to each user by setting up JSS user accounts and assigning different privileges to each one.

Individual JSS user accounts can be created manually or—if you have an LDAP server connection set up—added from a directory service. You can also grant access to groups from an LDAP server.

This section explains how to:

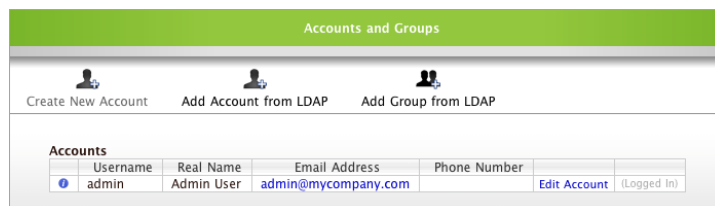
- Create a new user account in the JSS
- Add a user account from an LDAP server
- Upgrade the Distinguished Name (DN) from an LDAP account
- Grant access to a group from an LDAP server

**Note:** JSS users added from an LDAP server receive the privileges assigned to their individual user accounts. LDAP members that don't have individual accounts in the JSS, but are members of one or more groups with access, receive the privileges assigned to each group.

**Important:** It is recommended that you have at least one JSS user account that is not from an LDAP server in case the connection between the JSS and the LDAP server is interrupted.

**To create a new user account in the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Accounts** link.
4. Click the **Create New Account** button.



5. Enter user information on the Account pane.

**Create New Account**

Account Privileges API Privileges Notifications

Username: JSS User  
 Realname:   
 Email Address:   
 Phone:   
 Password: .....  
 Verify Password:

Cancel Save

6. Click the **Privileges** tab and select the checkbox next to each privilege you want to grant the user.

**Create New Account**

Account Privileges API Privileges Notifications

[Grant All Privileges](#)  
[Revoke All Privileges](#)

**JSS - Home Tab Privileges**

Change Password

**JSS - Inventory Tab Privileges**

View Inventory Tab  
 Perform Advanced Searches  
 Save Advanced Searches

7. Click the **API Privileges** tab and select the API privileges you want to grant the user.

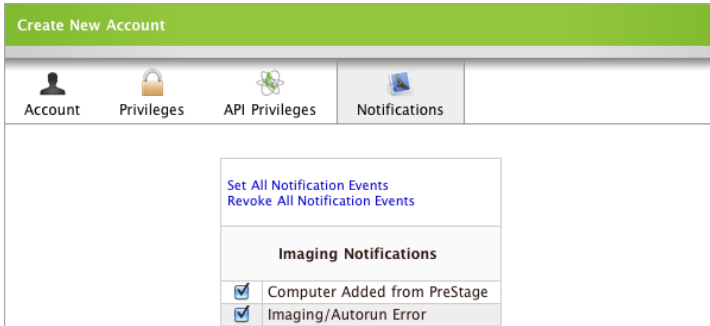
**Create New Account**

Account Privileges API Privileges Notifications

	Read	Update	Create	Delete
<b>Buildings</b>	<input checked="" type="checkbox"/>			
<b>Categories</b>	<input checked="" type="checkbox"/>			
<b>Computers</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Computer Groups</b>	<input type="checkbox"/>			
<b>Departments</b>	<input type="checkbox"/>			

- Click the **Notifications** tab and select the checkbox next to each event you want the user to receive a notification about.

**Note:** A valid email address must be entered on the Account pane for notifications to be sent.

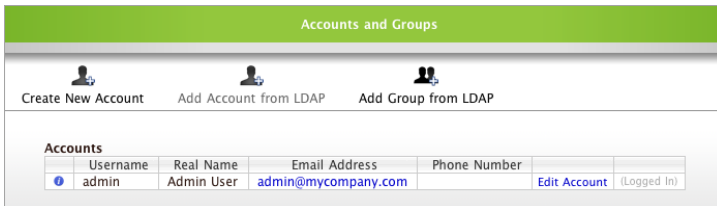


- Click **Save**.

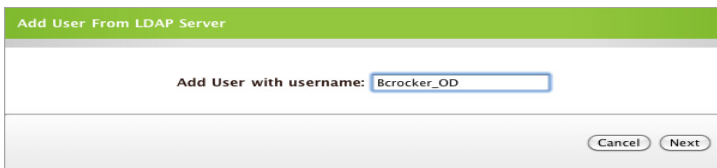
**To add a user account from an LDAP server:**

- Log in to the JSS with a web browser.
- Click the **Settings** tab.
- Click the **Accounts** link.
- Click the **Add Account from LDAP** button.

If you don't see this button, you need to set up an LDAP server connection before completing these steps. (For more information, see the "Integrating with LDAP Servers" section.)



- Enter the username for the account you want to add and click **Next**.



- When the JSS returns the results, click the **Add <username>** link next to the user you want to add.



7. Configure accounts settings on the Privileges, API Privileges, and Notifications panes.
8. Click **Save**.

**To update the Distinguished Name (DN) for an LDAP account:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Accounts** link.
4. Click the **Edit Account** link next to the account you want to modify.
5. Click the **Update DN** button.

The screenshot shows the 'Create New Account' form with the following fields and values:

- Username:** bcrocker\_OD
- Realname:** Betty Crocker
- Email Address:** bcrocker@jamfsoftware.co
- Phone:** (empty)
- Distinguished Name:** uid=bcrocker\_OD,cn=user

Below the Distinguished Name field is an **Update DN...** button. At the bottom of the form, it says "(This user is from an LDAP Server)". There are **Cancel** and **Save** buttons at the bottom right.

6. Enter the new Distinguished Name and click **Save**.

The screenshot shows the 'Create New Account' form with the **Update DN...** button clicked. The **New Distinguished Name** field now contains the following text:

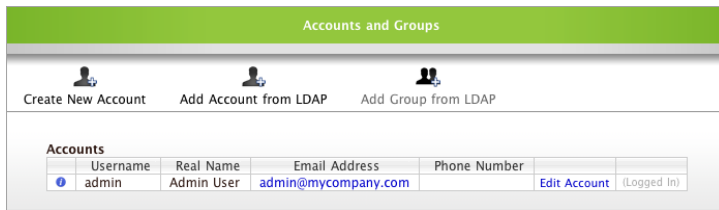
```
uid=bcrocker_OD,cn=users,dc=od,dc=jamfsw,dc=corp
```

There are **Cancel** and **Save** buttons at the bottom right.

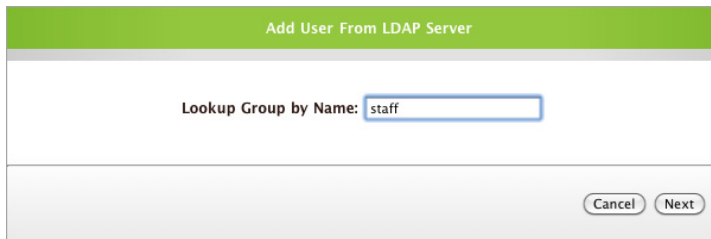
**To grant access to an LDAP group:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Accounts** link.

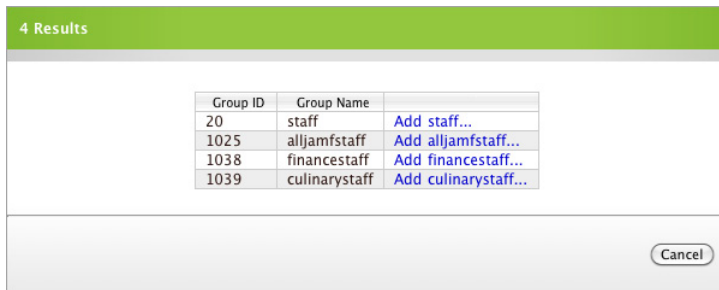
- Click the **Add Group from LDAP** button in the toolbar.  
If you don't see this button, you need to set up an LDAP server connection before completing these steps. (For more information, see the "Integrating with LDAP Servers" section.)



- Enter the name of the group you want to add and click **Next**.



- When the JSS returns the results, click the **Add <group name>** link next to the group you want to add.



- Set privileges for the group on the Privileges pane and click **Save**.

# Adding Software Update Servers

Apple allows you to host your own software update server internally using Mac OS X Server. This reduces bandwidth by downloading the packages once per server instead of once per client and allows you to approve updates before they become available.

Before using Casper Remote or a policy to run Software Update from an internally hosted software update server, you need to specify one or more servers in the JAMF Software Server (JSS).

When Casper Remote runs Software Update on remote computers, the process takes place in the background, so users don't see the process and are not prompted to authenticate. This also means the user does not need to be an administrator or even be logged in for Software Update to run on the client.

Running Software Update with Casper Remote or a policy installs all available software updates for the computer. You can control which updates are available using the Server Admin application on Mac OS X Server.

This section explains how to add, edit, and delete a software update server.

## To add a software update server:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Add Server** button in the toolbar.
5. Select the **Software Update** option and click **Continue**.
6. Enter a display name for the server.
7. Enter the DNS name or IP address for the Mac OS X Server on which the Software Update service is running.
8. If you are not using port 8088, enter the port you are using in the **Port** field.
9. If you do not want to use this server as the default software update server for all users, deselect the **Set Server System Wide** checkbox.

10. Click the **Save** button.

Edit Software Update Server: Untitled Software Update Server

Display Name: Software Update Serve

DNS Name or IP: SoftwareUpdate.mycor

Port: 8088

Set Server System Wide:

Cancel Save

#### To edit a software update server:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Software Update Servers** tab.
5. Click the **Edit Server** link next to the server and make the necessary changes.
6. Click the **Save** button.

#### To delete a software update server:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Software Update Servers** tab.
5. Click the **Delete Server** link next to the server.
6. Click the **Delete** button to confirm.

# Adding NetBoot Servers

If you have one or more NetBoot servers configured in the JAMF Software Server (JSS), you can reboot clients to a NetBoot server remotely using a policy or Casper Remote.

NetBoot servers are not set up automatically. To set up a NetBoot server, you need to set up Mac OS X Server, configure the NetBoot service, and then create the NetBoot image.

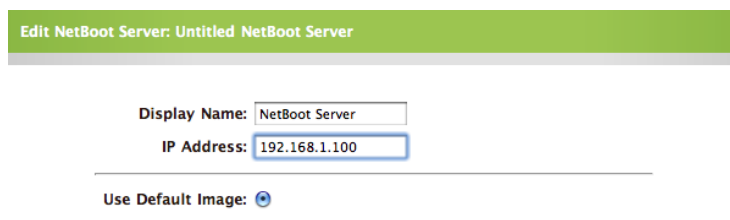
There are a few different ways you can set up a NetBoot server when you add it to the JSS—each gives you a different level of control. You can set up a NetBoot server that allows you to:

- Boot to a default image
- Boot to a non-default image
- Boot using manually entered information

This section explains how to set up, edit, and delete a NetBoot server in the JSS.

## To boot a NetBoot server to a default image:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Add Server** button in the toolbar.
5. Select the **NetBoot** option and click **Continue**.
6. Enter a display name for the server.
7. Enter the IP address for the NetBoot server.



Display Name:

IP Address:

Use Default Image:

8. Click the **Save** button.

## To boot a NetBoot server to a non-default image:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Add Server** button in the toolbar.



5. Select the **NetBoot** option and click **Continue**.
6. Enter a display name for the server.
7. Enter the IP address for the NetBoot server.
8. Select the **Use Specific Image** option.
9. Use the **Target Platform** pop-up menu to specify the processor architecture for the NetBoot image.
10. In the **Share Point** field, enter the share point for the image. This is usually something like NetBootSP0. You can locate the directory name in the folder on Mac OS X Server in the following location:  
/Library/NetBoot/
11. In the **Set** field, enter the set in the directory you specified in the **Share Point** field. This usually starts with Image\_ followed by the index of the NetBoot image, and the .nbi file extension. For example, image\_10012049807.nbi.
12. In the **Image** field, enter the NetBoot image in the directory you specified in the **Share Point** field. This is usually identified as System.dmg.
13. Choose "NFS" or "HTTP" from the **Protocol** pop-up menu.

The screenshot shows the 'Edit NetBoot Server: NetBoot Server' configuration window. The fields are as follows:

- Display Name: NetBoot Server
- IP Address: 192.168.1.100
- Use Default Image:
- Use Specific Image:
- Target Platform: Intel/x86
- Share Point: NetBootSP0
- Set: image\_10012049801.nbi
- Image: System.dmg
- Protocol: NFS
- Configure Manually:
- boot-args: (empty field)
- boot-file: (empty field)
- boot-device: enet:192.168.1.100

Buttons: Cancel, Save

14. Click the **Save** button.

**To boot a NetBoot server using manually entered information:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **Add Server** button in the toolbar.

5. Select the **NetBoot** option and click **Continue**.
6. Enter a display name for the server.
7. Enter the IP address for the NetBoot server.
8. Select the **Configure Manually** option.
9. In the fields provided, enter the boot -args, boot-file, and boot-device that should be set in Open Firmware/EFI and click the **Save** button.

**Note:** These items must be entered exactly. The arguments for NetBoot images used with PowerPC-based hardware should look similar to this:

**Boot -args**

```
rp=nfs:192.168.1.9:/private/tftpboot/NetBoot/NetBootSP0:Image_10012040959.nbi/System.dmg
```

**Boot-file**

```
enet:192.168.1.9,NetBoot\NetBootSP0\Image_10012040959.nbi\mach.macosx
```

**Boot-device**

```
enet:192.168.1.9,NetBoot\NetBootSP0\Image_10012040959.nbi\booter
```

The arguments for NetBoot images used with Intel-based hardware should look similar to:

**Boot -args**

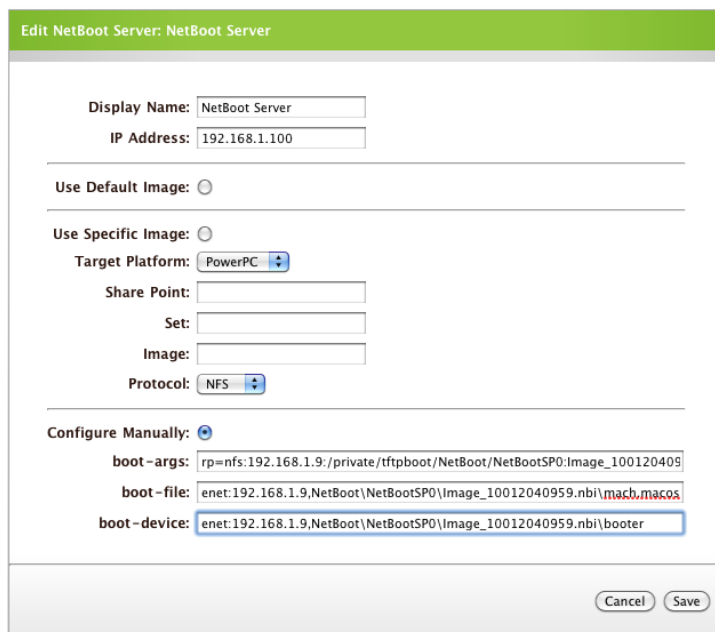
```
rp=nfs:192.168.1.9:/private/tftpboot/NetBoot/NetBootSP0:image_10012040959.nbi/System.dmg
```

**Boot-file**

```
tftp://192.168.1.9/NetBoot/NetBootSP0/image_10012040959.nbi/i386/mach.macosx
```

**Boot-device**

```
tftp://192.168.1.9/NetBoot/NetBootSP0/image_10012040959.nbi/i386/booter
```



**To edit a NetBoot server:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **NetBoot Servers** tab.
5. Click the **Edit Server** link next to the server and make the necessary changes.
6. Click the **Save** button.

**To delete a NetBoot server:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Servers** link.
4. Click the **NetBoot Servers** tab.
5. Click the **Delete Server** link across from the server.
6. Click the **Delete** button to confirm.

# Managing Buildings and Departments

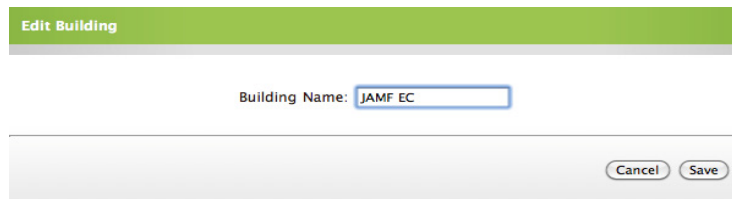
Buildings and departments are organizational components that give you an easy way to perform inventory searches, assign policies to client computers, and assign Managed Preferences to client computers.

## Buildings

This section explains how to create, edit, and delete a building in the JAMF Software Server (JSS).

### To create a building:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Buildings** link.
4. Click the **Create New Building** button.
5. Enter a name for the building and click the **Save** button.



### To edit a building:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Buildings** link.
4. Click the **Edit Building** link across from the building that you want to edit.
5. Change the name of the building.
6. Click **Save**.

### To delete a building:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Buildings** link.
4. Click the **Delete Building** link across from the building that you want to delete.

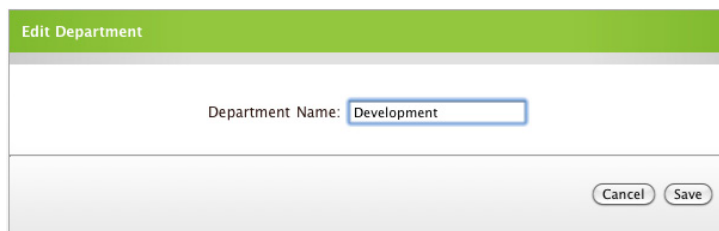
5. Click **Delete** to confirm.

## Departments

This section explains how to create, edit, and delete a department in the JSS.

### To create a department:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Departments** link.
4. Click the **Create New Department** button.
5. Enter a name for the department and click the **Save** button.



The screenshot shows a web form titled "Edit Department". The form has a light green header bar with the text "Edit Department". Below the header, there is a text input field labeled "Department Name:" containing the text "Development". At the bottom right of the form, there are two buttons: "Cancel" and "Save".

### To edit a department:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Departments** link.
4. Click the **Edit Department** link across from the department that you want to edit.
5. Change the name of the department.
6. Click **Save**.

### To delete a department:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Departments** link.
4. Click the **Delete Department** link across from the department that you want to delete.
5. Click **Delete** to confirm.

# Managing Network Segments

A network segment is a range of IP addresses that can be used to perform the following actions:

- Assign client computers to the closest distribution point.
- Update the department and/or building to which client computers belong.
- Limit a policy's scope to ensure that the policy does not run when client computers are offsite.
- Limit a PreStage's scope to image only client computers within the specified IP range.

Network segments can be class B or class C subnets, or any IP range therein.

This section explains how to create, edit, and delete a network segment in the JAMF Software Server (JSS).

## To create a network segment:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Network Segments** link.
4. Click the **Create New Network Segment** button in the toolbar.
5. Enter a display name for the network segment.
6. Specify an IP range for the network segment by entering starting and ending IP addresses.
7. If you want to assign a distribution point, NetBoot server, or Software Update server to the network segment, make your selections from the corresponding pop-up menus.

The screenshot shows the 'Edit Network Segment' dialog box. The fields are as follows:

- Display Name: Network Segment
- Starting IP Address: 10.10.12.1
- Ending IP Address: 10.10.14.255
- Default Distribution Point: No Distribution Point
- Default NetBoot Server: No NetBoot Server
- Default Software Update Server: No Software Update Server
- Default Department: No Department
- Default Building: No Building
- Override Departments in Inventory:
- Override Buildings in Inventory:

Buttons: Cancel, Save

8. If the IP range falls within a specific department and/or building, use the **Default Department** and **Building** pop-up menus to specify which one(s) it belongs to.
9. If you want clients within the network segment to reflect this department and/or building in their inventory record when they enter the segment, select the **Override Departments/Buildings in Inventory** option(s).

10. Click the **Save** button.

**To edit a network segment:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Network Segments** link.
4. Click the **Edit Network Segment** link across from the network segment that you want to edit and make the necessary changes.
5. Click **Save**.

**To delete a network segment:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Network Segments** link.
4. Click the **Delete Network Segment** link across from the network setting you want to delete.
5. Click **Delete** to confirm.

# Managing Packages

This section explains how to:

- Add new packages
- Change package attributes
- Add DMGs of Adobe Installer DVDs
- Add DMGs of Adobe Updaters
- Add DMGs of Mac OS X Installer DVDs
- Index packages
- Delete packages

## Adding New Packages

Before you deploy a package, you must add it to the JAMF Software Server (JSS) using Casper Admin and assign it to one or more distribution points.

There are two ways to add a new package to Casper Admin:

- Drag a package into Casper Admin
- Copy the package directly to a distribution point

### Dragging Packages into Casper Admin

When you drag a package into Casper Admin, it is copied to the master distribution point and displayed in blue text in the Unknown category until you assign it to a software category.

**To add a package to Casper Admin:**

1. Open Casper Admin and authenticate to the JSS.
2. Drag the package from the Finder to the Package pane in Casper Admin.

### Copying Packages Directly to the Distribution Point

This method copies the package to the Packages folder at the root of the file share. You can enter information about the package into the JSS manually.

If you open Casper Admin after adding the package, the name of the package is displayed in blue text in the **Unknown** category in the sidebar.

**To add a package manually:**

1. Copy the package to the Packages folder on your distribution point.
2. Log in to the JSS with a web browser.



3. Click the **Settings** tab.
4. Click the **Casper Admin** link.
5. Click the **New Package** button and enter information about the package on the Info pane.

**Note:** The information entered in **File Name** field must match the name of the file exactly.

6. Click **Save**.

The screenshot shows the 'Edit Package' dialog box with the 'Info' tab selected. The 'Package Info' section includes the following fields and options:

- Display Name:** Firefox.dmg
- Category:** Unknown (dropdown menu)
- File Name:** Firefox.dmg
- Note:** If you change the file name here, you will need to do so manually on your Distribution Point(s)
- Info:** (empty text area)
- Notes:** (empty text area)

Buttons for 'Cancel' and 'Save' are located at the bottom right of the dialog.

## Changing Package Attributes

You can change the attributes that determine how a package is installed.

This section explains:

- How to modify package attributes using Casper Admin or the JSS
- The attributes listed on the Summary, Info, and Options panes

### To change package attributes using Casper Admin:

1. Open Casper Admin.
2. Select the package that you want to change.
3. Click the **Info** button in the toolbar.
4. Make changes to the information on the Info and Options panes, and then click **OK**.

## To change package attributes using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link and click the package name.
4. Make changes on the Info and Options panes, and then click **Save**.

## Summary Pane

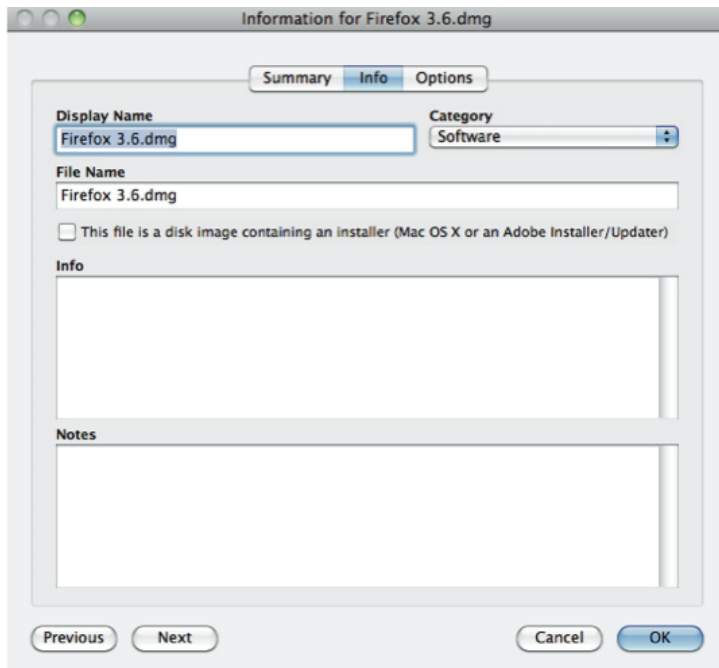
This pane displays an overview of the package. The **Reveal in Finder** button displays the package in a Finder window.

**Note:** The Summary pane exists in the Casper Admin application only. It is not included in the web version of Casper Admin.



## Info Pane

This pane allows you to modify basic information about a package.



The following attributes are displayed on this pane:

### Display Name

This is the customizable name that identifies a package when it is displayed in a list of packages or policies. The display name does not have to match the name of the package.

### File Name

This is the name of the package.

If you change a filename using the web version of Casper Admin, you must manually update the filename on each distribution point. If you change a filename using the Casper Admin application, this information is automatically updated for you.

### Category

This identifies the organizational category to which a package belongs.

### Info

The information displayed to the administrator when a package is being deployed.

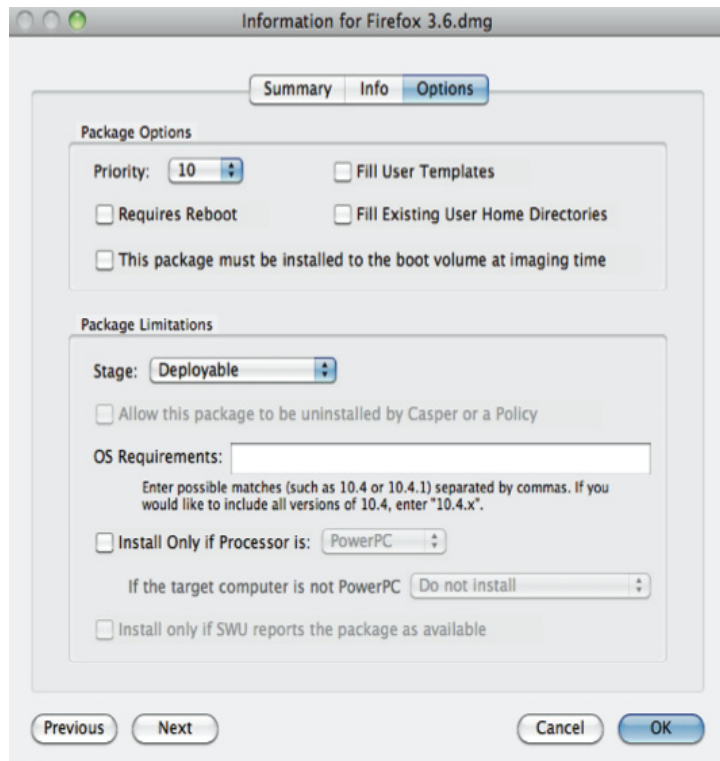
### Notes

Notes are only displayed in Casper Admin. They are helpful when tracking information about a package, such as who created it and when it was built.

## Options Pane

This pane allows you to specify deployment information and set criteria that limits whether a client computer can install or uninstall a package.

Setting these limitations prevents packages from being deployed to client computers that should not receive them.



The following attributes are displayed on this pane:

### Priority

This determines the order in which packages are installed. For example, an OS package should have a priority of 1 to ensure that it is installed first. An updater or a package that needs to overwrite files that may exist in another package should have a priority of 20.

### Fill User Templates

The default settings for a new user's home directory are located in the User Template folder. When you select this option, the files and folders in the first home directory located in `/Users/` are copied to the User Template directories in:

`/System/Library/User Template/`

Selecting this option allows you to distribute preferences or documents and provide a default work environment to any new user on a client computer.

**Note:** This option is only available for DMG packages.

### Fill Existing User Home Directories

Selecting this option copies the files and folders in the first home directory located in /Users/ to every existing home directory on the client computer.

**Note:** This option is only available for DMG packages.

### This package must be installed to the boot volume at imaging time

If this option is selected, Casper Imaging installs the package with the first run script.

### Stage

You can limit how a package is used and deployed by choosing one of the following options from the **Stage pop-up** menu:

- **Testing**—The package can only be deployed using Casper Remote (not a policy), and can only be pushed to five computers at a time.
- **Non-Deployable**—The package cannot be deployed. This setting is useful if the package needs to be taken out of production temporarily for licensing or other reasons.
- **Deleted**—The package has been deleted from Casper Admin.

### Allow Uninstall

Selecting this option allows administrators to uninstall a package using a policy or Casper Remote. Administrators will not be able to uninstall a package using a policy or Casper Remote unless this option is selected.

Some packages—for example, operating system updates and security updates—should not be uninstalled, since they contain files required to boot the client computer.

**Note:** A package must be indexed before this option can be selected. (For more information on indexing packages, see the “Indexing Packages” section.)

### OS Requirements

If certain operating system requirements are needed to install a package, enter the requirements in this field using the following guidelines:

- If a package can be installed on any version of OS X v10.6 (but not v10.5), type “10.6.x”.
- If a package can only be installed on OS X v10.5.6, type “10.5.6”.
- If the entry has more than one requirement, separate each requirement with a comma.
- If a package does not have any operating system requirements, leave this field blank.

### Install Only if Processor Is [PowerPC/x86]

Some packages are built only for a single architecture. You can specify this information by selecting this option and choosing **PowerPC** or **X86** from the pop-up menu.

To install an alternate package when a non-compliant architecture is encountered, choose an alternate package from the **If the target computer’s processor is not there** pop-up menu.

### Install Only if SWU Reports are Available

Selecting this option prompts Casper Remote or a policy to run Software Update for packages that may be available as updates.

For this feature to work properly, you must remove the .pkg or .mpkg file extension from the package's display name. If this still does not work, execute the following command in a Terminal window:

```
softwareupdate -l
```

It is important to ensure the information provided in the **Display Name** field matches the name of the package that is displayed in the command-line version of Software Update.

**Note:** This option is only available for PKG packages.

## Adding DMGs of Adobe Installer DVDs

Adobe CS3 and CS4 products can be deployed without repackaging by adding a DMG of the Adobe Installer DVD to Casper Admin and identifying it as an Adobe Installer Image.

If you download installer media directly from Adobe, it is already in DMG format. If you have installer media on DVD, you must first create the DMG using Disk Utility.

Since the Adobe Installer Image, itself, is not a deployable object, you must use Casper Admin or the JSS to create the Adobe installations that install and configure Adobe products.

Creating an Adobe installation involves the following steps:

1. Create the DMG.
2. Add the Adobe Installer DMG.
3. Create a new Adobe installation using Casper Admin or the JSS.

### Step 1: Create the DMG

1. Insert the installer DVD into a computer with Mac OS X.
2. Open **Disk Utility** from the **Utilities** folder.
3. Click the **DVD** button in the sidebar.
4. From the menu bar, choose **File > New > New Image From <name of the DVD>**.
5. Save as a compressed DMG.

### Step 2: Add the Adobe Installer DMG

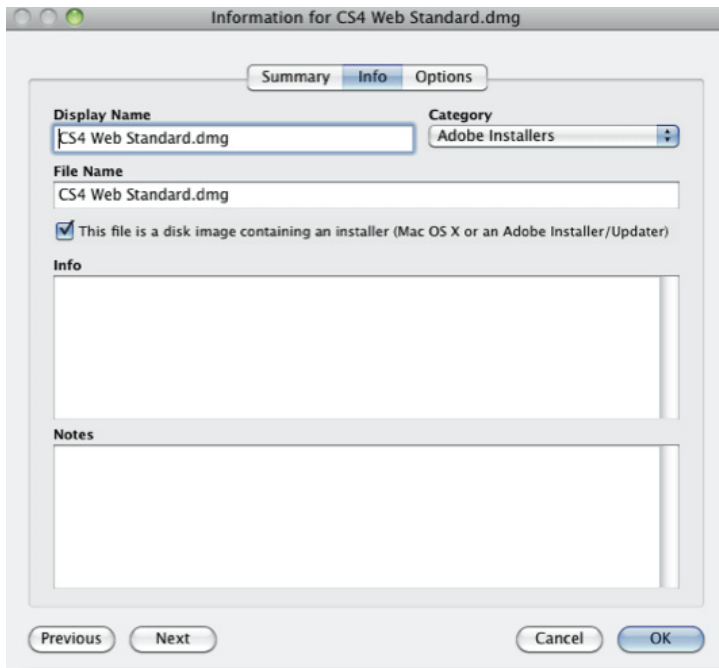
1. Open Casper Admin.
2. Drag the DMG of the Adobe Installer DVD into Casper Admin.

This copies the DMG directly to the master distribution point.

After Casper Admin copies the DMG, the Info pane is displayed. If it does not appear, click the **Info** button in the toolbar.

3. Click the **Info** tab and select the **This file is a disk image containing an installer (Mac OS X or an Adobe Installer/Updater)** option.

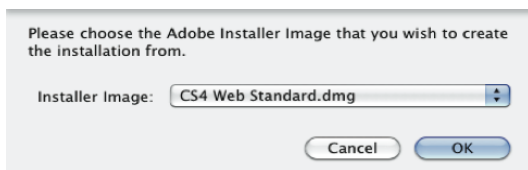
It can take Casper Admin up to 30 seconds to analyze the contents of the DMG. When this process is complete, the Options pane appears and a list of payloads available with the installer is displayed.



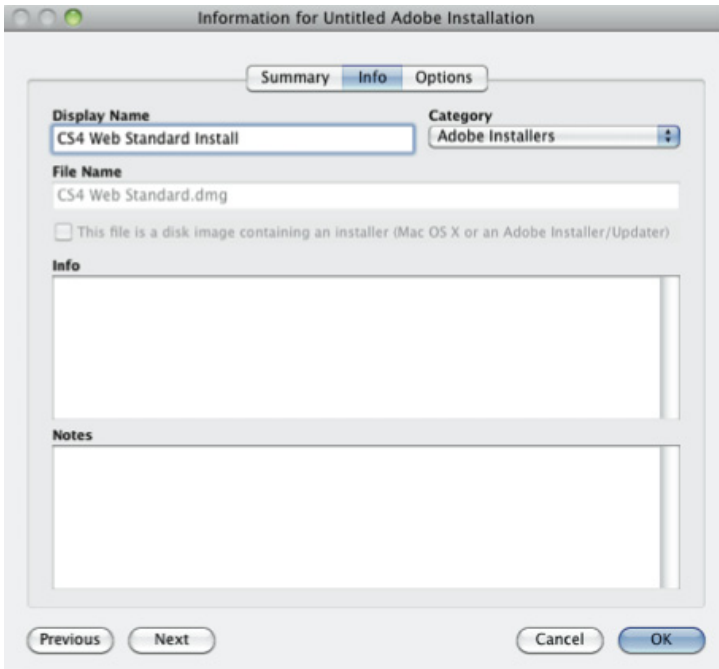
4. Click **OK** and select **Adobe Installer Images** in the **View Type** list to see the listing for the DMG.

### Step 3: Create a New Adobe Installation Using Casper Admin

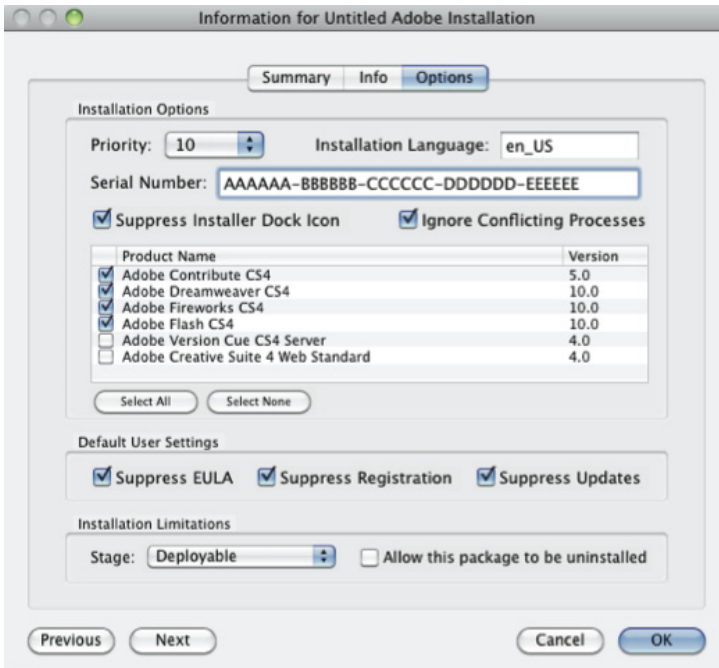
1. Open Casper Admin.
2. Click the **New Adobe Install** button in the toolbar.
3. If you have multiple Adobe Installer Images, choose the one on which you want to base your installation from the **Installer Image** pop-up menu.



4. Enter a display name for the installation.



5. Click the **Options** tab and set the installation options.

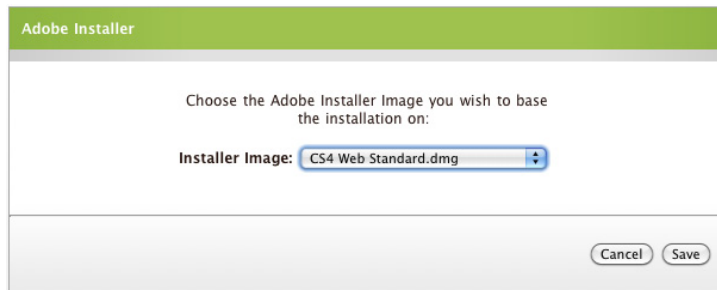


6. Click **OK**.

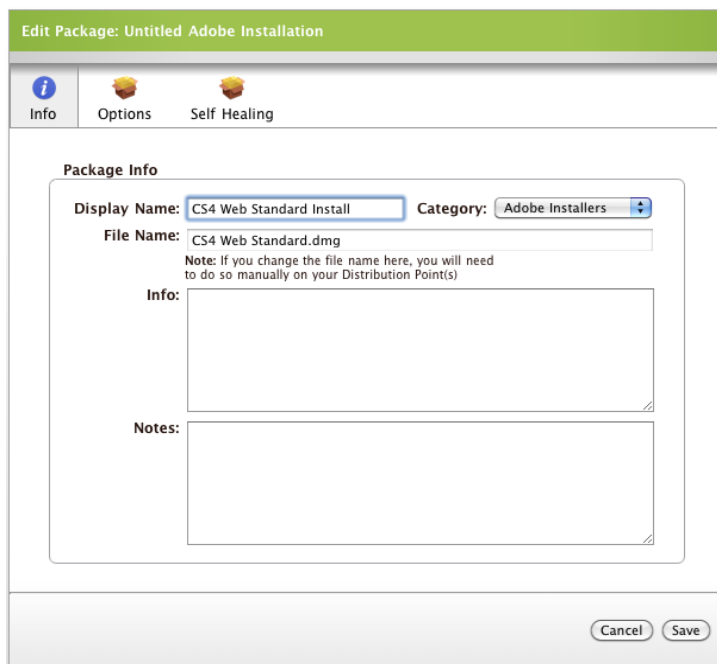


### Step 3: Create a New Adobe Installation Using the JSS

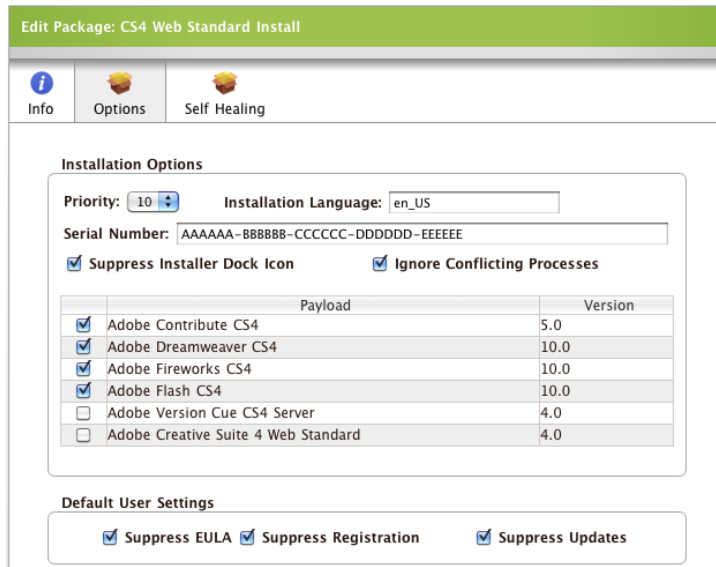
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Adobe Install** button in the toolbar.
5. If you have more than one Adobe Installer Image, choose the image on which you want to base your installation from the **Installer Image** pop-up menu.



6. Click **Save**.
7. Enter a display name for the installation on the Info pane.



- Click the **Options** tab and set the installation options. For more information about these options, see the “Options for an Adobe Install” section.



- Click **Save**.

## Options for Adobe Installations

The Options pane allows you to specify the following information for an Adobe installation:

### Priority

Setting the priority determines the order in which packages are installed.

### Serial Number

Providing this information identifies the serial number of products you are installing.

### Suppress Installer Dock Button

An Adobe Installer icon will appear in the Dock of any logged-in user even if the installer is deployed in “silent” mode. Selecting this option ensures that the icon does not appear in the Dock.

### Ignore Conflicting Processes

An Adobe Installer will fail if conflicting processes are found. Common conflicts include Safari, Firefox, and Microsoft Office applications. Selecting this option prompts the installer to ignore these conflicts.

As a result, any plug-ins installed for applications that are running during the installation will not be available until the applications are re-opened.

### List of Available Payloads

This provides a list of payloads available in the Adobe Installer Image.

You can use a single Adobe Installer Image to create multiple distributions of Adobe products that may contain different sets of the payloads.

### Suppress EULA

Ensures that users are not prompted with an End User License Agreement (EULA) when opening Adobe products.

### Suppress Registration

Ensures that users are not prompted to register Adobe products.

### Suppress Updates

Ensures that users are not prompted with available Adobe updates when using Adobe applications.

### Stage

You can set limitations on the use or deployment of a package by choosing one of the following options from the **Stage** pop-up menu:

- **Testing**—The package can only be deployed using Casper Remote (not a policy) and can only be pushed to five computers at a time.
- **Non-Deployable**—The package cannot be deployed. This setting is useful if the package needs to be taken out of production temporarily for licensing or other reasons.
- **Deleted**—This setting indicated that the package has been deleted in Casper Admin.

### Allow Uninstall

If you want the ability to uninstall the contents of your Adobe installation, select this option to make the Uninstall feature available when using Casper Remote or a policy.

The Adobe Silent Installer is used to uninstall software. Uninstalling software with this program generally takes more time than uninstalling normal PKG or DMG packages.

## Adding DMGs of Adobe Updaters

Most Adobe updates available for download on the Adobe support website are already in DMG format.

Updaters that support silent installation can be installed without repackaging. If you add the DMG to Casper Admin and it is not recognized as an Adobe Updater, it is possible that the updater does not support silent installation.

### To add an Adobe Updater DMG:

1. Open Casper Admin.
2. Drag the DMG of the Adobe Updater into Casper Admin.
3. This copies the DMG directly to the master distribution point.
4. After Casper Admin copies the DMG, the Info pane is displayed. If it does not appear, click the **Info** button in the toolbar.
5. Click the **Info** tab, and select the **This file is a disk image containing an installer (Mac OS X or an Adobe Installer/Updater)** option.

It can take Casper Admin up to 30 seconds to analyze the contents of the DMG. When this process is complete, the Options pane appears and a list of payloads available with the updater is displayed.

## Adding DMGs of Mac OS X Installer DVDs

Installing your operating system using a DMG of the Mac OS X Installer DVD ensures that client computers receive a clean operating system without requiring you to build a separate OS package.

You create a Mac OS X installation by adding a DMG of the Mac OS X Installer DVD to Casper Admin and identifying it as a Mac OS X Installer Image.

If you download installer media directly from Apple, it is already in DMG format. If you have installer media on DVD, you must first create the DMG using Disk Utility.

You can use a single image to create multiple installations, each with custom software and language settings.

Creating a Mac OS X installation involves the following steps:

1. Create the DMG.
2. Add the Mac OS X Installer DVD.
3. Customize a Mac OS X installation using Casper Admin or the JSS.

### Step 1: Create the DMG

1. Insert the installer DVD into a computer with Mac OS X.
2. Open **Disk Utility** from your **Utilities** folder.
3. Click the **DVD** button in the sidebar.
4. From the menu bar, choose **File > New > New Image From <name of the DVD>**.
5. Save as a compressed DMG.

### Step 2: Add the Mac OS X Installer DMG

1. Open Casper Admin.
2. Drag the DMG of the Mac OS X Installer into Casper Admin.  
This copies the DMG directly to the master distribution point.  
After Casper Admin copies the DMG, the Info pane is displayed. If it does not appear, click the **Info** button in the toolbar.
3. Click the **Info** tab and select the **This file is a disk image containing an installer (Mac OS X or an Adobe Installer/Updater)** option.

It can take Casper Admin up to 30 seconds to analyze the contents of the DMG.

When this process is complete, choose a default language for the installation from the **Language** pop-up menu.

**Note:** The initial Mac OS X Installer image cannot be customized beyond the language. For more information on customizing the installation, see the step entitled “Customize a Mac OS X Installation Using Casper Admin/the JSS”.

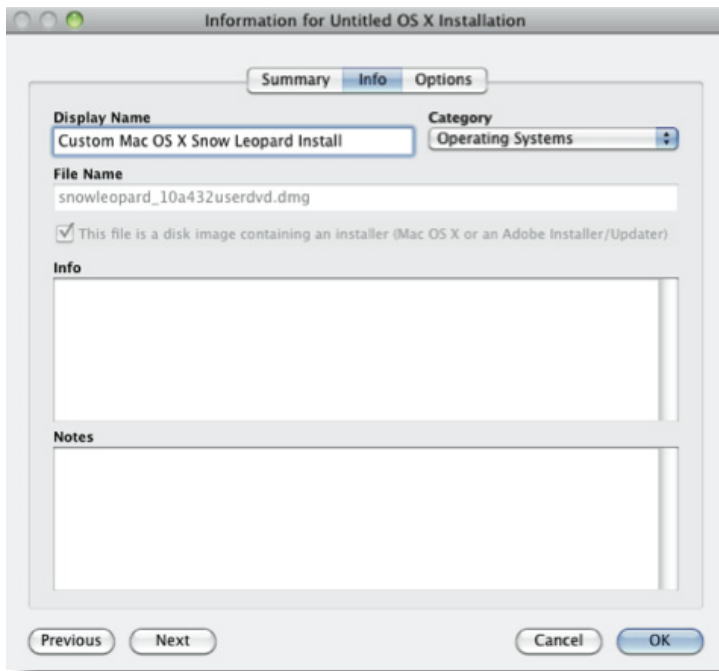


4. Click **OK**.

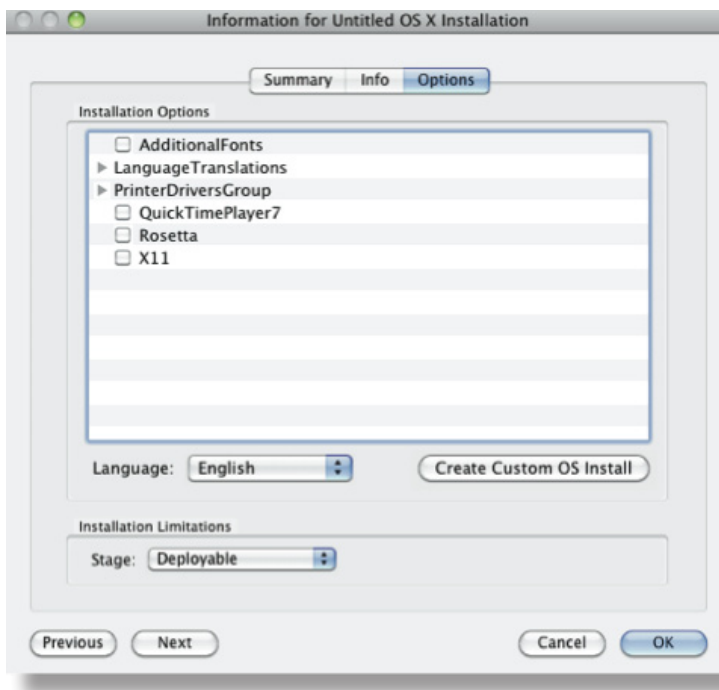
### **Step 3: Customize a Mac OS X Installation Using Casper Admin**

1. Open Casper Admin.
2. Select the Mac OS X installation on which you want to base your new installation.
3. Click the **Info** button in the toolbar.
4. Click the **Options** tab and click the **Create Custom OS Install** button.

5. Enter a display name for the installation on the Info pane.



6. Click the **Options** tab again and select the checkbox next to each package you want to install.

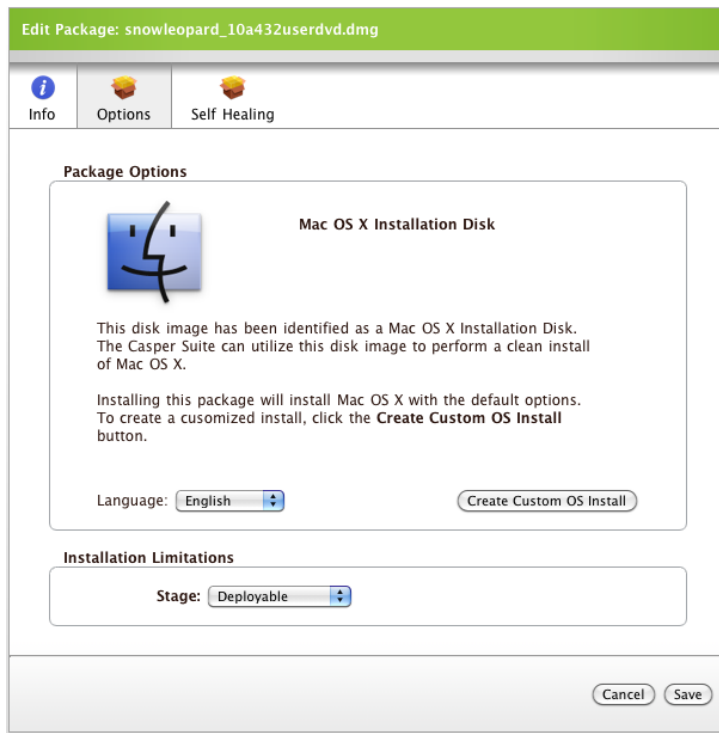


7. Click **OK**.

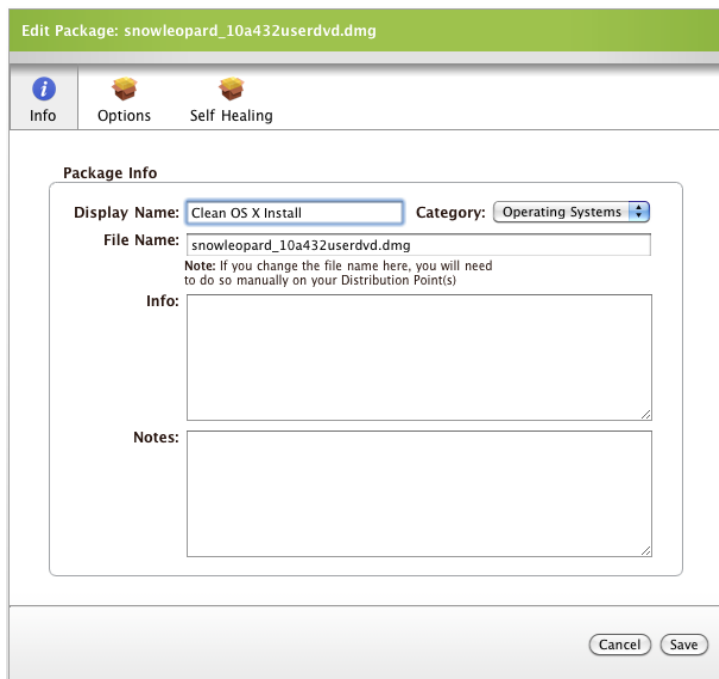
### Step 3: Customize a Mac OS X Installation Using the JSS

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.

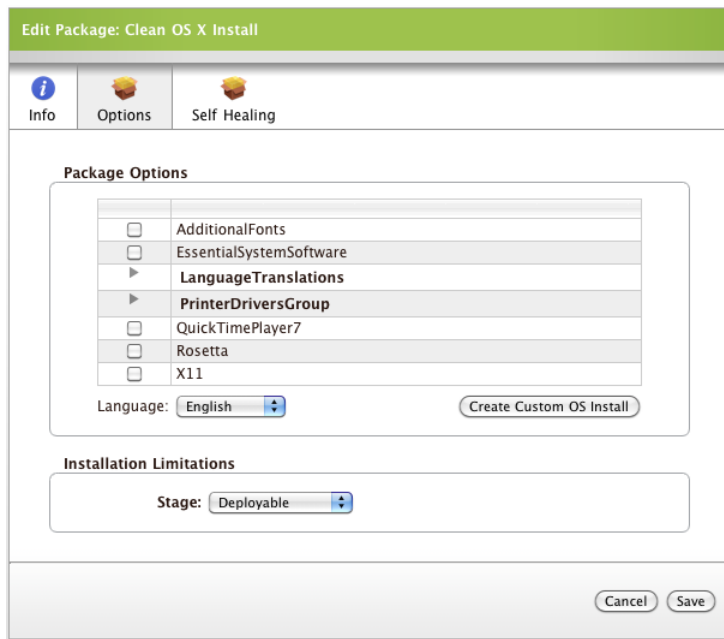
3. Click the **Casper Admin** link.
4. Click the link for the Mac OS X installation on which you want to base the new installation.
5. Click the **Options** tab and click the **Create Custom OS Install** button.



6. Enter a display name for the installation on the Info pane.



7. Click the **Options** tab and select the checkbox next to each package you want to install.



8. Click **Save**.

## Indexing Packages

Indexing creates a log of the individual files contained within a package.

Packages must be indexed before you can perform the following tasks:

- Uninstall the package using a policy or Casper Remote.
- Use the Self Healing feature.
- Search the contents of the package using the JSS.
- Create Application Difference reports.

### To index a package:

1. Open Casper Admin.
2. If prompted, authenticate to the JSS.
3. Select the package that you want to index in the Package pane, and then click the **Index** button at the bottom of the pane.
4. The username for an account on the client computer is displayed by default. Enter the corresponding password, and then click **OK**.
5. When the indexing process is complete, Casper Admin defaults back to the main window.
6. From the menu bar, choose **File > Save**.



## Enabling the Self Healing Feature

Self Healing is a maintenance feature used to ensure that the files from a package remain in their originally configured state on the client computer. For instance, if the permissions for an application installed on a client computer are changed due to an overwrite, Self Healing will detect the change and reinstall the application as originally configured.

Self Healing determines whether a maintenance action is needed by comparing the files in a package to those on the client computer. If the files on the client computer do not match those in the package, a Self Healing action is triggered.

There are two components that make up the Self Healing process:

- **Triggering files**—These are the files that you want to monitor for changes. If, at any time, the client computer does not contain matching triggering files, Self Healing will perform the specified maintenance action.
- **Self Healing actions**—There are three maintenance actions that Self Healing can perform in the event that the triggering files on the client computer do not match those in the package:
  - Reinstall the Entire Package
  - Reinstall the Triggering File
  - Send an Email Notification

This section explains how to specify these components of the Self Healing process.

**Note:** Before you enable Self Healing on a package, the package must be indexed. See the “Indexing Packages” section for details.

### To enable Self Healing:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. In the list of packages, click the link for the package on which you want to enable Self Healing.
5. Click the **Self Healing** tab and select a reinstallation option.
6. If you want an email notification to be sent each time a Self Healing event takes place, select the **Send Email Notification** option.

**Note:** The JSS sends emails to JSS users that have Self Healing notification enabled on their account.

7. Use the **Choose Files**, **Add All Apps**, **Add All Fonts**, and **Add All Plug-ins** buttons in the **Triggering Files for Self Healing** group box to specify the files for which you want to monitor changes.

8. Use the **Compare** pop-up menu to specify the type of change that you want to monitor for each triggering file. For instance, if you select “File Exists” from the pop-up menu, Self Healing will be triggered if the triggering file does not exist on the client computer. If you select “Permissions” from the pop-up menu, Self Healing will be triggered if the permissions for the file on the client computer do not match those in the package.
9. Click **Save**.

## Deleting Packages

If you no longer need a package, you can delete it using Casper Admin or the JSS.

When you delete a package, it is moved from the Packages folder to the Deleted Packages folder that is located in the Casper Data folder. To permanently delete the package, empty the trash after the package has been deleted.

After a package is deleted, change the stage to “Deleted” so it cannot be used.

This section explains how to:

- Delete a package using Casper Admin or the JSS
- Empty the trash using Casper Admin or the JSS

### To delete a package using Casper Admin:

1. Open Casper Admin, and make sure the **Repository** list is highlighted in the sidebar.
2. Select the packages that you want to delete.
3. Click the **Delete** button in the toolbar.
4. Click **OK** to confirm the deletion.

### To delete a package using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click **Casper Admin** link.
4. In the list of packages, click the link for package that you want to delete.
5. Click the **Options** tab and choose “Deleted” from the **Stage** pop-up menu.
6. Click **Save**.

### To empty the trash using Casper Admin:

1. Open Casper Admin.
2. Click the **Empty Trash** button in the toolbar.

3. Click **OK** to confirm the deletion.

**To empty the trash using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **Deleted Items** button in the toolbar and click **Empty Trash**.

# Managing Scripts

This section explains how to:

- Add new scripts
- Change script attributes
- Delete scripts

## Adding New Scripts

Before you deploy a script, you must add it to the JAMF Software Server (JSS) using Casper Admin and assign it to one or more distribution points.

There are two ways to add a new script to Casper Admin:

- Drag the script into Casper Admin.
- Copy the script directly to a distribution point.

### Dragging Scripts into Casper Admin

When you drag a script into Casper Admin, it is copied to the master distribution point and displayed in blue text in the **Unknown** category until you assign it to a software category.

**To add a script using Casper Admin:**

1. Open Casper Admin and authenticate to the JSS.
2. Drag the script from the Finder into the Package pane in Casper Admin.

### Copying Scripts Directly to the Distribution Point

This method copies the script to the Scripts folder at the root of the file share. You can enter information about the script into the JSS manually.

If you open Casper Admin after adding the script, the name of the script is displayed in blue text in the **Unknown** category in the sidebar.

**To add a script manually:**

1. Add the script to the Scripts folder on your distribution point.
2. Log in to the JSS with a web browser.
3. Click the **Settings** tab.
4. Click the **Casper Admin** link.

5. Click the **New Script** button and enter information about the script on the Info pane.

**Note:** The information entered in the **File Name** field must match the name of the file exactly.

6. Click **Save**.

## Changing Script Attributes

You can change the attributes that determine how a script is executed.

This section explains:

- How to change script attributes using either Casper Admin or the JSS
- The attributes listed on the Summary, Info, and Options panes

### To change script attributes using Casper Admin:

1. Open Casper Admin.
2. Select the script that you want to change.
3. Click the **Info** button in the toolbar.
4. Make changes to the information on the Info and Options panes, and then click **OK**.

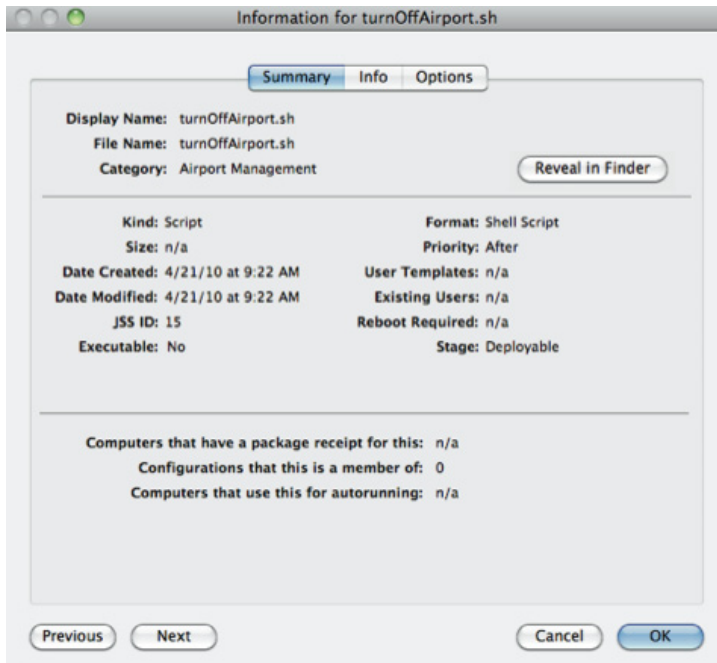
### To change script attributes using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link and click the name of the script.
4. Make changes on the Info and Options panes, and then click **Save**.

## Summary Pane

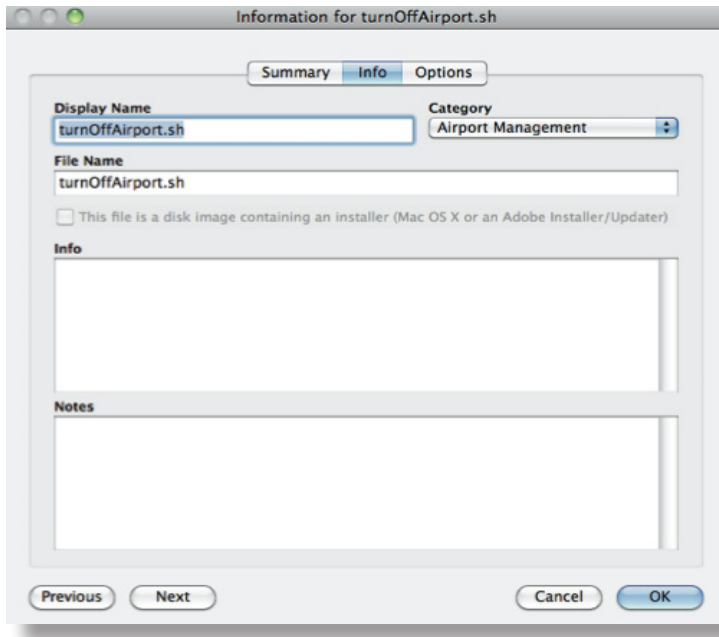
This pane displays an overview of the script. The button **Reveal in Finder** button displays the script in a Finder window.

**Note:** The Summary pane exists in the Casper Admin application only. It is not included in the web version of Casper Admin.



## Info Pane

This pane allows you to modify basic information about a script.



The following attributes are displayed on this pane:

### Display Name

This is the customizable name that identifies a script when it is displayed in a list of scripts or policies. The display name does not have to match the name of the script file.

### File Name

This is the name of the script file. If you change a filename using the web version of Casper Admin, you must manually update the filename on each distribution point. If you change a filename using the Casper Admin application, this information is automatically updated for you.

### Category

This identifies the organizational category to which a script belongs.

### Info

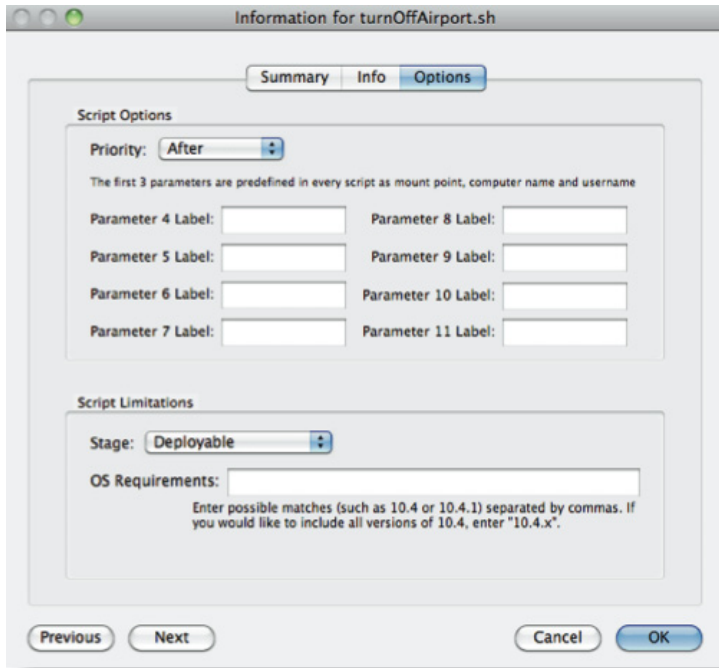
The information displayed to the administrator when a script is being deployed.

### Notes

Notes are only displayed in Casper Admin. They are helpful when tracking information about a script, such as who created it and when it was created.

## Options Pane

This pane allows you to specify deployment information and limit the operating systems on which a script can be run.



The following attributes are displayed on this pane:

### Priority

This determines the order in which scripts will run. For example, you can choose whether a script should run before the imaging process, after the imaging process, or the first time the computer boots after imaging.

### Parameter Labels

Three parameters are predefined for every script by default, but you can assign up to eight additional parameters.

You can enter names for these additional parameters in the Parameter Labels fields. If you do not enter a name, the script will be displayed as “Parameter x” in deployment interfaces.

### Stage

You can limit how a script is used and deployed by choosing one of the following options from the **Stage** pop-up menu:

- **Testing**—The script can only be deployed using Casper Remote (not a policy), and can only be pushed to five client computers at a time.
- **Non-Deployable**—The script cannot be deployed. This setting is useful if the script needs to be taken out of production temporarily.
- **Deleted**—The script has been deleted from Casper Admin.



## OS Requirements

If certain operating system requirements are needed to run a script, enter the requirements in this field using the same guidelines that you would use for a package (see the “Managing Packages” section).

## Deleting Scripts

If you no longer need a script, you can delete it using Casper Admin or the JSS.

When you delete a script, the script file is moved from the Scripts folder to the Deleted Scripts folder that is located in the Casper Data folder. To permanently delete a script, empty the trash after the script has been deleted.

After a script is deleted, change the stage to “Deleted” so it can’t be used.

This section explains how to:

- Delete a script using Casper Admin or the JSS
- Empty the trash using Casper Admin or the JSS

### To delete a script using Casper Admin:

1. Open Casper Admin, and make sure the **Repository** list is highlighted in the sidebar.
2. Select the scripts that you want to delete.
3. Click the **Delete** button in the toolbar.
4. Click **OK** to confirm the deletion.

### To delete a script using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click **Casper Admin** link.
4. In the list of scripts, click the link for the script that you want to delete.
5. Click the **Options** tab and choose **Deleted** from the **Stage** pop-up menu.
6. Click **Save**.

### To empty the trash using Casper Admin:

1. Open Casper Admin.
2. Click the **Empty Trash** button in the toolbar.
3. Click **OK** to confirm the deletion.

**To empty the trash using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **Deleted Items** button in the toolbar and click **Empty Trash**.

# Managing Printers

This section explains how to:

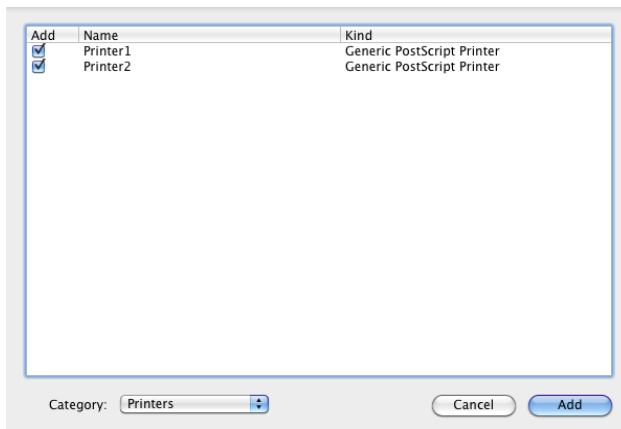
- Add new printers
- Change printer attributes
- Delete printers

## Adding New Printers

Before you deploy a printer, you must add it to the JAMF Software Server (JSS) using Casper Admin as a deployable object.

To add a printer using Casper Admin:

1. Open Casper Admin and authenticate to the JSS.
2. Click the **Add Printers** button in the toolbar.
3. Authenticate locally if prompted.
4. Select the checkbox next to each printer you want to add.
5. Using the **Category** pop-up menu, choose the category to which the printers should be added, and then click the **Add** button.



## Changing Printer Attributes

Printers, like packages and scripts, have attributes that determine how they are organized and deployed.

This section explains:

- How to change printer attributes using Casper Admin or the JSS
- The attributes listed on the Summary, Info, and Options panes

### To change printer attributes using Casper Admin:

1. Open Casper Admin.
2. Select the printer.
3. Click the **Info** button in the toolbar.
4. Make changes to the information on the Info and Options panes, and then click **OK**.

### To change printer attributes using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link and click the printer name.
4. Make changes on the Info and Options panes, and then click **Save**.

## Summary Pane

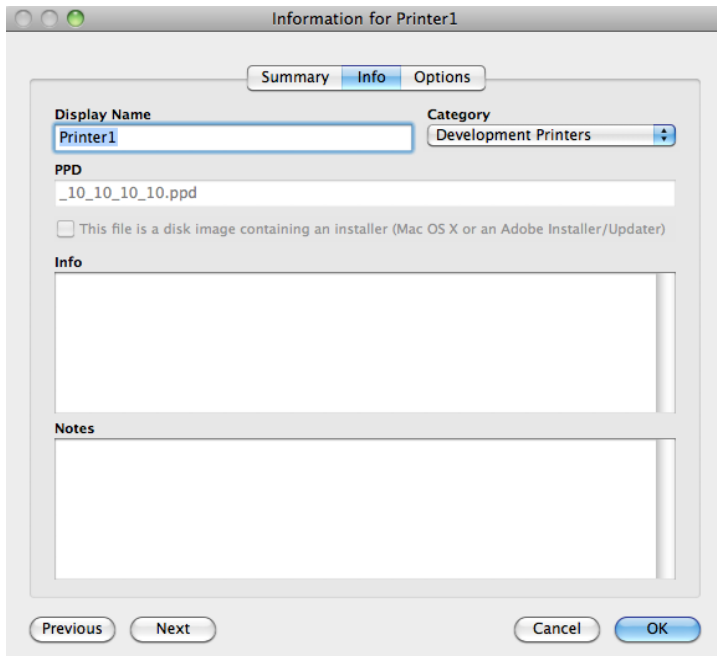
This pane displays an overview of the printer.

**Note:** The Summary pane exists in the Casper Admin application only. It is not included in the web version of Casper Admin.



## Info Pane

This pane allows you to modify basic information about a printer.



The following attributes are displayed on this pane:

### Display Name

This is the customizable name that identifies a printer when it is displayed in Casper Imaging, Casper Remote, or policies.

This name can differ from the Postscript Printer Description file (PPD).

### File Name

This is the name of the Postscript Printer Description file (PPD).

### Category

This identifies the organizational category to which a printer belongs.

### Info

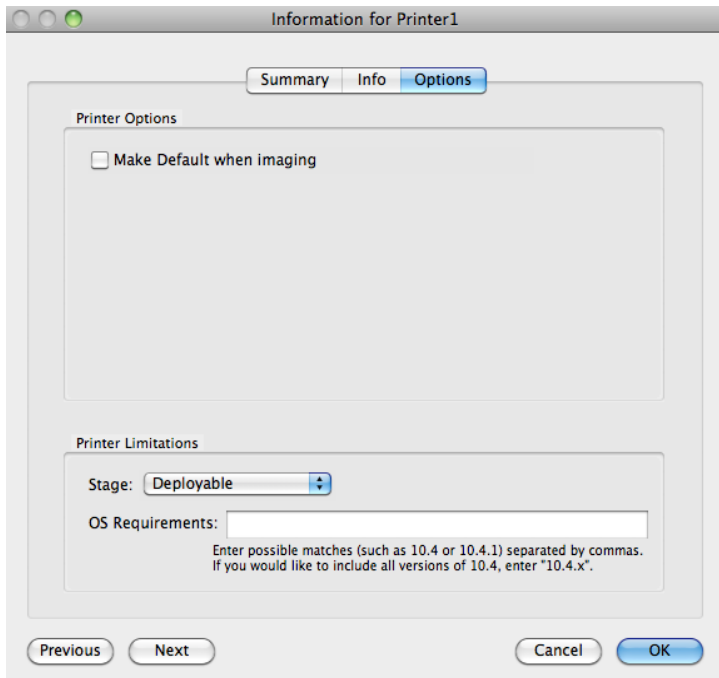
The information displayed to the administrator when a printer is being deployed.

### Notes

Notes are only displayed in Casper Admin. They are helpful when tracking information about a printer or package, such as who created it and when it was built.

## Options Pane

This pane allows you to specify deployment information and limit the operating systems to which a printer can be mapped.



The following attributes are displayed on this pane:

### Stage

You can limit how a printer is used and deployed by choosing one of the following options from the **Stage** pop-up menu:

- **Non-Deployable**—The printer cannot be deployed. This setting is useful if the package needs to be taken out of production temporarily for licensing or other reasons.
- **Deleted**—The printer has been deleted from Casper Admin.

## Deleting Printers

If you no longer need a printer, you can delete it using Casper Admin.

After a printer is deleted, change the stage to “Deleted” so it cannot be used.

This section explains how to:

- Delete a printer using Casper Admin or the JSS
- Empty the trash using Casper Admin or the JSS

### To delete a printer using Casper Admin:

1. Open Casper Admin and make sure the **Repository** list is highlighted in the sidebar.

2. Select the printers that you want to delete.
3. Click the **Delete** button in the toolbar.
4. Click **OK** to confirm the deletion.

**To delete a printer using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. In the list of printers, click the link for the printer that you want to delete.
5. Click the **Options** tab and choose "Deleted" from the **Stage** pop-up menu.
6. Click **Save**.

**To empty the trash using Casper Admin:**

1. Open Casper Admin.
2. Click the **Empty Trash** button in the toolbar.
3. Click **OK** to confirm the deletion.

**To empty the trash using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **Deleted Items** button in the toolbar and click **Empty Trash**.

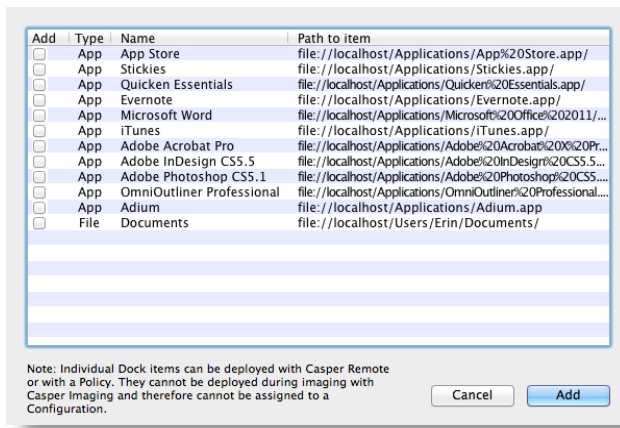
# Managing Dock Items

## Adding Dock Items

Before you deploy a Dock item, you must add it to the JAMF Software Server (JSS) using Casper Admin as a deployable object.

To add a Dock item:

1. Open Casper Admin.
2. Click the **Add Dock Items** button in the toolbar.
3. Select the checkbox next to each item you want to add, and then click the **Add** button.



## Deleting Dock Items

If you are no longer using a Dock item, you can delete it using Casper Admin.

To delete a Dock item:

1. Open Casper Admin, and make sure the **Repository** list is highlighted in the sidebar.
2. Select the items you want to delete.
3. Click the **Delete** button in the toolbar.
4. Click **OK** to confirm the deletion.



# Creating Directory Bindings

Directory bindings bind client computers to directory services. You can create the following directory bindings:

- Active Directory (using Apple's built-in tools)
- Open Directory (using Apple's built-in tools)
- Active Directory using Likewise
- Active Directory using ADmitMac
- Active Directory using Centrify

This section explains how to create each directory binding in the JAMF Software Server (JSS).

## To create an Active Directory binding:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Directory Binding** button in the toolbar.
5. Select the **Active Directory Binding (built into Mac OS X)** option and click the **Continue** button.
6. Enter a display name for the binding.  
This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the Active Directory domain.
8. Enter the username and password for an Active Directory account that has permissions to add computers, and enter the password again to verify it.
9. In the **Computer OU** field, enter the OU in which the computer object should be placed.

The screenshot shows a web-based form titled "Edit Directory Binding: New AD Binding". The form is organized into a header with a green bar, a navigation bar with four tabs (General, User Experience, AD Mappings, Administrative), and a main content area. The "General" tab is selected. The form contains the following fields and values:

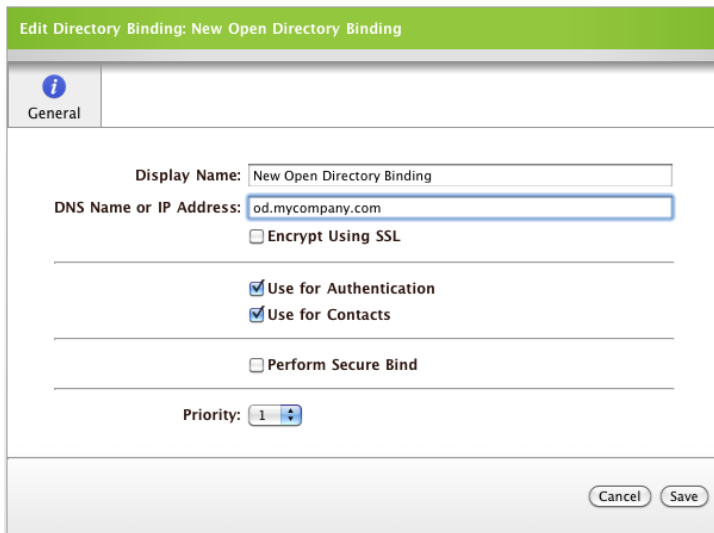
- Display Name: New AD Binding
- Active Directory Domain: ad.mycompany.corp
- Network Admin Username: Service
- Password: [masked]
- Verify Password: [masked]
- Computer OU: CN=computers,DC=domain,DC=company,DC=com
- Priority: 1

At the bottom right of the form, there are "Cancel" and "Save" buttons.

10. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings should be applied.
11. Enter any additional information on the User Experience, AD Mappings, and Administrative panes. The information specified on these panes is the same information entered when using Apple's Directory Utility application.
12. Click **Save**.

**To create an Open Directory binding:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Directory Binding** button in the toolbar.
5. Select the **Open Directory Binding (built into Mac OS X)** option and click the **Continue** button.
6. Enter a display name for the binding.  
This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the DNS name or IP address for the server hosting the Open Directory service.
8. If you use SSL to bind to the Open Directory service, select the **Encrypt Using SSL** checkbox.



9. If you want to allow users from Open Directory to log in to other bound clients, select the **Use For Authentication** option.
10. If you want users from Open Directory to be listed as contacts on other client computers, select the **Use For Contacts** option.
11. If you want to bind to Open Directory securely, select the **Perform Secure Bind** checkbox and enter the username and password for the directory account.

12. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings should be applied.
13. Click **Save**.

#### To create a Likewise Active Directory binding:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Directory Bindings** button in the toolbar.
5. Select the **Likewise Binding** option and click the **Continue** button.
6. Enter a display name for the binding.  
This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the domain to which you are binding.
8. Enter the username and password for an administrator account and enter the password again to verify it.
9. In the **Computer OU** field, enter the OU in which the computer object should be placed.

Dialog box titled "Edit Directory Binding: New Likewise Directory Binding". The "General" tab is selected. Fields include: Display Name: New Likewise Directory Binding; Domain: ad.mycompany.corp; Network Admin Username: Service; Password: masked; Verify Password: masked; Computer OU: CN=computers,DC=domain,DC=company,DC=com; Priority: 1. Buttons: Cancel, Save.

10. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings will be applied.
11. Click **Save**.

#### To create an ADmitMac Active Directory binding:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.

4. Click the **New Directory Bindings** button in the toolbar.
5. Select the **ADmitMAC Binding** option and click the **Continue** button.
6. Enter a display name for the binding.  
This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the DNS name or IP address for the server to which you are binding.
8. Enter the username and password for an administrator account and enter the password again to verify it.
9. In the **Computer OU** field, enter the OU in which the computer object should be placed.

10. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings will be applied.
11. Enter any additional information on the Home Folders, Login Policy, Admin, OUs, and Mappings panes.  
The information specified on these panes is the same information entered when using Thursby's ADmitMac interface.
12. Click **Save**.

**To create a Centrify Active Directory binding:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Directory Bindings** button in the toolbar.
5. Select the **Centrify Binding** option and click the **Continue** button.
6. Enter a display name for the binding.  
This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the domain to which you are binding.

8. Enter the username and password for an administrator account and enter the password again to verify it.
9. In the **Container DN** field, enter the DN in which the client computers should be placed.

Dialog box titled "Edit Directory Binding: New Centrify Directory Binding".

General | Centrify Options

Display Name: New Centrify Directory Binding

Domain: ad.mycompany.corp

Network Admin Username: Service

Password: .....

Verify Password: .....

Container DN: CN=computers,DC=domain,DC=company,DC=com

Priority: 1

Buttons: Cancel, Save

10. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings will be applied.
11. Enter any additional information on the Centrify Options pane.  
The information specified on this pane is the same information entered when using the Centrify interface.
12. Click **Save**.

# Creating Disk Encryption Configurations

The JSS allows you to create disk encryption configurations that you can deploy to activate FileVault 2 on OS X v10.8 computers.

Creating a disk encryption configuration requires a JSS user account with the "Manage Disk Encryption" privilege enabled. If you plan to use an institutional recovery key, you need the "Manage Disk Encryption Institutional Key" privilege enabled as well.

Disk encryption configurations allow you to set the following information:

- The type of recovery key to use for encrypted drives
- The user that will be the enabled FileVault 2 user

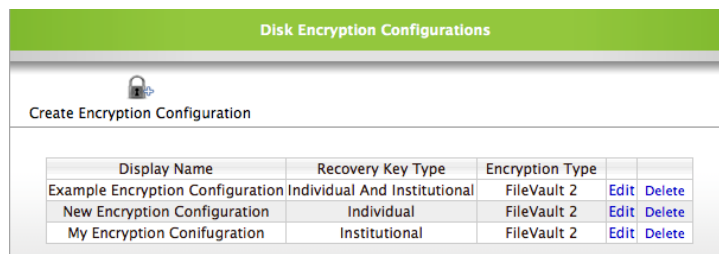
**Note:** A complete workflow for administering FileVault 2 on OS X v10.8 computers is provided in the "Administering FileVault 2 on OS X Mountain Lion with the Casper Suite" technical paper. You can download this technical paper from:

[http://www.jamfsoftware.com/libraries/pdf/white\\_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf](http://www.jamfsoftware.com/libraries/pdf/white_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf)

This section explains how to create, edit, and delete a disk encryption configuration.

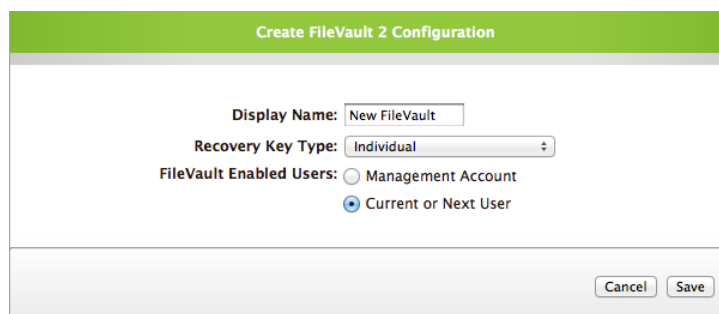
**To create a disk encryption configuration:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Disk Encryption Configurations** link.
4. Click the **Create Encryption Configuration** button.



Display Name	Recovery Key Type	Encryption Type		
Example Encryption Configuration Individual And Institutional	Individual And Institutional	FileVault 2	Edit	Delete
New Encryption Configuration	Individual	FileVault 2	Edit	Delete
My Encryption Conifugration	Institutional	FileVault 2	Edit	Delete

5. Enter a name for the disk encryption configuration in the **Display Name** field.



Display Name:

Recovery Key Type:

FileVault Enabled Users:  Management Account  Current or Next User

6. Choose a type of recovery key type option from the **Recovery Key Type** pop-up menu:
  - **Individual**—Uses a unique recovery key for each client computer.
  - **Institutional**—Uses a single recovery key that is shared by client computers.
  - **Individual and Institutional**—Uses a unique recovery key and a shared recovery key for each client computer.

Individual recovery keys are created and stored in the JSS when the encryption takes place. Institutional recovery keys must be created with Keychain Access, and then uploaded to the JSS for storage.

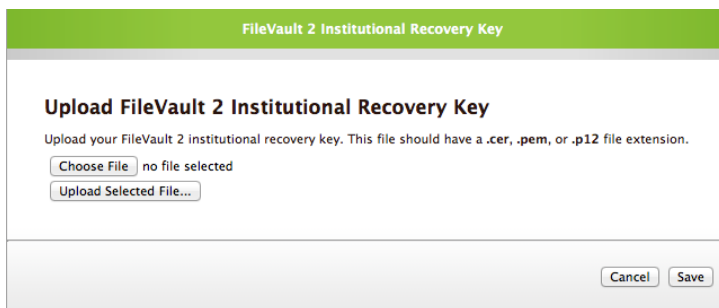
If you plan to use an institutional recovery key type or an individual and institutional recovery key type, you must first create the institutional recovery key using Keychain Access. For instructions, see "Creating and Exporting an Institutional Recovery Key" in the "Administering FileVault 2 on OS X Mountain Lion with the Casper Suite" technical paper, available at:

[http://www.jamfsoftware.com/libraries/pdf/white\\_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf](http://www.jamfsoftware.com/libraries/pdf/white_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf)

7. If you choose to use an institutional recovery key type or an individual and institutional recovery key type, upload the recovery key file to the JSS:
  - a. Click the **Upload** button.
  - b. Click the **Choose File** button and select the recovery key file.

The recovery key file must be a .p12, .cer, or .pem file.
  - c. Click the **Upload Selected File** button.

If you are uploading a .p12 file, you are prompted to enter your password. Enter the password that you created when you exported the recovery key from Keychain Access.
  - d. Click the **Save** button.



8. Choose the user that you want to be the enabled FileVault 2 user.
  - **Management Account**—Makes the management account on the computer the enabled FileVault 2 user.
  - **Current or Next User**—Makes the user that is logged into the computer when the encryption takes place the enabled FileVault 2 user. If no user is logged in, the next user to log in becomes the enabled FileVault 2 user.
9. Click the **Save** button.

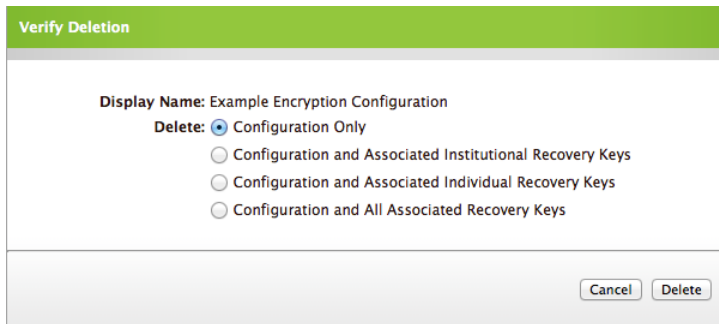
#### To edit a disk encryption configuration:

1. Log in to the JSS with a web browser.

2. Click the **Management** tab.
3. Click the **Disk Encryption Configurations** link.
4. Click the **Edit** link across from the disk encryption configuration you want to edit.
5. Make changes as needed, and then click the **Save** button.

**To delete a disk encryption configuration:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Disk Encryption Configurations** link.
4. Click the **Delete** link across from the disk encryption configuration you want to delete.
5. Choose a deletion option, and then click the **Delete** button.



The image shows a 'Verify Deletion' dialog box with a green header. The dialog contains the following text and options:

**Display Name:** Example Encryption Configuration  
**Delete:**  Configuration Only  
 Configuration and Associated Institutional Recovery Keys  
 Configuration and Associated Individual Recovery Keys  
 Configuration and All Associated Recovery Keys

At the bottom right of the dialog are two buttons: 'Cancel' and 'Delete'.



# Configuring the Computer Management Framework

Use the Global and Computer Management Framework settings to control how the JAMF Software Server (JSS) and the other applications in the Casper Suite interact with client computers.

## Global Management Framework Settings

The Global Management Framework settings allow you to configure and manage the following security components for the JSS:

- JSS URL
- Public key infrastructure (PKI)
- Apple Push Notification service (APNs) certificate

### JSS URL

The JSS URL is the URL that client computers connect to when communicating with the JSS. The full URL of the JSS must be entered on this pane, including the correct protocol, domain, and port. For example:

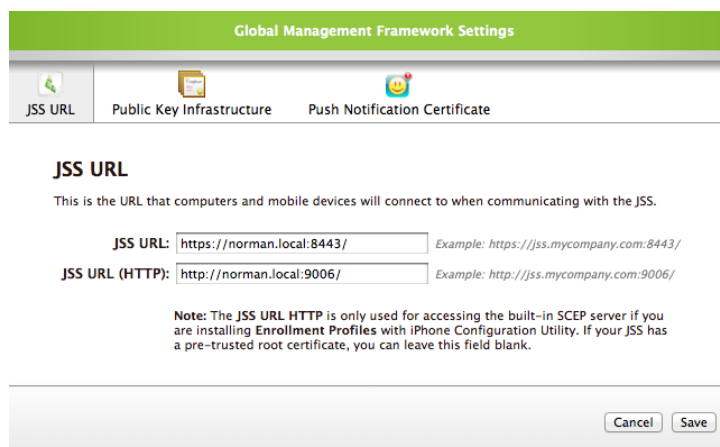
`https://jss.mycompany.com:8443/`

If this field is blank or the URL is incorrect, client computers are unable to connect to the server.

#### To view the JSS URL:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.
4. Click the **JSS URL** tab.

The URL of the JSS is entered in the **JSS URL** field.



The screenshot shows a dialog box titled "Global Management Framework Settings". It has three tabs: "JSS URL", "Public Key Infrastructure", and "Push Notification Certificate". The "JSS URL" tab is selected. Below the tabs, the text reads: "JSS URL. This is the URL that computers and mobile devices will connect to when communicating with the JSS." There are two input fields. The first is labeled "JSS URL:" and contains the text "https://norman.local:8443/". To its right is an example: "Example: https://jss.mycompany.com:8443/". The second is labeled "JSS URL (HTTP):" and contains "http://norman.local:9006/". To its right is an example: "Example: http://jss.mycompany.com:9006/". Below the input fields is a note: "Note: The JSS URL HTTP is only used for accessing the built-in SCEP server if you are installing Enrollment Profiles with iPhone Configuration Utility. If your JSS has a pre-trusted root certificate, you can leave this field blank." At the bottom right of the dialog are "Cancel" and "Save" buttons.

5. Click **Save**.

## Public Key Infrastructure

To ensure the security of over-the-air tasks, the JSS requires a PKI that supports certificate-based authentication. This includes:

- A certificate authority (CA) with Simple Certificate Enrollment Protocol (SCEP) capabilities
- A signing certificate
- A CA certificate

If you do not have access to an external CA with SCEP capabilities, you can use the built-in CA that is enabled by default in the JSS. The built-in CA has the signing and CA certificates uploaded for you.

If your organization uses an external CA with SCEP capabilities, you can integrate it with the JSS using one of the following methods:

- **Create a signing certificate and upload a CA certificate**  
This method allows you to use the JSS to generate a certificate signing request (CSR) that you will use to obtain the signing certificate. After you obtain the signing certificate from the CA, upload it and the CA certificate to the JSS to complete the integration.
- **Upload a signing certificate keystore and a CA certificate**  
This method allows you to include a certificate chain for the signing certificate. To do this, you must upload a signing certificate keystore (.jks or .p12 file) that includes a private key and its associated certificate or certificate chain. Once you've selected the certificate to use as your signing certificate, you can upload a CA certificate or CA certificate bundle to complete the integration.

### To integrate an external CA with the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.
4. Click the **Public Key Infrastructure** tab.

5. Select **Use External Certificate Authority** and specify information about the CA and the SCEP server. Be sure to choose the type of challenge password that will be used as the pre-shared secret for enrollment.
  - If you want computers and devices to use the same challenge password, select the **Static** option.
  - If you have a non-Microsoft CA and want computers and devices to use unique challenge passwords, select the **Dynamic** option.

The **Dynamic** option requires use of the JSS API and membership in the JAMF Software Developer Program. Before selecting this option, contact your Account Manager to learn more about the JAMF Software Developer Program and the additional steps you need to take to use this option.

- If you have a Microsoft CA and want computers and devices to use unique challenge passwords, select the **Dynamic-Microsoft CA** option.

**Note:** If you want mobile devices to use unique challenge passwords, you must enroll them over-the-air (OTA). For more information on OTA enrollment, see "Enrolling Mobile Devices OTA".

The screenshot shows the 'Global Management Framework Settings' dialog box with the 'Public Key Infrastructure' tab selected. The 'Use External Certificate Authority' radio button is selected. The form contains the following fields and options:

- Base URL for the SCEP Server:** [required] (text input)
- The name of the instance: CA-IDENT:** [optional] (text input)
- Subject (Representation of a X.500 name):** [optional] (text input)
- Subject Alternative Name Type:** None (dropdown menu)
- Challenge Type:** Static (selected), Dynamic, Dynamic-Microsoft CA
- Challenge:** [masked text input]
- Verify Challenge:** [masked text input]
- Key Size in bits:** 1024 (dropdown menu)
- Use as digital signature:**
- Use for key encipherment:**
- Fingerprint hex string:** (text input)
- Signing Certificate:** Signing and CA Certificate Assistant... (link)

Buttons for 'Cancel' and 'Save' are located at the bottom right of the dialog.

6. Click the **Signing and CA Certificate Assistant** link.
7. Choose a method for providing the signing and CA certificates, and then click **Continue**.
8. Follow the onscreen instructions.
9. When you complete the assistant, click **Save**.

## Apple Push Notification Service Certificate

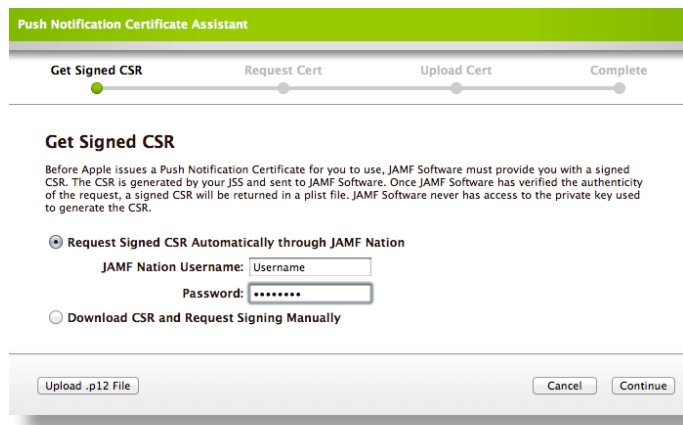
For the JSS to perform over-the-air management tasks, it must be able to communicate with Apple Push Notification service (APNs). To enable this communication, you must obtain an APNs certificate (.pem) from Apple and upload it to the JSS.

The JSS guides you through the process of generating or renewing an APNs certificate from the Apple Push Certificates Portal. This process requires:

- A valid JAMF Nation account  
To create a JAMF Nation account, go to:  
<https://jamfnation.jamfsoftware.com/createAccount.html>
- A valid Apple ID

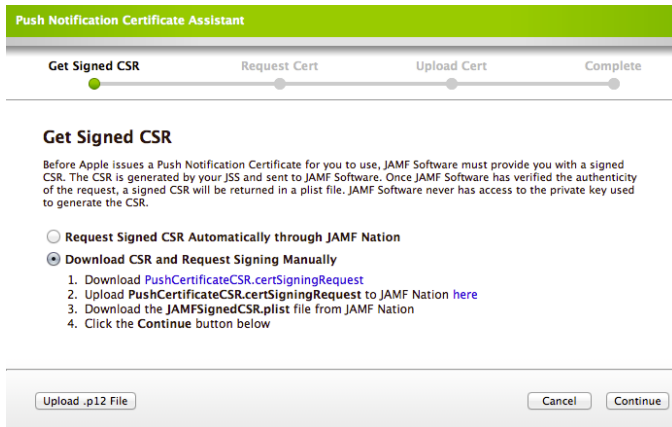
**To generate or renew an APNs certificate:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.
4. Click the **Push Notification Certificate** tab.
5. To generate an APNs certificate for the first time, click the **Create a certificate using the Push Notification Certificate Assistant** link.  
To renew your APNs certificate, click the **Renew your Push Notification Certificate** link.
6. Choose how you want to obtain the CSR.
  - If the server hosting the JSS has an outbound connection, select **Request Signed CSR Automatically through JAMF Nation**. Enter the username and password for your JAMF Nation account, and then click **Continue**.

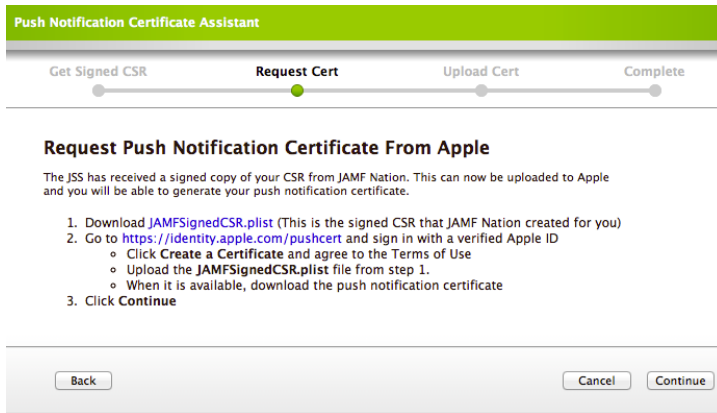


The JSS connects to JAMF Nation over port 443 and obtains the signed CSR. (You will download the CSR in the next step.)

- If the server hosting the JSS does not have an outbound connection, select **Download CSR and Request Signing Manually**. Then, follow the onscreen instructions to get the CSR signed.



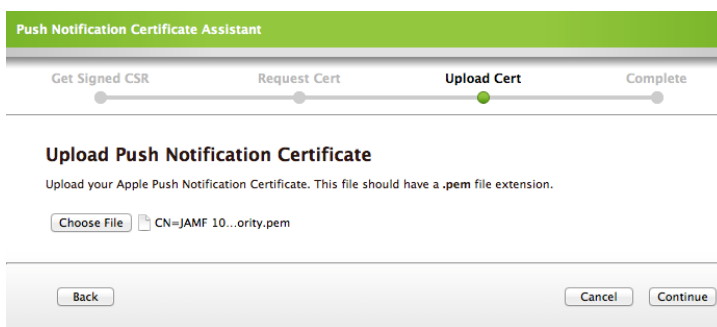
7. On the Request Cert pane, follow the onscreen instructions to request an APNs certificate from Apple.



**Note:** It is recommended that you sign in to the Apple Push Certificates Portal with a corporate Apple ID, since the account will be associated with your corporate APNs certificate.

If you are renewing an APNs certificate originally obtained from Apple's iOS Developer Enterprise Program (iDEP), you must sign in using the Apple ID for the iDEP Agent account.

8. On the Upload Cert pane, click **Choose File**. Select the APNs certificate (.pem) that you want to upload and click **Choose**. Then, click **Continue** in the JSS.



9. Click **Done** to save the certificate.

# Computer Management Framework Settings

The Computer Management Framework settings allow you to set up and manage preferences for the following aspects of client management:

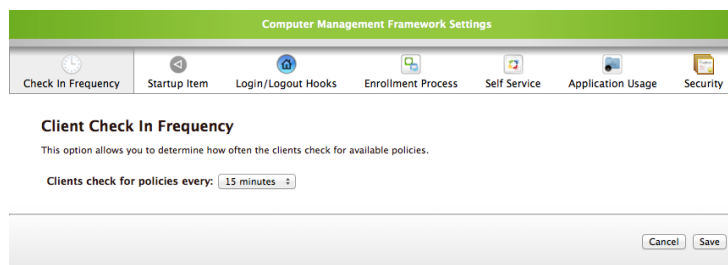
- Client check-in frequency
- Login and logout hooks
- User-initiated enrollment process
- Self Service application
- Application Usage
- Security

## Check-In Frequency

The check-in frequency allows you to control how often client computers check the JSS for available policies.

To view or modify the check-in frequency:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. On the Check-In Frequency pane, choose a check-in frequency from the pop-up menu.



5. Click **Save**.

## Startup Item

Use this pane to create or remove a startup item and set preferences for how you want to use it. The following options are displayed on this pane:

### Create startup item

Creates a launchd item that executes once at startup. The launchd item is stored in the following location:  
`/Library/LaunchDaemons/com.jamfsoftware.startupItem.plist`

### Log startup action

Logs the startup action and IP address of each client computer at reboot

### Check for policies triggered by startup

Enables computers to check the JSS for policies triggered at startup

### Apply Computer Level Enforced Managed Preferences

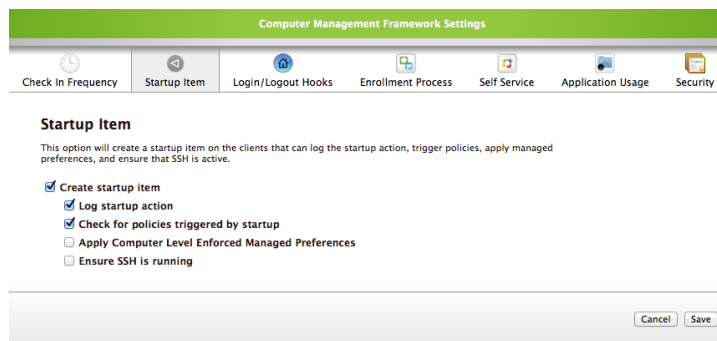
Applies computer-level Managed Preferences

### Ensure SSH is running

Ensures SSH is active at reboot using the startup script

### To set up or modify startup item preferences:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Startup Item** tab.
5. Select or deselect the **Create startup item** checkbox to create or remove the startup item.
6. Select or deselect additional options as needed.



7. Click **Save**.

## Login and Logout Hooks

Use this pane to create or remove login/logout hooks and set preferences for how you want to use them. The following options are displayed on this pane:

### Create login and logout hooks

Creates hooks that execute each time a user logs in or logs out

### Log username with login and logout

Logs usernames at login/logout and updates the IP address for the computer in the JSS

### Check for Policies with login and logout

Runs policies at login or logout that are used for tasks such as extending login/logout hooks by running custom scripts

## Apply User Level Managed Preferences

Applies user-level and user-level enforced Managed Preferences

## Hide Restore partition at login

Hides the Restore partition when a two or three-scheme partition is in use

## Perform login actions in background

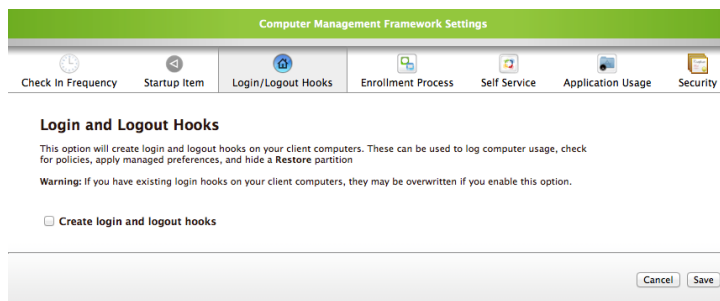
Allows large package deployments triggered at login or logout to take place without stopping the user's login process

## Display status to user during login and logout

Displays the status of non-background login/logout hook actions to users when they log in or out of a computer

To set up or modify login and logout hook preferences:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Login/Logout Hooks** tab.
5. Select or deselect the **Create login and logout hooks** checkbox to create or remove login/logout hooks.



6. Select or deselect additional options as needed.
7. Click **Save**.

## User-Initiated Enrollment Process

User-initiated enrollment allows users to enroll their computers using a QuickAdd package. Use the Enrollment Process pane to enable or disable user-initiated enrollment. When user-initiated enrollment is enabled, you can use this pane to configure the following settings for the QuickAdd package and the Login page for user-initiated enrollment:

### Management Username and Password

The credentials for the account that you want to use for management. (These fields are required.)

### Create this account if it does not exist

Create the management account that you specified if it does not already exist.



### **Hide account from OS X Login Window**

Hides the management account from users.

**Note:** This option is only displayed if the **Create account if it does not exist** checkbox is selected.

### **Configure SSH (Remote Login) to only allow access for this user**

Makes the management account the only account that has SSH access to computers.

**Note:** This option is only displayed if the **Create account if it does not exist** checkbox is selected.

### **Ensure SSH is running**

Enables SSH (remote login) on computers that have it disabled.

### **Check for policies when done**

Ensures that computers check for policies immediately after they are enrolled.

### **Launch Self Service when done**

Ensures that computers launch Self Service immediately after they are enrolled.

### **Login page title and description**

Allows you to customize the text that is displayed to users on the Login page of the user-initiated enrollment process.

### **Sign QuickAdd package**

Ensures that the QuickAdd package is signed and appears as verified to users. Enabling this option allows users to install the QuickAdd package on computers that have Apple's Gatekeeper feature set to only allow applications downloaded from the Mac App Store and identified developers.

Signing the QuickAdd package requires an installer certificate (.p12) from Apple's Developer Certificate Utility. To obtain an installer certificate from Apple's Developer Certificate Utility, you must be a registered Apple Developer in the Mac Developer Program. To enroll in the Mac Developer Program, visit the following website:

<https://developer.apple.com/programs/mac/>

### **To set up or modify User-Initiated Enrollment preferences:**

1. Log in to the JSS in a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Framework Settings** link.
4. Click the **Enrollment Process** tab.

5. Enter or modify the management account information as needed.

Computer Management Framework Settings

Check in Frequency Startup Item Login/Logout Hooks Enrollment Process Self Service Application Usage Security

### User-Initiated Enrollment Process

User-initiated enrollment allows end users to enroll their computers by navigating to <https://10.1.20.130:8443/enroll>. The settings below will determine the behavior of the QuickAdd Package your end users will download and install.

Enable User-Initiated Enrollment

**Management Account Information**

Username:

Password:

Verify Password:

Create account if it does not exist

Ensure SSH is running

Check for policies when done

Login page title:

Login page description:

Sign QuickAdd package:

Cancel Save

6. Select or deselect additional options as needed.
7. To sign the QuickAdd package, select the **Sign QuickAdd package** checkbox and upload an installer certificate (.p12) obtained from Apple's Developer Certificate Utility.
8. Customize text for the Login page as needed.  
This page is displayed to users during the user-initiated enrollment process.
9. Click **Save**.

## Self Service

The Self Service pane allows you to perform the following management tasks for Self Service:

- Automatically install Self Service on all enrolled computers.
- Configure User Authentication preferences.
- Add plug-ins.

For more information about these tasks and how to perform them, see the following sections:

- "Installing Self Service"
- "Managing User Authentication Preferences"
- "Managing Self Service Plug-ins"

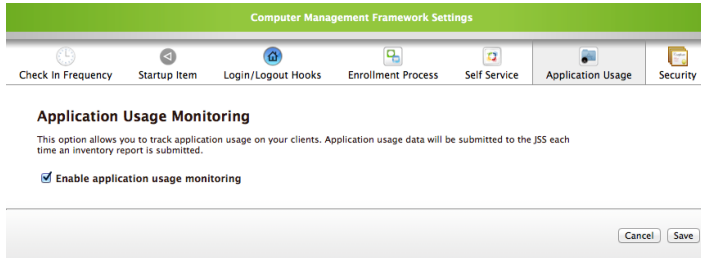
## Application Usage

Use this pane to enable application usage for client computers. For information about application usage, see the "Application Usage" section.

**To enable application usage monitoring:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.

3. Click the **Computer Management Framework Settings** link.
4. Click the **Application Usage** tab.
5. Select or deselect the **Enable application usage monitoring** checkbox to enable or disable application usage monitoring, and then click **Save**.



## Security

Use this pane to set up or modify the following security preferences for client management:

### Enable Certificate-Based Communication

Ensures that all messages from Mac OS X clients to the JSS are signed with a valid signature. The JSS rejects the message if the signature is invalid. (This option is selected by default for all fresh installs of the JSS.)

### Enable Push Notifications for OS X v10.7 or later clients

Allows clients with OS X v10.7 or later to perform secure transactions between the jamf binary and the JSS.

**Note:** This option is only displayed if certificate-based communication is enabled and an APNs certificate is uploaded to the JSS. See the “Apple Push Notification Service Certificate” section for more information.

### This JSS has a valid certificate installed

Indicates that there is a valid web server certificate installed on the server.

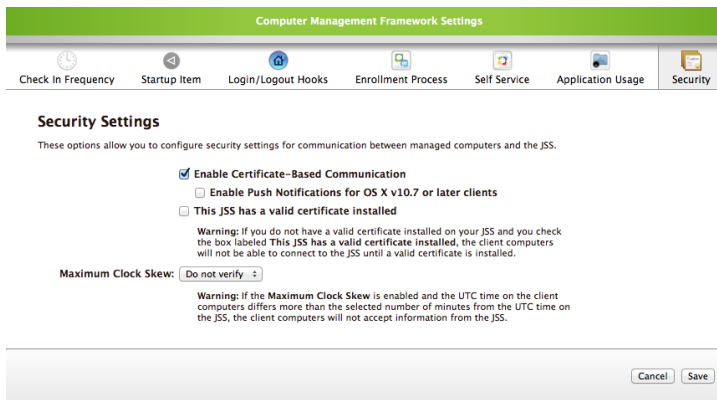
### Maximum Clock Skew

Sets a maximum difference in clock settings for the server and enrolled computers.

### To set up or modify security preferences:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Security** tab.

5. Select or deselect options as needed.



6. Set or modify a maximum clock skew by choosing an option from the **Maximum Clock Skew** pop-up menu.
7. Click **Save**.

# Managing Removable MAC Addresses

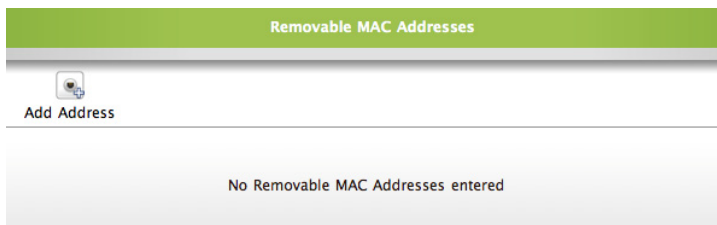
Computers are identified by their MAC addresses during the imaging process. This makes utilizing USB Ethernet dongles during imaging problematic, since the JAMF Software Server (JSS) assumes that each computer with a specific dongle is connected to the same computer.

To work around this issue, you can enter a list of MAC addresses that the JSS should ignore when identifying a computer.

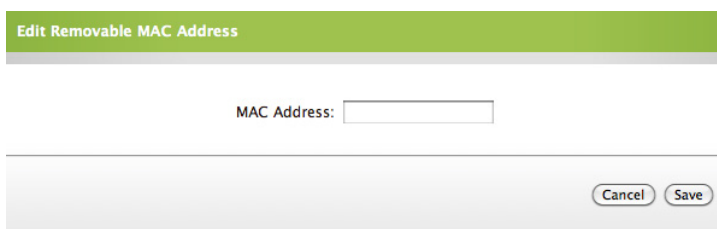
This section explains how to add, edit, and delete a removable MAC address.

## To add a removable MAC address:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Removable MAC Addresses** link.
5. Click the **Add Address** button.



6. Enter the MAC address you want the JSS to ignore in the **MAC Address** field.

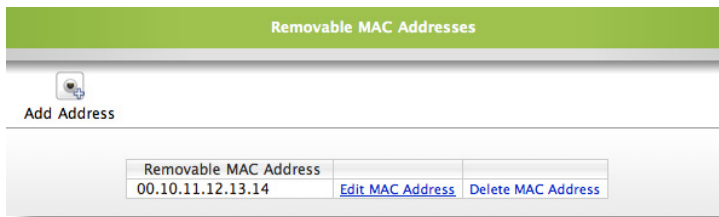


7. Click the **Save** button.

## To edit a removable MAC address:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Removable MAC Addresses** link.

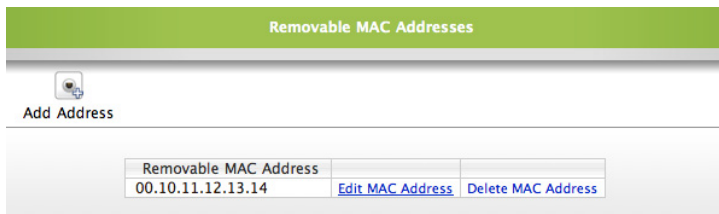
5. Click the **Edit MAC Address** link across from the MAC address you want to edit and update the address.



6. Click **Save**.

**To delete a removable MAC address:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Removable MAC Addresses** link.
5. Click the **Delete MAC Address** link across from the MAC address you want to delete.



6. Click **Delete** to confirm.

# Policies

Policies allow you to automate remote management tasks on client computers by pre-configuring the tasks and caching them in the JAMF Software Server (JSS). This reduces the time you spend configuring individual tasks and pushing them out to computers by allowing clients to initiate the tasks when they check in with the JSS.

The following tasks are commonly performed with a policy:

- Install and uninstall packages.
- Run scripts.
- Add and remove printers.
- Run Software Update.
- Add and remove Dock items.
- Bind clients to directory services.
- Update computer inventory.
- Perform maintenance functions (Self Healing, fix permissions, update computer names, etc.).
- Manage account passwords.

## How Policies Work

Using policies to automate remote management tasks allows you to specify the task(s) you want to perform, when and how often the task(s) should take place, and the clients that should execute the task(s).

After saving the policy, it is stored in the JSS. Each time clients check in with the JSS, they check to see if any policies are available.

Clients execute policies based on three main criteria: trigger, scope, and execution frequency.

### Trigger

A trigger is the action on a client that executes the policy. Clients can execute policies at the following triggers:

- **None (Self Service only)**—Users initiate the policy through the Self Service application
- **Any**—The next time the client checks in with the JSS
- **Startup**—When the client starts up
- **Login**—When a user logs in on a client
- **Logout**—When a users logs out on a client
- **Check-In Frequency**—This is one of the following intervals:
  - 5 minutes
  - 15 minutes
  - 30 minutes
  - Hour

Check-in frequency is configured as part of your Computer Management Framework settings. For information on how to change the check-in frequency, see the “Changing the Computer Management Framework” section.

- **Other**—A custom trigger

## Scope

The scope is the computer or group of computers that runs the policy. Scopes can be based on one or more of the following components:

- Individual computers
- Computer groups
- Departments
- Buildings
- LDAP user groups
- Network segments

## Execution Frequency

The execution frequency is how often clients execute the policy. This depends largely on the task you want to perform. For example, if you’re installing a piece of software, you may want to choose “Once Per Computer” to ensure only one copy of the software is installed on each computer. If you’re updating inventory or performing a routine maintenance task, you may want to choose “One Every Day”, “Once Every Week”, or “Once Per Month”.

Policies can be set at the following execution frequencies:

- Once per computer
- Once per user (At login or logout)
- Once every day
- Once every week
- Once per month (Every 30 days after the first day the policy runs on the computer)
- Ongoing (Every time the trigger takes place)
- Disable (Makes the policy inactive)

## Configuring Policies

There are two ways to configure policies with the Casper Suite: using the Policy Assistant or manually.

The Policy Assistant guides you through the process of configuring a policy to perform the following basic tasks:

- Install a package.
- Cache a package.
- Install a cached package.

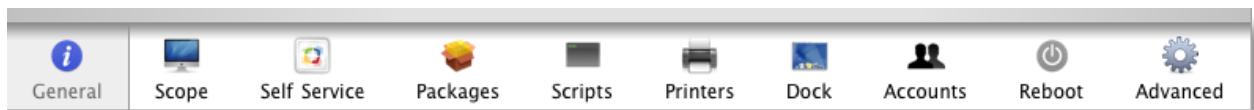


- Uninstall a package.
- Add a printer.
- Remove a printer.
- Run a script.

Configuring a policy manually gives you a variety of extended policy options. The following options allow you to configure date, time, and network limitations:

- Override default settings.
- Perform multiple tasks with a single policy.
- Set reboot criteria.

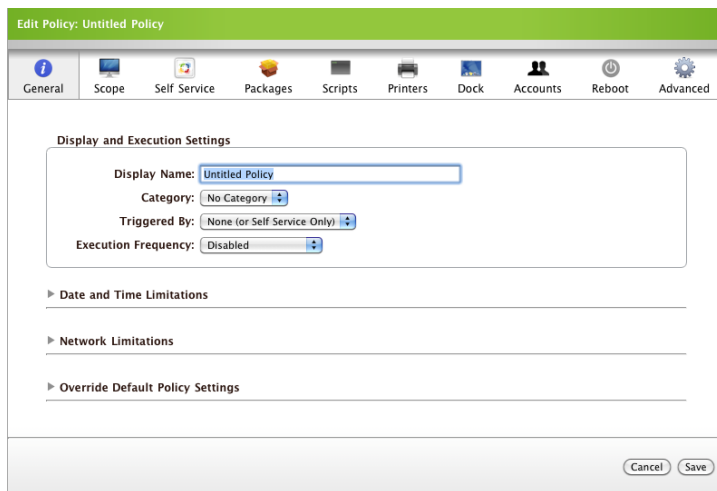
The manual policy interface is made up of the following panes:



The General and Scope panes allow you to configure trigger, scope, and execution frequency, while the other eight panes allow you to set tasks and specify additional criteria.

This section explains each pane in the policy framework and provide basic instructions on how to configure policies using the Policy Assistant and manually.

## General Pane



This pane allows you to configure the following criteria for a policy:

### Display Name (Required)

Enter a display name for the policy.

### Category

Assign the policy to a category.

### Triggered By (Required)

Choose the event in which client computers initiate the policy.

### Execution Frequency (Required)

Choose how often client computers execute a policy.

### Server-Side Limitations

Choose when you want the policy to become active and expire on the server. The policy is available to client computers between the times you specify.

### Client-Side Limitations

Specify the days and times you don't want client computers to run the policy.

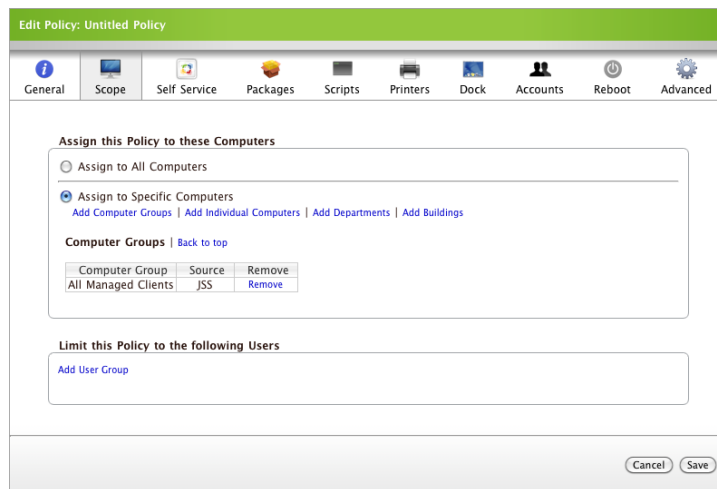
### Network Limitations

Specify the network requirements client computers must meet to run a policy.

### Override Default Policy Settings

Choose the distribution point, Software Update Server, or NetBoot Server from which client computers should pull packages, run software updates, or reboot. This allows you to install packages to a drive other than the current drive.

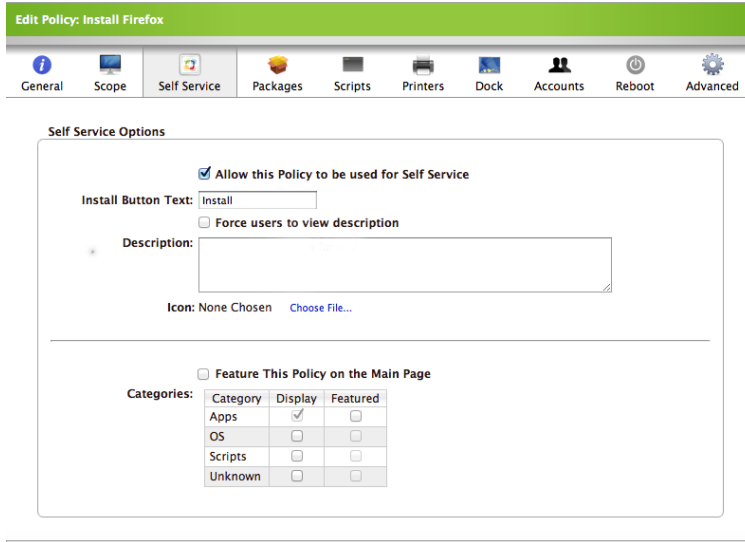
## Scope Pane



This pane allows you to specify which client computers execute the policy.

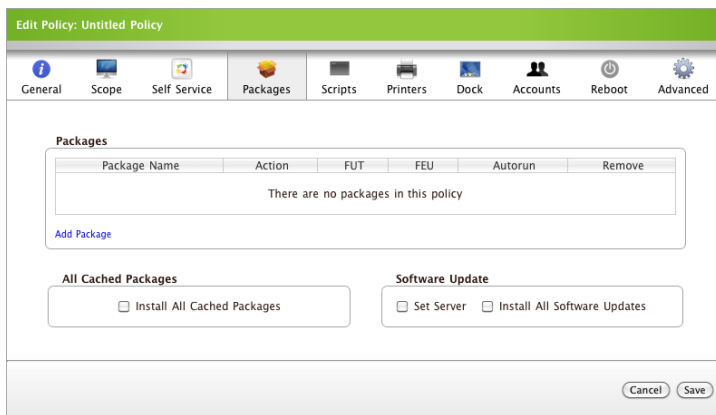
If you integrate with an LDAP server, you can further limit the scope to users of an LDAP group.

## Self Service Pane



This pane allows you to make the policy available through Self Service. For detailed instructions on how to make policies available through Self Service, see the “Making Policies Available in Self Service” section.

## Packages Pane

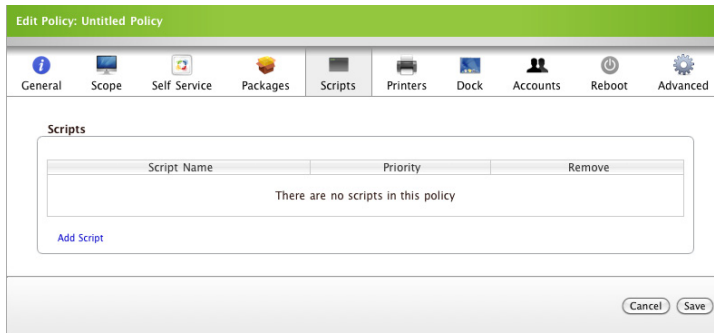


This pane allows you to configure the policy to perform the following software distribution tasks:

- Install, cache, install cached, or uninstall a package.
- Set the default Software Update server.
- Run Software Update.

For detailed instructions on how to configure a policy to perform these tasks, see the “Software Distribution” chapter and the “Running Software Update” section.

## Scripts Pane

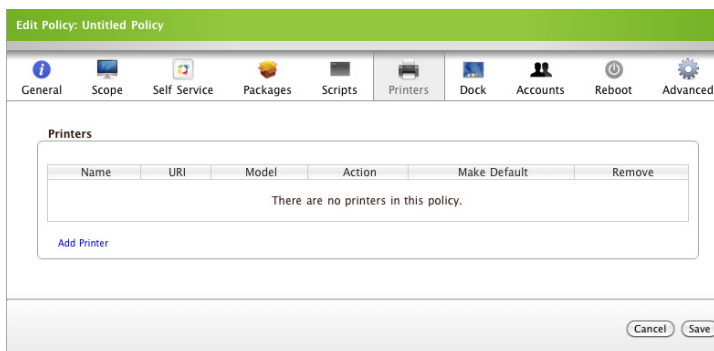


This pane allows you to configure the policy to run a script and set the following script-related information:

- Priority (Run the script at the beginning or end of the policy.)
- Parameters

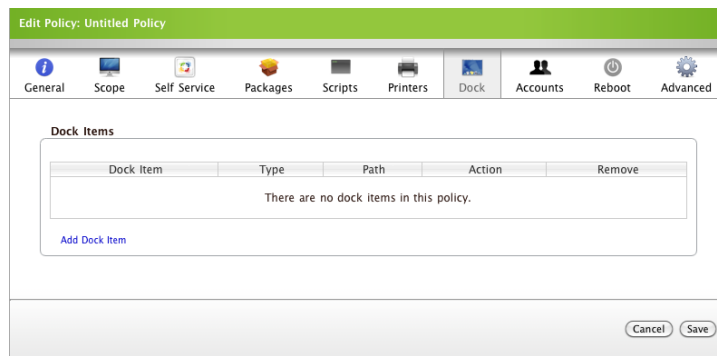
For detailed instructions on how to configure a policy to run a script, see the “Running Scripts” section.

## Printers Pane



This pane allows you to configure the policy to add or remove a printer. For detailed instructions on how to configure a policy to add or remove a printer, see the “Managing Printers” section.

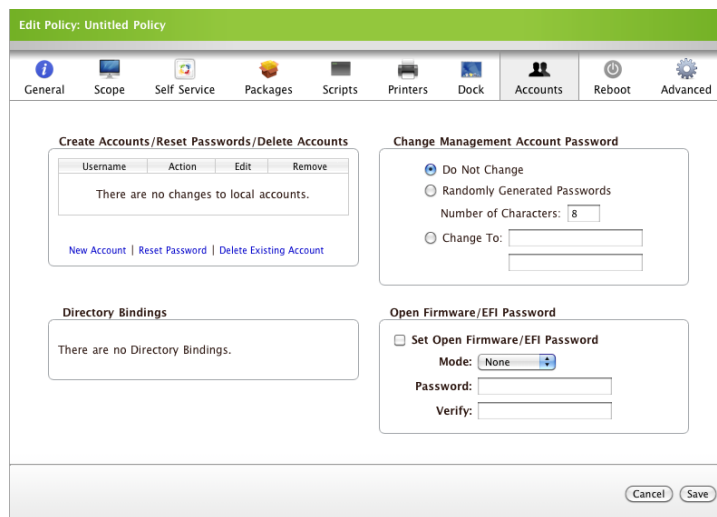
## Dock Pane



This pane allows you to configure the policy to add or remove a Dock item. If you are adding a Dock item, you can also specify where to add the item on the Dock.

For detailed instructions on how to configure a policy to add or remove a Dock item, see the “Managing Dock Items” section.

## Accounts Pane



This pane allows you to configure the policy to perform the following account-related tasks:

- Create and delete local accounts.
- Reset local, management, and Open Firmware/EFI account passwords.
- Create directory bindings.

For detailed instructions on how to configure a policy to perform these tasks, see the following sections:

- “Managing Local Accounts”
- “Binding to Directory Services”
- “Managing Open Firmware/EFI Passwords”

## Reboot Pane

The screenshot shows the 'Reboot' pane of the 'Edit Policy: Untitled Policy' window. The pane is divided into three main sections. The first section, 'If Nobody Is Logged In', has three radio button options: 'Do not Reboot', 'Reboot Immediately', and 'Reboot only if a package or SWU requires', with the third option selected. The second section, 'If Anybody Is Logged In', has three radio button options: 'Do not Reboot', 'Reboot', and 'Reboot only if a package or SWU requires', with the third option selected. Below these is a text input field for 'Give User' with the value '5' and a 'minutes after clicking OK' label, and a 'Reboot Immediately' radio button. The third section, 'Reboot Options', contains a 'Message' text area with the text 'This computer will reboot in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.' and a 'Display message if not rebooting' checkbox. Below the message is a 'Reboot To:' dropdown menu set to 'Current Startup Disk' and a 'Disk Name:' text input field. At the bottom right are 'Cancel' and 'Save' buttons.

This pane allows you to set reboot specifications for client computers executing the policy, display a message at reboot, and specify the drive to which clients reboot.

## Advanced Pane

The screenshot shows the 'Advanced' pane of the 'Edit Policy: Untitled Policy' window. The pane is divided into two main sections. The first section, 'Maintenance', contains a grid of nine checkboxes: 'Update Inventory', 'Reset Computer Names', 'Self Heal Packages', 'Update Prebindings', 'Fix Permissions', 'Fix ByHost Files', 'Flush System Caches', 'Flush User Caches', and 'Verify Startup Disk'. The second section, 'Files & Processes', contains four text input fields: 'Search for file by path:', 'Search for file by name:', 'Spotlight Search:', and 'Search for Process:'. To the right of these fields are two checkboxes: 'Delete if found' and 'Kill if found'. Below the 'Files & Processes' section is a section titled 'Management Framework Options - Not required for clients running 7.3 or later'. At the bottom right are 'Cancel' and 'Save' buttons.

This pane allows you to configure the policy to execute the following maintenance-related tasks:

- Update inventory.
- Reset computer names.
- Update pre-bindings.
- Fix permission.
- Fix ByHost file.
- Flush system caches.

- Flush user caches.
- Verify startup disk.

If you are using the Self Healing feature, you can also configure the policy to run Self Healing on this pane. For detailed instructions on how to configure a policy to run Self Healing, see the “Using the Self Healing Feature” section.

#### To configure a policy using the Policy Assistant:

1. Open the JSS in a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Select the task you want to perform with the policy, and then click **Continue**.
6. Follow instructions on each pane to configure the policy.

When you’re finished using the assistant, you can make changes or configure additional options manually by clicking the **Edit Manually** button on the last pane.

#### To configure a policy manually:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Select **Create policy manually**, and then click **Continue**.
6. Enter a display name for the policy and assign it to a category.
7. Choose a trigger from the **Triggered By** pop-up menu.  
If you choose “Other”, you must enter a manual trigger.
8. Choose an execution frequency from the **Execution Frequency** pop-up menu.  
If you choose “Ongoing”, you can make the policy available to client computers that are offline by selecting the **Make Available Offline** checkbox. This caches each component of the policy on client computers, making them available even when clients are not on the network.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Use the rest of the tabs to configure the policy.
11. Click **Save**.

Client computers execute the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

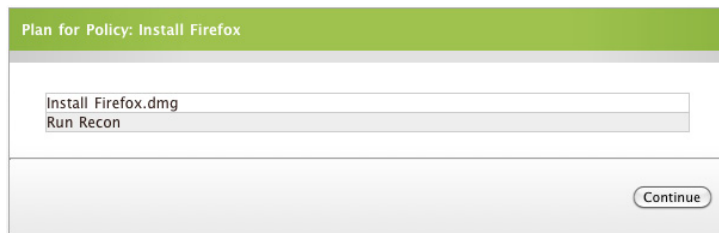
## Managing Policies

This section explains how to:

- View the plan for a policy
- View the status of a policy
- Duplicate a policy
- Edit a policy
- Delete a policy

### To view the plan for a policy using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Show Plan** link across from the policy.  
A complete task list for the policy is displayed.



5. Click **Continue**.

### To view the status of a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **View Status** link across from the policy.  
The table at the top of the page displays an overview of the policy's status. Beneath it is a list of client computers that have executed the policy.  
Clients that have encountered a problem while executing the policy are displayed in red text.
5. If there are clients that encountered problems, you can have them execute the policy again by clicking the **Flush All History With Problems** link.
6. If you want to execute the policy again on all clients, click the **Flush Entire Policy History** link.  
This resets the policy, making it appear as if it had never been executed.



7. Click **Continue**.

Clients execute the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

**To duplicate a policy:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Duplicate Policies** button.
5. Locate the policy you want to duplicate and click the **Duplicate** link across from it.
6. Make changes if necessary.
7. Click **Save**.

**To edit a policy using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Edit Policy** link across from the policy and make changes.
5. Click **Save**.

**To delete a policy using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Delete Policy** link across from the policy.
5. Click **Delete**.

# Inventory

## Managing Inventory Preferences

Inventory preferences are divided into two sections:

- **Inventory Collection preferences**—These preferences allow you to collect additional inventory items and specify how you want to collect them.
- **Inventory Display preferences**—These preferences allow you to change how inventory data is displayed in the JAMF Software Server (JSS).

This section explains both types of inventory preferences and how to set them.

### Inventory Collection Preferences

Inventory Collection preferences allows you to:

- Collect additional inventory items
- Create extension attributes to collect custom data
- Specify additional locations in which to search for software

### Collecting Additional Inventory Items

If the items you want to collect are not included in your inventory by default, you can choose to add any of the following items:

- Application details
- Fonts
- Plug-ins
- UNIX executables
- Package receipts
- Software updates
- Accounts
- Home directory sizes
- Hidden accounts
- Printers
- Running services
- Scheduled tasks
- Command-line tools
- Mobile devices
- Mobile device app purchasing information
- Computer location information

Collecting some of these items may add reporting time and network traffic to the inventory process. The following table provides an estimate of how much time and traffic each item adds.

**Note:** These numbers are based on a MacBook Pro with approximately 100 applications, 2000 UNIX executable files, 300 fonts, 900 plug-ins, and 300 GB of user home directories.

Additional Inventory Items	Time (Seconds)	Traffic (KB)
Default (No Additional Items)	9	102
Application Details (Size, Copyright Info, Date Modified, Bundle ID, and Permissions)	30	133
Fonts	10	128
Plug-ins	13	248
UNIX Executable Files	28	200
Available Software Updates	110	104
Sizes of Home Directories	25	104
All Additional Options	180	726

#### To collect additional inventory items:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Collection Preferences** link.
5. Click the tabs to see a list of additional items in each category and select the checkbox next to each item you want to add.

**Note:** If you choose to collect application details, the .app bundles on Mac OS X computers are searched for additional applications. If you choose to collect application details and UNIX executables, the executable files in any .app bundle are also searched.

6. Click **Save**.

## Creating Extension Attributes

Extension attributes are custom fields that allow you to collect almost any data from a computer. You can create an extension attribute manually or from a template stored in the JSS. You can also upload an extension attribute obtained from an outside source, such as JAMF Nation.

Creating an extension attribute manually allows you to populate data by displaying a text field or pop-up menu, or by running a custom script. Extension attributes created from a template or obtained from an outside source are populated by script.

When an extension attribute is populated by a script, the text between the `<result></result>` tag is stored in the JSS. For Mac OS X computers, scripts can be written in any language that has an interpreter installed. All scripts must start with a shebang (`#!`) followed by the absolute path to the interpreter. The most common interpreters are:

```
/bin/bash
/bin/sh
/usr/bin/perl
/usr/bin/python
```

For example, the script for an extension attribute that collects the host name from Mac OS X computers looks like this:

```
#!/bin/sh
echo "<result>`hostname`&1`</result>"
```

For Windows computers, scripts can be written in VBScript, Batch file, and PowerShell.

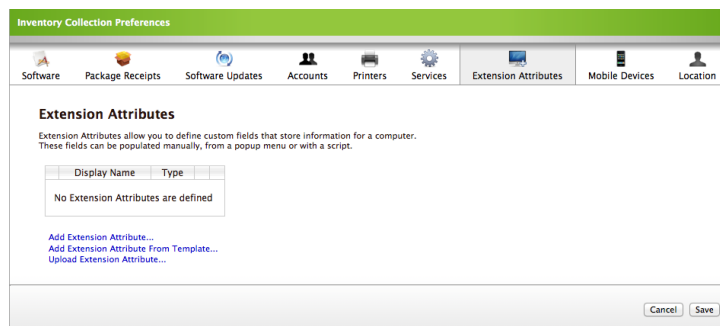
**Note:** PowerShell scripts only run on computers that have components installed to run the script.

Extension attributes can add time and network traffic to the inventory process depending on the type of data you choose to collect and how you choose to collect it.


Like other inventory data, extension attributes can be used as criteria for smart computer groups and advanced computer searches.

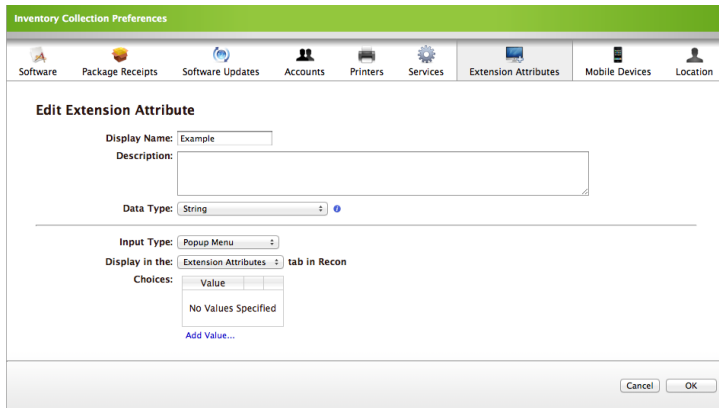
#### To create an extension attribute manually:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Collection Preferences** link.
5. Click the **Extension Attributes** tab.
6. Click the **Add Extension Attribute** link.



7. Enter a display name for the attribute.

8. (Optional) Enter a description.  
This description is displayed when you hover over the **Info**  icon in the list of extension attributes on the Extension Attributes pane.
9. Choose “String, Integer/Real” or “Date” from the **Data Type** pop-up menu.  
This is how the field is evaluated when creating smart computer groups or performing advanced computer searches.
10. Choose whether to populate the information using a text field, pop-up menu, or script.
  - If you choose a text field or pop-up menu, choose the pane on which you want to display the attribute in the Recon interface.
  - If you choose to run a script, enter or paste the script into the field that appears.
11. If you chose to populate the information using a pop-up menu, click the **Add Value** link and enter menu options for the pop-up menu.

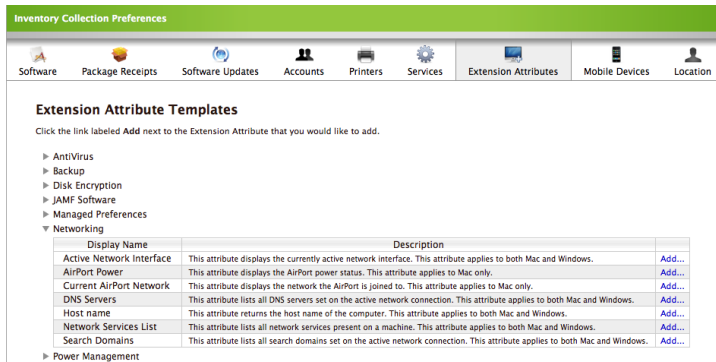


12. Click the **OK** button, and then click **Save**.

**To create an extension attribute using a template:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Collection Preferences** link.
5. Click the **Extension Attributes** tab.
6. Click the **Add Extension Attribute From Template** link.

- Click the disclosure triangles to see a list of the templates in each category and click the **Add** link across from the template you want to add.

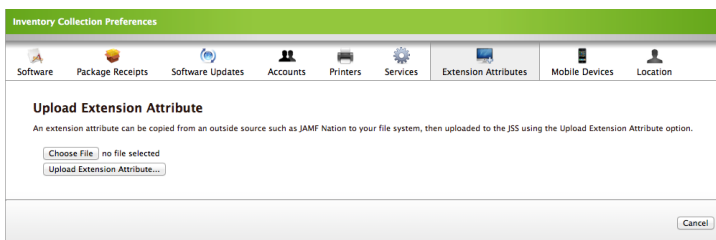


- Click **Save**.

Computers run the script and populate the attribute field each time they submit inventory to the JSS.

### To upload an extension attribute to the JSS:

- Log in to the JSS with a web browser.
- Click the **Settings** tab.
- Click the **Inventory Options** link.
- Click the **Inventory Collection Preferences** link.
- Click the **Extension Attributes** tab.
- Click the **Upload Extension Attribute** link.
- Click **Choose File** and select the extension attribute (.xml) that you want to upload. Then, click **Upload Extension Attribute**.



- Click **Save**.

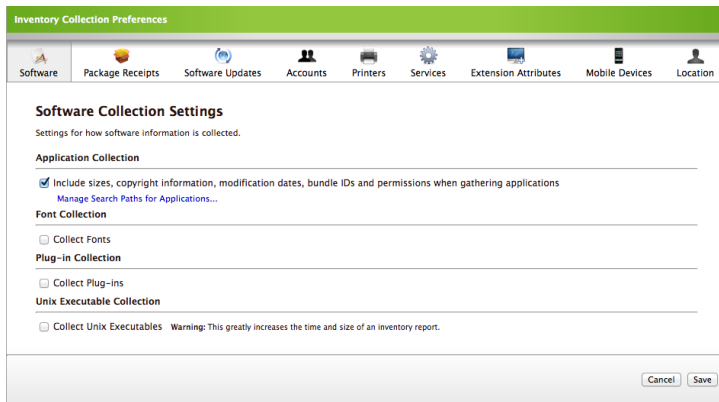
Computers run the script and populate the attribute field each time they submit inventory to the JSS.

## Adding Custom Search Paths

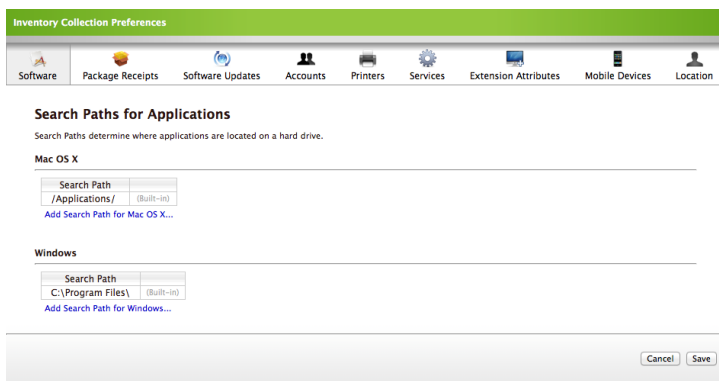
By default, Recon searches for software items (application details, fonts, plug-ins, and UNIX executables) in common locations on Mac OS X and Windows computers. You can define additional locations in which you want Recon to search by adding one or more search paths.

To add custom search paths:

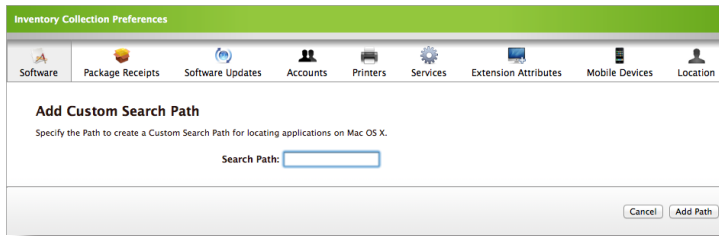
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Collection Preferences** link.
5. On the Software pane, click the **Manage Search Paths for <item>** link below the software item.



6. Click the **Add Search Path for <platform>** link that indicates the correct platform.



7. Enter the search path you want to add, and then click **Add Path**.  
To add every user's home directory to the search path, enter a tilde (~) at the beginning of the search path.  
To add all users on the computer to the search path, enter \$USERNAME in the search path.



8. Click **Save**.

## Inventory Display Preferences

Inventory Display preferences allow you to modify how inventory data is displayed throughout the JSS.

This section explains how to:

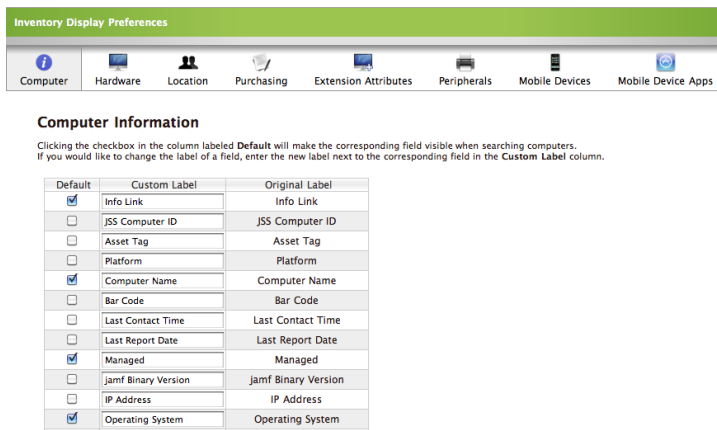
- Add or remove attribute fields from the default inventory search results (Standard Webpage report)
- Create custom field labels
- Group extension attributes on the Computer Details page and the Criteria pane for advanced inventory searches and smart computer groups
- Display app icons on the Mobile Device Details page

**To change the attribute fields displayed in inventory search results:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Display Preferences** link.
5. Click the tabs to locate the attribute fields you want to display or remove.



6. Select the **Default** checkbox to display the attribute or deselect it to remove the attribute.

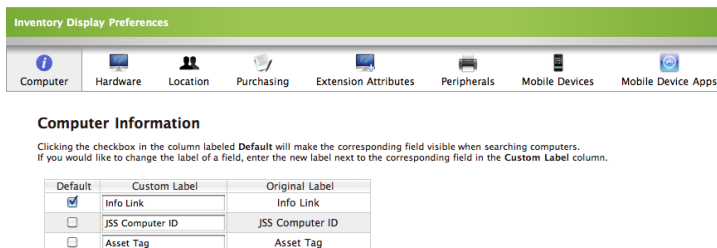


7. Click **Save**.

### To change the name of an attribute field:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Display Preferences** link.
5. Click the tabs to locate the attribute field you want renamed.
6. Enter a new name in the **Custom Label** field next to it.

If you are renaming an extension attribute, enter a new name in the **Display Name** field.



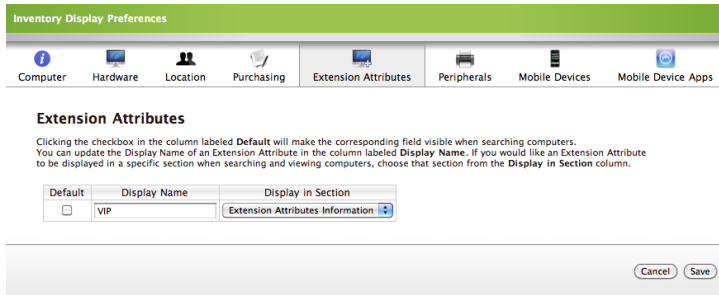
7. Click **Save**.

### To group extension attributes:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Display Preferences** link.

5. Click the **Extension Attributes** tab and use the **Display in Section** pop-up menus to choose a category in which to display the attribute.

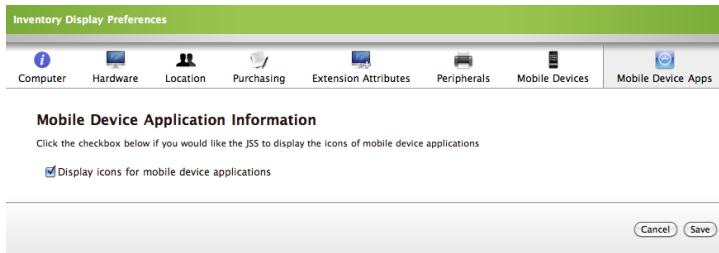
This determines where the attributes are displayed on the Computer Details page and the Criteria pane when you are configuring advanced inventory searches and smart computer groups.



6. Click **Save**.

### To display app icons in the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Display Preferences** link.
5. Click the **Mobile Device Apps** tab and select the **Display icons for mobile device applications** checkbox. This displays the icons in the **Installed Applications** section on the Mobile Device Details page.



6. Click **Save**.

# Managing Peripheral Types

You can track an unlimited number peripherals as part of your inventory. Purchasing and location information are included for each peripheral by default.

This section explains how to add, edit, and delete a peripheral type in the JAMF Software Server (JSS).

## To add a peripheral type:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Peripheral Types** link.
5. Click the **Create Peripheral Type** button in the toolbar.
6. Enter a name for the peripheral type, such as “Scanner” or “Printer”.
7. In the **Field 1–7 Label** fields, enter the name of the attribute that you want to track, such as “Make”, “Model”, “Serial Number”, or “Connection Type”.
8. If you entered an attribute that has a finite number of choices, such as “Connection Type”:
  - a. Select the **Menu** option.
  - b. Use the **Choices** pop-up menu to specify the number of menu options you want to include in the menu. For instance, if your connection possibilities are USB, FireWire, and Parallel, and SCSI select “4” from the **Choices** pop-up menu.

The screenshot shows the 'Add New Peripheral Type' form. The 'Peripheral Type' field is set to 'Scanner'. The form includes seven fields for labels, each with a radio button to select the field type (Text, Menu, or Choices) and a 'Choices' pop-up menu. The 'Choices' menu for 'Field 5 Label' (Connection Type) is open, showing the number '4'. The 'Next...' button is visible at the bottom of the form.

9. Click the **Next** button.

10. If you chose to display an attribute field as a menu, enter the menu options in the fields provided.

**Add New Peripheral Type**

Peripheral Type: Scanner  
Make: *Text Field*  
Model: *Text Field*  
Asset Tag: *Text Field*  
Serial Number: *Text Field*  
Connection Type:

11. Click the **Finish** button.

#### To edit a peripheral type:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Peripheral Types** link.
5. Click the **Edit Peripheral Type** link across from the peripheral you want to edit.
6. If you want to change the order in which the fields are listed, use the **Reorder** pop-up menus to do so, and then click the **Change Order** button.
7. Make the necessary changes and click the **Confirm Changes** button.
8. Verify the changes and click the **Save Changes** button.

#### To delete a peripheral type:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Peripheral Types** link.
5. Click the **Delete Peripheral Type** link across from the peripheral you want to delete.
6. Click **Delete** to confirm.

# Acquiring Mac OS X Computers

Acquisition is the process of adding computers to the JSS. If you only want to search and report on computers as part of your inventory, acquire them using one of the following methods:

- Image computers with a configuration that is not associated with a management account.
- Run Recon locally without specifying a management account.
- Manually add computers to the JSS.

To fully manage computers with the Casper Suite, acquire them using one of the enrollment methods explained in “Enrolling Mac OS X Computer with the JSS”.

You also can enroll a computer after you acquire it. See the “Enrolling Computers by Editing Computer Records” section in “Enrolling Mac OS X Computers with the JSS” for more information.

## Acquiring Computers by Imaging

The first time you image a computer, it is acquired. Using a configuration that is not associated with a management account allows you to acquire the computer without enrolling it. For detailed instructions on creating a configuration, see “Managing Configurations”. For detailed instructions on imaging a computer, see one of the following sections:

- “Imaging Drives”
- “PreStage Imaging”
- “Target Mode Imaging”

## Acquiring Computers by Running Recon Locally

Running Recon locally allows you to collect detailed location information for a specific computer, but it requires your time at the workstation.

**To acquire a computer by running Recon locally:**

1. Copy Recon to the local drive.

**Note:** Recon is a self-contained application and does not require an installer.

2. Open Recon.  
If prompted, enter the DNS name or IP address for the JSS.
3. Select **Local Inventory** in the sidebar.  
The computer name appears by default.

4. Enter the asset tag in the field provided and/or utilize a barcode scanner to enter a bar code.

Recon for My Company - Local Computer Inventory

Local Inventory  
Remote Inventory  
QuickAdd Package  
Network Scanner

Computer  
10.1.20.117

Location

Purchasing

Extension Attributes

Peripherals  
0 Peripherals

Computer

Computer Name: MyCompany0004

Asset Tag:

Bar Code 1:

Bar Code 2:

Username:


Password:

Verify Password:

Account:  No account for remote management.

SSH:  SSH (Remote Login) is running.

Submit

5. (Optional) Select **Location** in the categories list and enter location information for the computer. If an LDAP connection is set up in the JSS, click the **Search**  icon to populate information from the LDAP server.

Recon for My Company - Local Computer Inventory

Local Inventory  
Remote Inventory  
QuickAdd Package  
Network Scanner

Computer  
10.1.20.117


Location

Purchasing

Extension Attributes

Peripherals  
1 Peripheral

Location

Username:  

Real Name:

Email Address:

Phone:

Position:

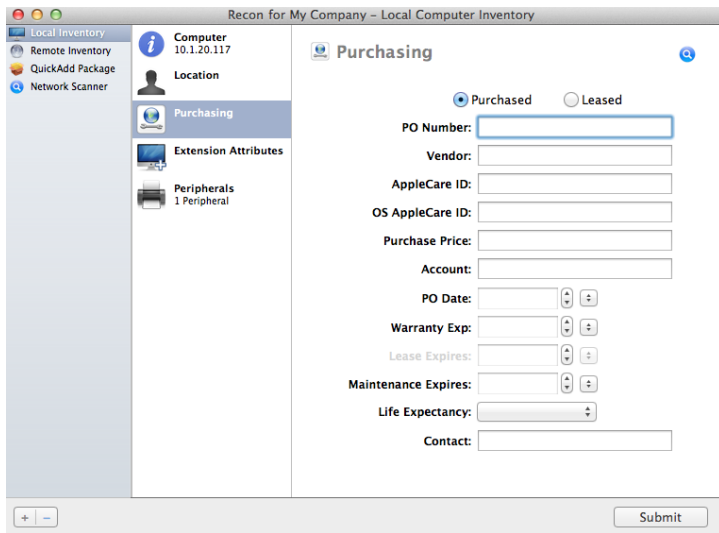
Department: Choose... ▾

Building: Choose... ▾

Room:

Submit

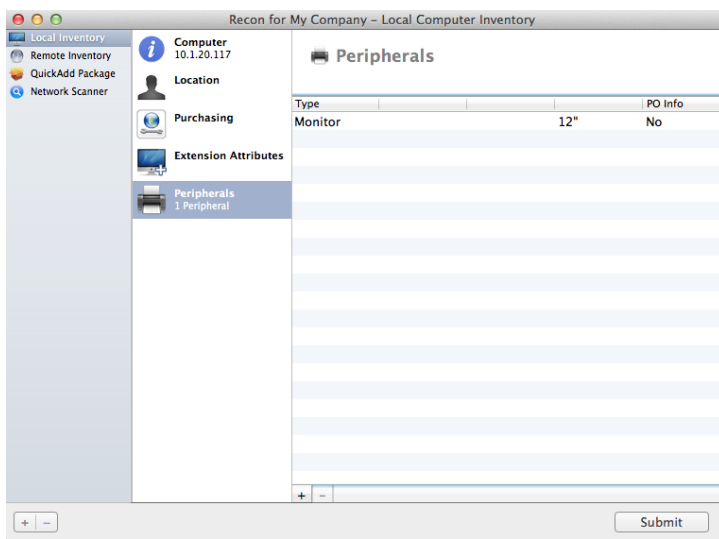
- (Optional) Select **Purchasing** in the categories list and enter purchasing information for the computer. If a GSX connection is set up in the JSS, click the **Search** icon to populate information from Apple's Global Service Exchange (GSX).



- (Optional) Select **Extension Attributes** in the categories list and enter information as needed.
- (Optional) Select **Peripherals** in the categories list. Click the **Add (+)** button to enter information for a new peripheral, and then click **OK** when you are done.



- Click the **Submit** button.



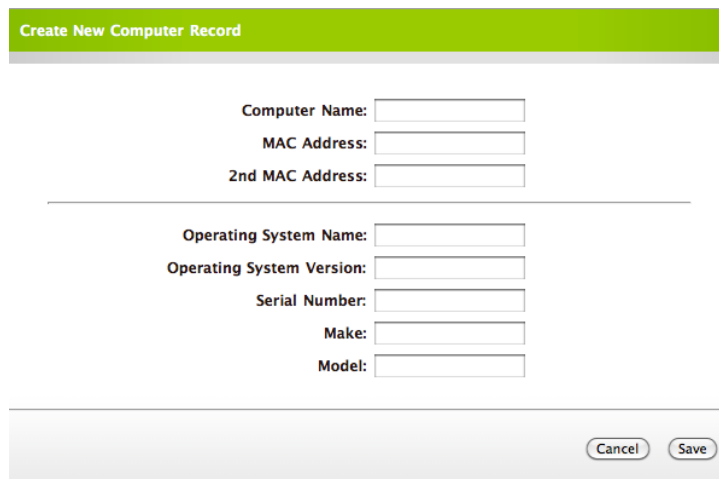
When Recon finishes acquiring the computer, the JSS ID for the computer is displayed at the top of the pane.

## Manually Adding Computers to the JSS

You can acquire a computer manually by entering information about the computer into the JSS.

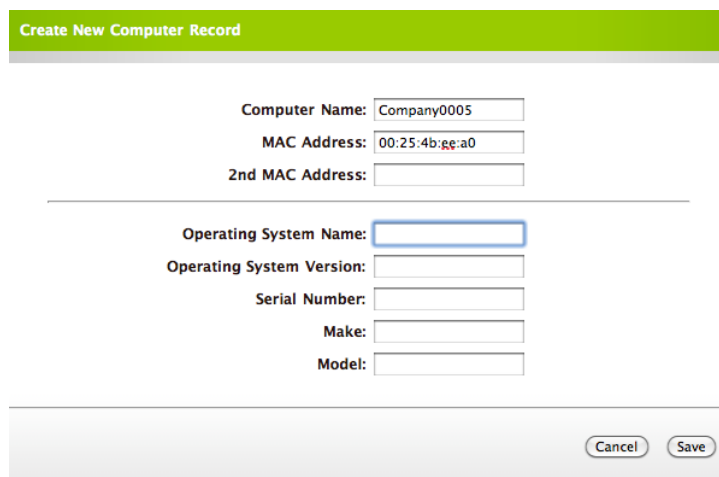
**To add a computer manually:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Add Computer Manually** link.
4. Enter the name of the computer.



The screenshot shows a web form titled "Create New Computer Record" with a green header bar. The form contains several input fields for computer information, all of which are currently empty. The fields are arranged in two columns. The first column includes "Computer Name:", "MAC Address:", and "2nd MAC Address:". The second column includes "Operating System Name:", "Operating System Version:", "Serial Number:", "Make:", and "Model:". At the bottom right of the form, there are two buttons: "Cancel" and "Save".

5. Enter one or more MAC addresses for the computer.
6. (Optional) Enter the name and version of the operating system of the computer.



This screenshot shows the same "Create New Computer Record" form, but with some data entered. The "Computer Name" field contains "Company0005". The "MAC Address" field contains "00:25:4b:ge:a0", with a red error indicator (a small 'x') to its right. The "Operating System Name" field is highlighted with a blue border, indicating it is the active field. All other fields remain empty. The "Cancel" and "Save" buttons are still present at the bottom right.

7. (Optional) Enter the serial number, make, and model of the computer.
8. Click the **Save** button.
9. Use the Details report pane to enter additional information as needed. (See "Viewing Computer Details" for more information.)



# Enrolling Mac OS X Computers with the JSS

Enrollment is the process of adding computers to the JSS and installing a device certificate on them for full management with the Casper Suite. You can perform inventory and remote management and configuration tasks on enrolled computers.

There are several ways to enroll Mac OS X computers with the JSS:

- Provide an enrollment URL.
- Send an OTA invitation.
- Use a QuickAdd package created with Recon.
- Scan the network.
- Run Recon remotely.
- Image computers with a configuration that is associated with a management account.
- Run Recon locally.
- Edit computer records in the JSS.

If you only want to search and report on computers as part of your inventory, add them to the JSS using one of the methods explained in “Acquiring Mac OS X Computers”.

## Providing an Enrollment URL

You can allow users to enroll their own computers by providing them with an enrollment URL. The enrollment URL is the full URL for the JSS followed by /enroll/. For example:

<https://jss.mycompany.com/8443/enroll/>

Users go to the URL, log in with an LDAP directory account or JSS user account, and then follow the onscreen instructions to download and install a QuickAdd package that enrolls their computer.

If users log in with an LDAP directory account, location information for the computer is collected during enrollment.

Enrolling computers by providing an enrollment URL requires:

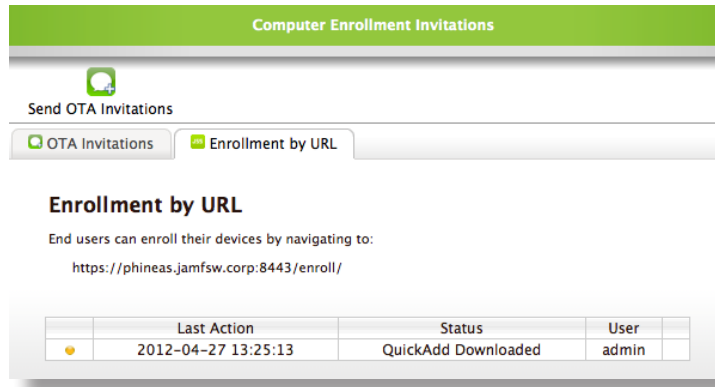
- An LDAP server connection set up in the JSS or a JSS user account with privileges to enroll Mac OS X computers (See “Integrating with LDAP Servers” or “Managing JSS User Accounts” for instructions on how to set up one of these requirements.)
- User-initiated computer enrollment enabled and the QuickAdd package configured in the JSS (See the “User-Initiated Enrollment Process” section in “Configuring the Computer Management Framework” for more information.)

In addition, if the QuickAdd package is signed, client computers must have Apple’s Developer ID Certification Authority intermediate certificate in the system keychain in Keychain Access. For instructions on how to obtain this certificate and import it to the system keychain on client computers, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=294>

### To view the status of URL enrollments:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Computer Enrollment** link, and then click the **Enrollment by URL** tab.



## Sending OTA Invitations

You can allow users to enroll their own computers by sending them an OTA invitation via email. Users click the URL in the invitation and follow the onscreen instructions to download and install a QuickAdd package that enrolls their computers.

Enrolling computers by sending an OTA invitation requires:

- An SMTP server set up in the JSS (See “Enabling Email Notifications” for detailed instructions.)
- A JSS user account with privileges to enroll Mac OS X computers
- User-initiated computer enrollment enabled and the QuickAdd package configured in the JSS (See the “User-Initiated Enrollment Process” section in “Configuring the Computer Management Framework” for more information.)

### To enroll computers by sending an OTA invitation:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Computer Enrollment** link.
4. Click the **Send OTA Invitations** button.

5. Enter the email addresses that you want to send the invitation to, and then click **Continue**. Each entry must be separated with a line break or comma.

The screenshot shows the 'Computer Enrollment Invitation Assistant' dialog box. At the top, a green header bar contains the title. Below it, a progress bar has four steps: 'Recipients', 'Message', 'Security', and 'Complete'. The 'Recipients' step is currently active, indicated by a green dot. The main area is titled 'Enter Email Addresses' and includes the instruction: 'The JSS will send the invitation via email.' Below this is a large, empty text input field. At the bottom right, there are 'Cancel' and 'Continue' buttons.

6. Customize the invitation message as needed, and then click **Continue**.

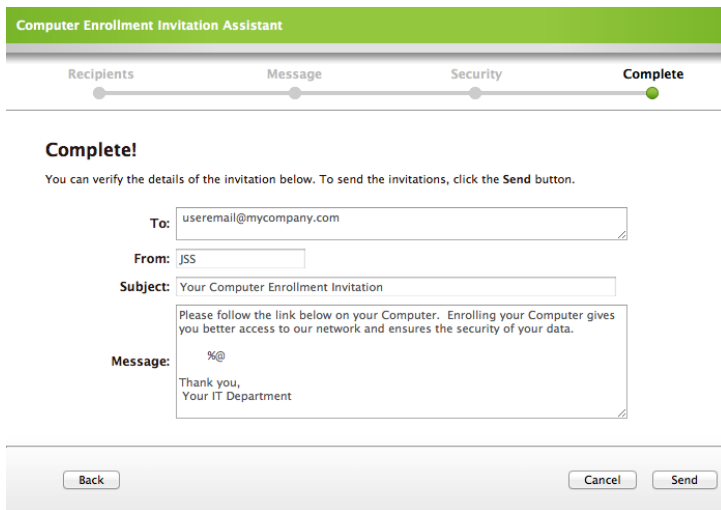
The screenshot shows the 'Computer Enrollment Invitation Assistant' dialog box. The progress bar now has the 'Message' step active, indicated by a green dot. The main area is titled 'Enter Invitation Message' and includes the instruction: 'Enter the subject and content of the invitation that will be sent via email. The %@ will be automatically replaced with the URL in the message.' Below this are several input fields: 'Sender's name:' with 'JSS' and '(optional)', 'Reply-To:' with '(optional)', and 'Subject:' with 'Your Computer Enrollment Invitation'. A larger text area for the message content contains the text: 'Please follow the link below on your Computer. Enrolling your Computer gives you better access to our network and ensures the security of your data.' followed by 'Message: %@' and 'Thank you, Your IT Department'. At the bottom, there are 'Back', 'Cancel', and 'Continue' buttons.

7. Specify an expiration date for the invitation.

The screenshot shows the 'Computer Enrollment Invitation Assistant' dialog box. The progress bar now has the 'Security' step active, indicated by a green dot. The main area is titled 'Invitation Security Options' and includes the instruction: 'Choose the security options for the enrollment invitations.' Below this is an 'Expires On:' field with a date picker set to '6 / 3 / 2012' and a time picker set to '10 : 00 AM'. A checkbox labeled 'Allow multiple uses of invitations' is checked. At the bottom, there are 'Back', 'Cancel', and 'Continue' buttons.

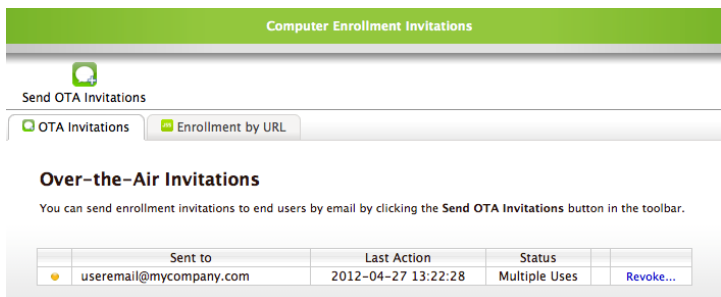
8. If you want to allow multiple uses of the invitation, leave the **Allow multiple uses of invitations** checkbox selected, and then click **Continue**.

- Verify that the information on the Complete pane is correct, and then click **Send**.



**To view the status of OTA enrollments:**

- Log in to the JSS with a web browser.
- Click the **Management** tab.
- Click the **Mobile Device Enrollment** link, and then click the **OTA Invitations** tab.



## Using QuickAdd Packages Created with Recon

Recon allows you to create QuickAdd packages that you can install on computers to enroll them. You can deploy QuickAdd packages using almost any deployment tool, such as Apple Remote Desktop, the Casper Suite, or other client management systems. You can also give QuickAdd packages to users to install.

When you create a QuickAdd package with Recon, you can configure it to perform the following actions on computers:

- Set a management account. *(Required)*
- Enable SSH (remote login).
- Check for policies after the package is installed.
- Launch Self Service after the package is installed.

You can also sign the QuickAdd package with an installer certificate (.p12) obtained from Apple's Developer Certificate Utility. Signing the QuickAdd package ensures that it appears as verified to users. It also allows users to install the QuickAdd package on computers that have Apple's Gatekeeper feature set to only allow applications downloaded from the Mac App Store and identified developers.

To sign a QuickAdd package, Recon must be running on OS X v10.7 or later.

To obtain an installer certificate from Apple's Developer Certificate Utility, you must be a registered Apple Developer in the Mac Developer Program. To enroll in the Mac Developer Program, visit the following website:

<https://developer.apple.com/programs/mac/>

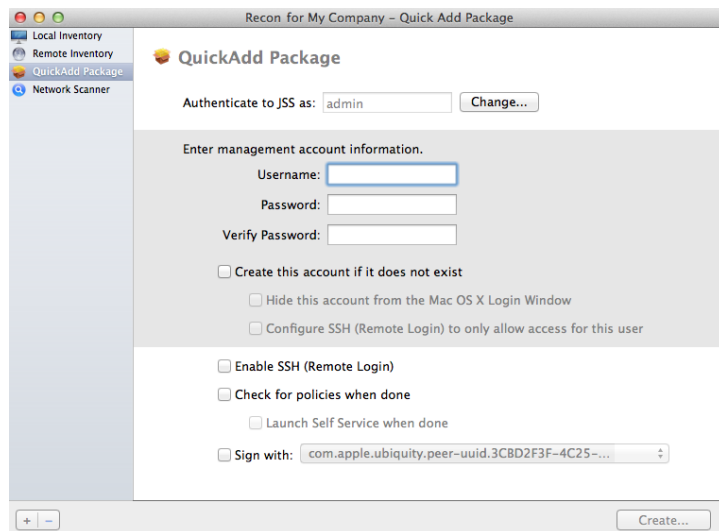
To install a signed QuickAdd package, the system keychain in Keychain Access must contain Apple's Developer ID Certification Authority intermediate certificate. For instructions on how to obtain this certificate and import it to the system keychain on client computers, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=294>

#### To enroll computers using a QuickAdd package created with Recon:

1. Open Recon.
2. Authenticate to the JSS and click **Connect**.
3. Select **QuickAdd Package** in the sidebar.
4. To change the account that the QuickAdd package uses to authenticate to the JSS, click the **Change** button. Enter credentials for the account, and then click **Connect**.

The account must have the "Add Hardware" privilege.

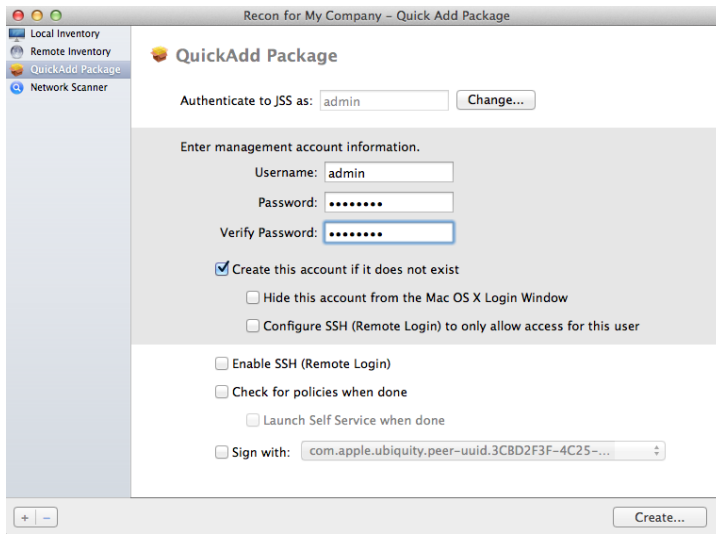


5. Specify the account that you want to use for management.

This can be a new account or an existing account.

If the management account is a new account, select the **Create this account if it does not exist** checkbox and Recon will create the account for you.

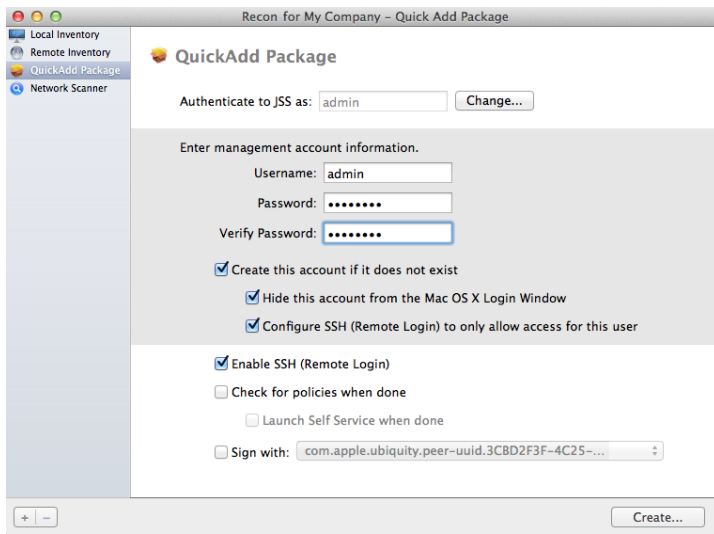
6. If the management account is a new account, you can configure the following options:
  - Hide the account by selecting the **Hide this account from the Mac OS X Login Window** checkbox.
  - Make the account the only account that has SSH access to the computers by selecting the **Configure SSH (Remote Login) to only allow access for this user** checkbox.



7. To enable SSH on the computers, select the **Enable SSH (Remote Login)** checkbox.
8. If you want the computers to check for policies immediately after the package is installed, select the **Check for policies when done** checkbox.
9. If you want computers to launch Self Service immediately after the package is installed, select the **Launch Self Service when done** checkbox.  
This option is only available if you selected the **Check for policies when done** checkbox.
10. If you want to sign the QuickAdd package, select the **Sign with** checkbox and choose an installer certificate from the pop-up menu.  
Installer certificates that are located in the login keychain in Keychain Access are displayed in the pop-up menu.

**Note:** The pop-up menu also displays application certificates that are located in the login keychain in Keychain Access. It is important that you use an installer certificate, not an application certificate, to sign QuickAdd packages.

11. Click the **Create** button.



12. Save the QuickAdd package to the desired location.
13. Deploy the package using a remote deployment tool or give the package to users to install.

When users install the QuickAdd package, the computers are enrolled with the JSS.

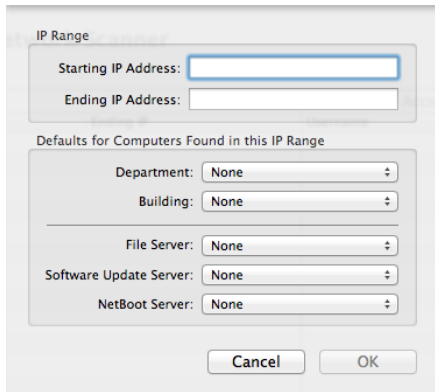
## Scanning the Network

The network scanner in Recon allows you to enroll computers that have SSH (remote login) enabled. This requires you to specify a range of IP addresses and one or more administrator accounts that have SSH access to the computers. Recon then scans the specified IP range and enrolls any computers that it can connect to over SSH.

### To enroll computers by scanning the network:

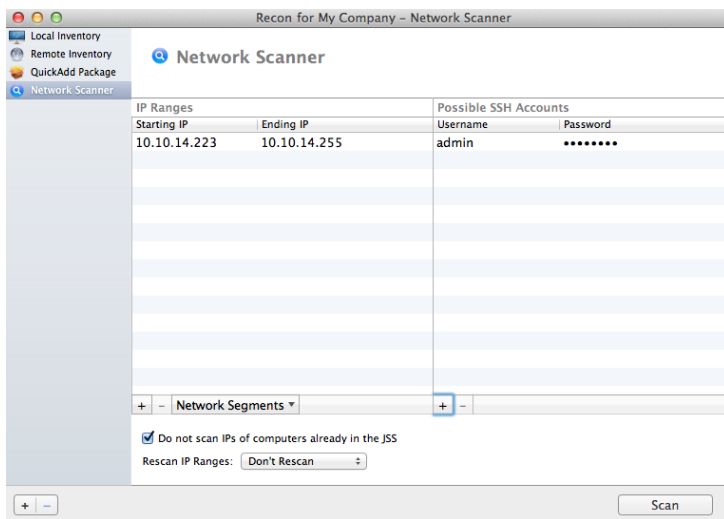
1. Open Recon.
2. Authenticate to the JSS and click **Connect**.
3. Select **Network Scanner** in the sidebar.

- If you have network segments specified in the JSS, choose the network segment(s) you want to scan by clicking the **Network Segments** button below the IP ranges list.  
Alternatively, you can create custom IP ranges by clicking the **Add (+)** button below the IP Ranges list and entering the beginning and ending IP address. Then, use the pop-up menus to set default locations and servers for the computers, and click **OK**.



The dialog box is titled "IP Range". It contains two input fields: "Starting IP Address:" and "Ending IP Address:". Below these is a section titled "Defaults for Computers Found in this IP Range" with five dropdown menus: "Department: None", "Building: None", "File Server: None", "Software Update Server: None", and "NetBoot Server: None". At the bottom are "Cancel" and "OK" buttons.

- Specify one or more administrator accounts that have SSH access to the computers by clicking the **Add (+)** button below the Possible SSH Accounts list.  
If more than one administrator account exists on the network, enter credentials for each account. Recon tries each set of credentials until it finds a valid account for the computer.  
The SSH account is used as the management account.
- To ignore computers that are already in the JSS, select the **Do not scan IPs of computers already in the JSS** checkbox.



The screenshot shows the "Network Scanner" window in the "Recon for My Company" application. It features a sidebar with "Local Inventory", "Remote Inventory", "QuickAdd Package", and "Network Scanner". The main area contains a table with two columns: "IP Ranges" and "Possible SSH Accounts".

Starting IP	Ending IP	Username	Password
10.10.14.223	10.10.14.255	admin	*****

Below the table is a "Network Segments" dropdown menu with a "+" button. A checkbox labeled "Do not scan IPs of computers already in the JSS" is checked. Below that is a "Rescan IP Ranges:" dropdown menu set to "Don't Rescan". At the bottom right is a "Scan" button.

- To continuously scan the network for new computers, use the **Rescan IP Ranges** pop-up menu to specify how often Recon should rescan.
- Click **Save As** to save the settings.  
This creates a .recon file that can be opened with Recon.



9. Click the **Scan** button.

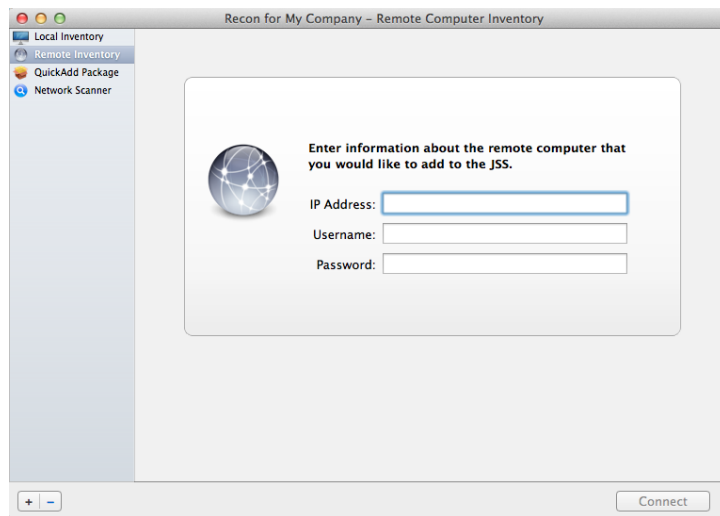
Once you complete these steps, Recon attempts to connect and authenticate to each IP address that has SSH enabled. The results of the scan are displayed on the Inventoried, Not Found, and Problems panes.

## Running Recon Remotely

If you know the DNS name or IP address for the computer that you want to enroll and SSH (remote login) is enabled on the computer, you can use Recon to enroll it remotely. This allows you to enter detailed information for the computer before you enroll it.

### To enroll a computer by running Recon remotely:

1. Open Recon.
2. Authenticate to the JSS and click **Connect**.
3. Select **Remote Inventory** in the sidebar.
4. Enter the IP address of the computer you want to add.



5. Enter credentials for an administrator account that has SSH access to the computer, and click the **Connect** button.

This account is used as the management account.

- (Optional) Select **Location**, **Purchasing**, **Extension Attributes**, and/or **Peripherals** in the categories list and enter information as needed.

Recon for My Company - Remote Computer Inventory

Local Inventory  
Remote Inventory  
QuickAdd Package  
Network Scanner

Computer  
10.1.24.76

Location  
Purchasing  
Extension Attributes  
Peripherals  
0 Peripherals

Computer

Computer Name: MyCompany0004  
Asset Tag:  
Bar Code 1:  
Bar Code 2:

Username: admin  
Password: .....  
Verify Password: .....

Account: ✔ Ready to submit.  
SSH: ✔ SSH (Remote Login) is running.

Close Submit

- Click the **Submit** button.

When Recon finishes enrolling the computer, the JSS ID for the computer is displayed at the top of the pane.

## Enrolling Computers by Imaging

The first time you image a computer, it is acquired. Using a configuration that is associated with a management account allows you to enroll the computer with the JSS. For detailed instructions on creating a configuration, see “Managing Configurations”. For detailed instructions on imaging a computer, see one of the following sections:

- “Imaging Drives”
- “PreStage Imaging”
- “Target Mode Imaging”

## Enrolling Computers by Running Recon Locally

Running Recon locally allows you to collect detailed location information for a specific computer, but it requires your time at the workstation.

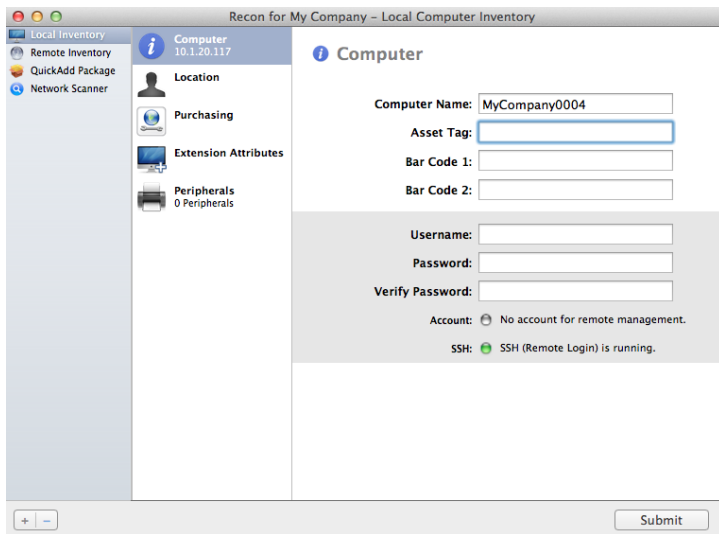
**To enroll a computer by running Recon locally:**

- Copy Recon to the local drive.

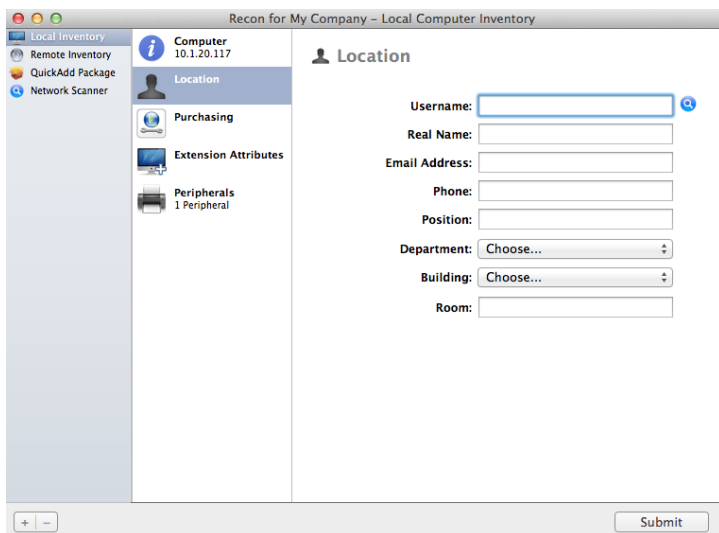
**Note:** Recon is a self-contained application and does not require an installer.


- Open Recon.  
If prompted, enter the DNS name or IP address for the JSS.

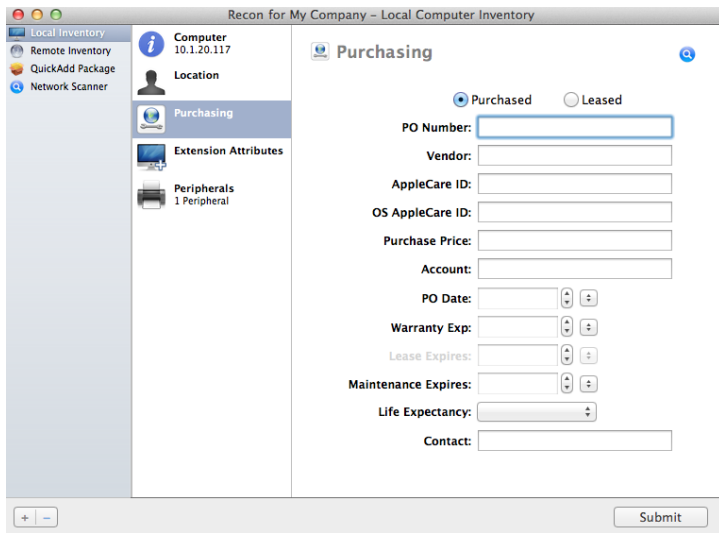
3. Select **Local Inventory** in the sidebar.  
The computer name appears by default.
4. Enter the asset tag in the field provided and/or utilize a barcode scanner to enter a bar code.



5. Enter credentials for the account that you want to use for management.  
This can be an existing account or a new account. If it is a new account, Recon creates the account for you. If SSH (remote login) is not enabled on the computer, Recon activates it automatically.
6. (Optional) Select **Location** in the categories list and enter location information for the computer.  
If an LDAP connection is set up in the JSS, click the **Search** icon to populate information from the LDAP server.



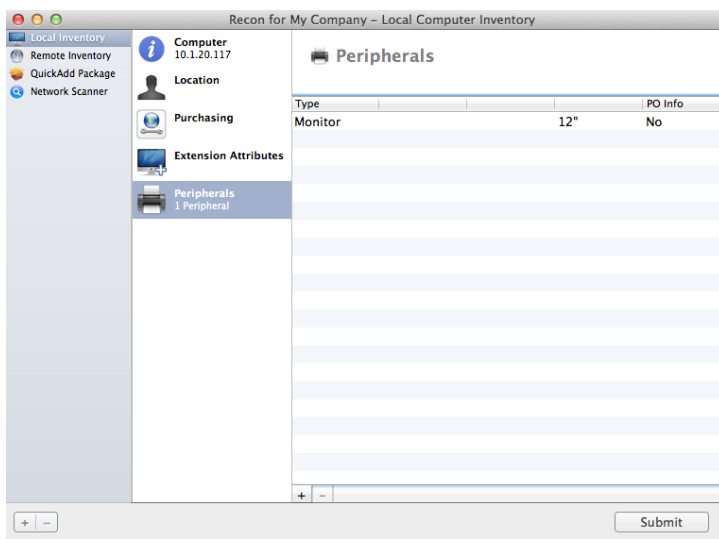
- (Optional) Select **Purchasing** in the categories list and enter purchasing information for the computer. If a GSX connection is set up in the JSS, click the **Search**  icon to populate information from Apple's Global Service Exchange (GSX).



- (Optional) Select **Extension Attributes** in the categories list and enter information as needed.
- (Optional) Select **Peripherals** in the categories list. Click the **Add (+)** button to enter information for a new peripheral, and then click **OK** when you are done.



- Click the **Submit** button.




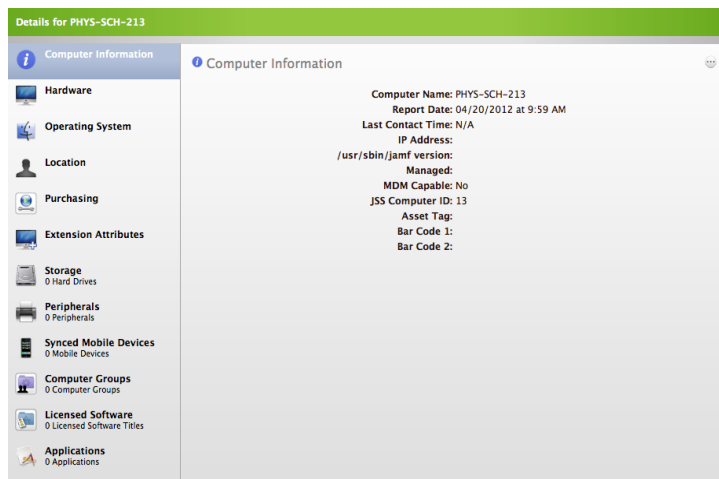
When Recon finishes enrolling the computer, the JSS ID for the computer is displayed at the top of the pane.

# Enrolling Computers by Editing Computer Records

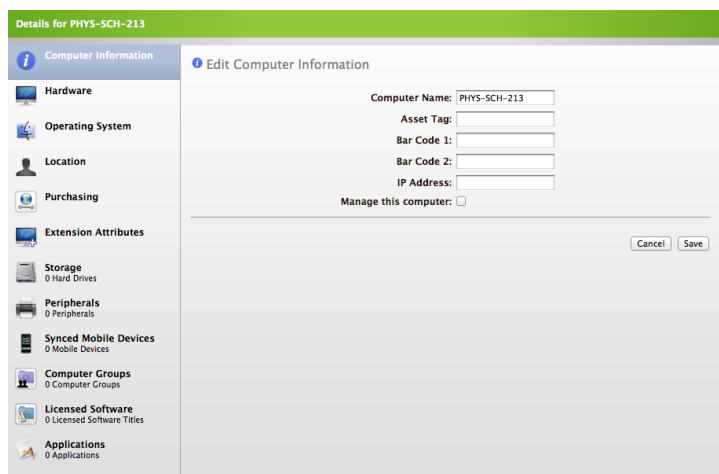
If you added a computer to the JSS using one of the methods explained in “Acquiring Mac OS X Computers”, you can enroll it afterward by editing the computer record in the JSS.

To enroll a computer by editing the computer record in the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab and perform a simple or advanced computer search. See the “Performing a Simple Computer Search” or “Performing an Advanced Computer Search” section in “Searching Computers” for complete instructions.
3. Find the computer that you want to enroll, and click the **Details** link across from it.
4. On the Computer Information pane, click the **Ellipsis**  button.



5. Select the **Manage this computer** checkbox.



- Specify the account that you want to use for management.  
This must be an existing account.

The screenshot shows a web-based management interface for a computer named 'PHYS-SCH-213'. The interface has a green header bar with the title 'Details for PHYS-SCH-213'. Below the header is a navigation pane on the left with icons and labels for various categories: Computer Information, Hardware, Operating System, Location, Purchasing, Extension Attributes, Storage (Hard Drives), Peripherals, Synced Mobile Devices (Mobile Devices), Computer Groups, Licensed Software (Licensed Software Titles), and Applications. The main content area is titled 'Edit Computer Information' and contains the following fields:

- Computer Name: PHYS-SCH-213
- Asset Tag: [text input]
- Bar Code 1: [text input]
- Bar Code 2: [text input]
- IP Address: [text input]
- Manage this computer:
- SSH Username: [text input]
- SSH Password: [text input]
- Verify SSH Password: [text input]

At the bottom right of the form are 'Cancel' and 'Save' buttons.

- Click Save.

# Acquiring Windows Computers

Acquisition is the process of adding computers to the JSS. There are three ways to acquire Windows computers as part of your inventory:

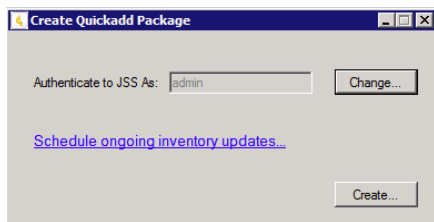
- Use a QuickAdd package.
- Run Recon locally.
- Manually add computers to the JSS.

## Using QuickAdd Packages

Recon.exe allows you to create QuickAdd packages (.mist) that you can install on Windows computers to acquire them. You can deploy QuickAdd packages using a remote deployment tool, such as Apple Remote Desktop, or you can give them to users to install.

**To acquire computers using a QuickAdd package:**

1. Open Recon.exe.  
If prompted, enter the DNS name or IP address for the JSS.
2. Authenticate to the JSS and click **OK**.
3. Click the **QuickAdd Package** button.
4. To change the account that the QuickAdd package uses to authenticate to the JSS, click the **Change** button. Enter credentials for the account, and then click **OK**.



5. If you want to create an inventory schedule, click the **Schedule ongoing inventory updates** link. Configure the schedule and click **Save**.
6. Click the **Create** button.
7. Save the package to the desired location.
8. Deploy the package using a remote deployment tool or give the package to users to install.

When users install the QuickAdd package, the computers are added to inventory.

## Running Recon Locally

Running Recon locally allows you to collect detailed location information for a specific computer, but it requires your time at the workstation.

### To acquire a computer by running Recon locally:

1. Copy Recon.exe to the local drive.

**Note:** Recon.exe is a self-contained application and does not require an installer.

2. Open Recon.exe.

If prompted, enter the DNS name or IP address for the JSS.

When Recon.exe opens, the computer name appears by default.

3. Enter the asset tag in the field provided and/or utilize a barcode scanner to enter a bar code.

The screenshot shows the 'Recon for JAMF Software - Local Computer Inventory' application window. The 'Computer Information' tab is active. The 'Computer Name' field contains 'COMPANY-MTILCQL'. There are empty fields for 'Asset Tag', 'Bar Code 1', and 'Bar Code 2'. Below these are fields for 'Username', 'Password', and 'Verify Password', along with radio buttons for 'Account' and 'SSH'. A 'Submit' button is located at the bottom right of the form area.

4. (Optional) Click the **Location** tab and enter location information for the computer.

If an LDAP connection is set up in the JSS, click the **Check Name** button to populate information from the LDAP server.

The screenshot shows the 'Recon for JAMF Software - Local Computer Inventory' application window with the 'Location' tab selected. Fields include 'Username', 'Real Name', 'Email Address', 'Position', 'Phone', 'Department', 'Building', and 'Room'. There are 'Clear' and 'Check Name' buttons. A 'Submit' button is at the bottom right.



- (Optional) Click the **Purchasing Information** tab and enter purchasing information for the computer.

The screenshot shows the 'Recon for JAMF Software - Local Computer Inventory' application window. The 'Purchasing Information' tab is selected. At the top, there are radio buttons for 'Purchased' (selected) and 'Leased'. Below this, there are several input fields and dropdown menus: 'PO Number', 'Vendor', 'AppleCare ID', 'Purchase Price', 'Account', 'PO Date', 'Warranty Expires', 'Life Expectancy', and 'Contact'. A 'Submit' button is located at the bottom right of the form area.

- (Optional) Click the **Extension Attributes** tab and enter information as needed.
- (Optional) Click the **Peripherals** tab. Click the **Add (+)** button to enter information for a new peripheral, and then click **OK**.

The screenshot shows the 'Add Peripheral' dialog box. It contains a 'Type' dropdown menu, two 'Bar Code' input fields (Bar Code 1 and Bar Code 2), a 'Show Purchasing Information' checkbox, and 'Cancel' and 'OK' buttons at the bottom.

- Click the **Submit** button.

The screenshot shows the 'Recon for JAMF Software - Local Computer Inventory' application window. The 'Peripherals' tab is selected. It displays a table with columns for 'Type' and 'PO Info'. Below the table are '+' and '-' buttons. A 'Submit' button is located at the bottom right of the window.

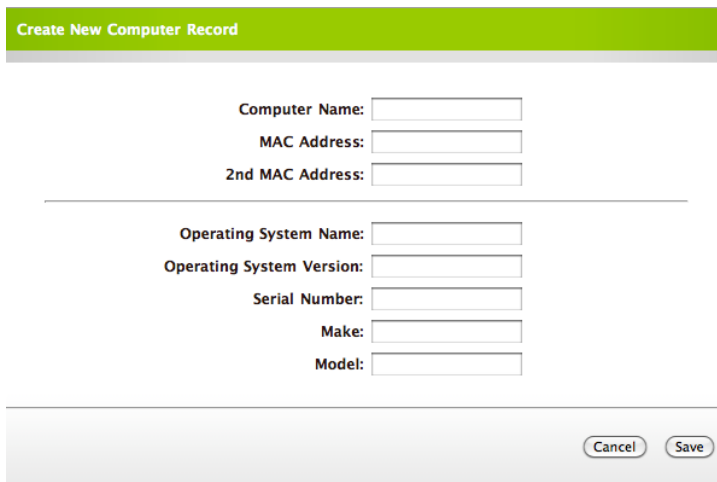
When Recon.exe finishes acquiring the computer, the JSS ID for the computer is displayed at the top of the pane.

## Acquiring Computers Manually

You can acquire a computer manually by entering information about the computer into the JSS.

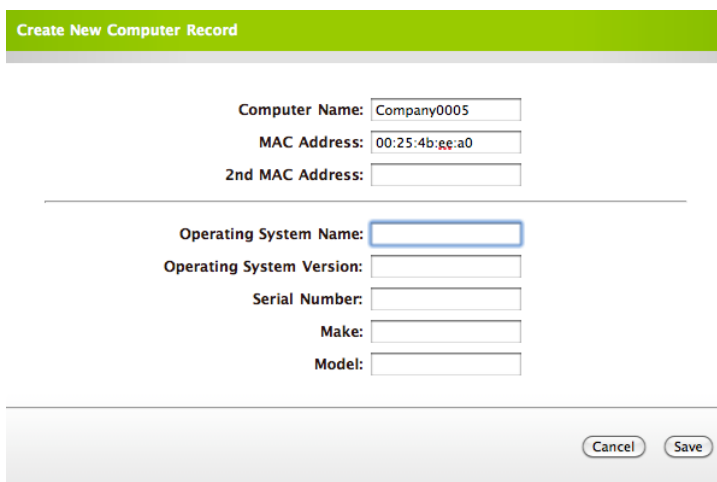
To add a computer manually:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Add Computer Manually** link.
4. Enter the name of the computer.



The screenshot shows a web form titled "Create New Computer Record" with a green header. The form contains several input fields for computer information, all of which are currently empty. The fields are arranged in two sections separated by a horizontal line. The first section includes "Computer Name:", "MAC Address:", and "2nd MAC Address:". The second section includes "Operating System Name:", "Operating System Version:", "Serial Number:", "Make:", and "Model:". At the bottom right of the form, there are two buttons: "Cancel" and "Save".

5. Enter one or more MAC addresses for the computer.
6. (Optional) Enter the name and version of the operating system of the computer.



The screenshot shows the same "Create New Computer Record" form, but now with some data entered. The "Computer Name" field contains "Company0005". The "MAC Address" field contains "00:25:4b:ee:a0". The "2nd MAC Address" field is empty. The "Operating System Name" field is highlighted with a blue border, indicating it is the active field. The other fields in the second section ("Operating System Version:", "Serial Number:", "Make:", "Model:") are still empty. The "Cancel" and "Save" buttons are visible at the bottom right.

7. (Optional) Enter the serial number, make, and model of the computer.
8. Click the **Save** button.
9. Use the Details report pane to enter additional information as needed. (See the "Viewing Computer Details" section for more information.)

# Acquiring Mobile Devices

You can acquire mobile devices by syncing them with the iTunes library on a Mac OS X or Windows computer. This allows Recon to collect information about the device from the iTunes library and send it back to the JAMF Software Server (JSS) each time the computer submits an inventory report.

Recon collects the following information from the iTunes library:

- General information
- Location information
- Purchasing information
- Apps
- App purchasing information (Optional)

To ensure that the JSS reflects updated inventory information for a synced device, make sure the device is synced regularly.

Syncing a device with a computer's iTunes library does not enroll the device with the JSS. For instructions on enrolling devices, see "Enrolling Mobile Devices with the JSS".

In addition, syncing an enrolled device with a computer's iTunes library does not update the device's inventory in the JSS. Enrolled devices submit inventory over-the-air. For more information on collecting inventory from enrolled devices, see "Inventory Collection Frequency" in the "Configuring the Mobile Device Management Framework" section.

This section explains how to acquire synced devices.

## To acquire synced mobile devices:

1. Log in to the JSS in a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Inventory Collection Preferences** link.
5. Click the **Mobile Devices** tab.
6. Select the **Gather mobile devices** checkbox.
7. To only collect devices that already exist in the JSS (from previous inventory reports), select the **Only include mobile devices already in the JSS** checkbox.
8. To track purchasing information for apps from the App Store, select the **Gather mobile device application purchasing information** checkbox.
9. Click **Save**.

# Searching Computers

Once you acquire computers, they can be viewed for inventory or reporting purposes. Since the JAMF Software Server (JSS) is web-based, you can view your inventory from virtually any web browser on any platform.

This section explains how to:

- Perform simple and advanced computer searches
- View computer search results
- View computer details

## Performing Simple Computer Searches

A simple computer search functions like a search engine, allowing you to locate a general range of results quickly and easily.

Simple searches can be performed based on the following attributes of a computer:

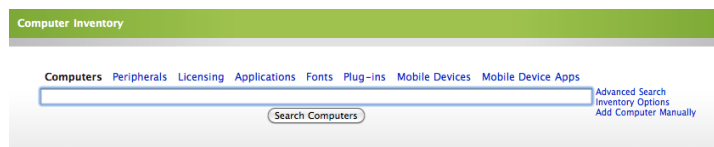
- Computer name
- MAC address
- Bar code
- IP address
- Asset tag
- Serial number
- Username
- Real name
- Email address
- Phone number
- Position
- Department
- Building
- Room

**Note:** Performing an empty search (with no criteria in the search field) returns all computers in your database.

**To perform a simple computer search:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.

The **Computers** link above the search field is selected by default.



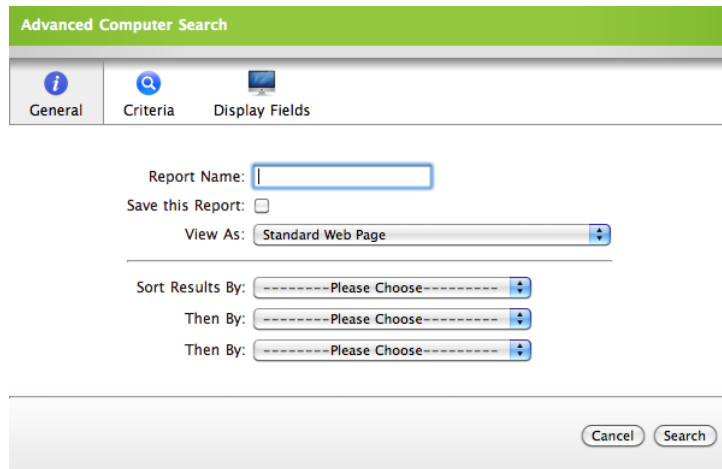
3. Enter one or more search terms into the search field.
4. Click the **Search Computers** button, or press the Enter key.

## Performing Advanced Computer Searches

When used to search for computers and create reports, advanced searches offer a variety of powerful options. The advanced computer search interface consists of three panes: General, Criteria, and Display Fields.

A detailed description of the information on each pane follows:

### General Pane



The screenshot shows the 'Advanced Computer Search' interface with the 'General' pane selected. The interface includes a header bar with three tabs: 'General' (selected), 'Criteria', and 'Display Fields'. Below the tabs, there is a 'Report Name' text input field, a 'Save this Report' checkbox, and a 'View As' dropdown menu currently set to 'Standard Web Page'. Below these are three 'Sort Results By' dropdown menus, each currently set to 'Please Choose'. At the bottom right, there are 'Cancel' and 'Search' buttons.

This pane allows you to choose a reporting format and save the report so you can access it in the future. If you choose to save a report, you can perform the same search at a later date.

Saved computer searches can be accessed on the Computer Inventory pane. You can edit or delete a saved computer search by clicking the disclosure triangle next to the search and then clicking the **Edit** or **Delete** link.

## Criteria Pane

Field	Search Type	Criteria	-	+
		Computer Information		+
		Location Information		+
		Hardware Information		+
		Storage Information		+
		OS Configuration Information		+
		Software Information		+
		Purchasing Information		+
		Receipts Information		+
		Extension Attributes Information		+

This pane allows you to specify the attributes on which to base your search. These options are broken down into the following categories:

- Computer Information
- Location Information
- Hardware Information
- Storage Information
- OS Configuration Information
- Software Information
- Purchasing Information
- Receipts Information
- Extension Attributes Information (This category is only displayed if extension attributes are configured in your Inventory Collection preferences.)

## Display Fields Pane

General	Criteria	Display Fields	
<input checked="" type="checkbox"/> Info Link	<input type="checkbox"/> JSS Computer ID	<input type="checkbox"/> Asset Tag	<input type="checkbox"/> Platform
<input checked="" type="checkbox"/> Computer Name	<input type="checkbox"/> Bar Code	<input checked="" type="checkbox"/> Last Contact Time	<input type="checkbox"/> Last Report Date
<input checked="" type="checkbox"/> Managed	<input checked="" type="checkbox"/> jamf Binary Version	<input type="checkbox"/> IP Address	
<input checked="" type="checkbox"/> Username	<input checked="" type="checkbox"/> Real Name	<input checked="" type="checkbox"/> Email Address	<input type="checkbox"/> Department
<input checked="" type="checkbox"/> Building	<input type="checkbox"/> Room	<input type="checkbox"/> Phone	<input type="checkbox"/> Position
<input type="checkbox"/> Live LDAP Lookups			
<input type="checkbox"/> Make	<input checked="" type="checkbox"/> Model	<input type="checkbox"/> MAC Address	<input type="checkbox"/> NIC Speed
<input type="checkbox"/> Optical Drive	<input type="checkbox"/> Boot ROM	<input type="checkbox"/> Bus Speed	<input checked="" type="checkbox"/> Serial Number
<input type="checkbox"/> Processor Speed	<input type="checkbox"/> Number of Processors	<input type="checkbox"/> Processor Type	<input type="checkbox"/> Processor Architecture
<input type="checkbox"/> Total RAM	<input type="checkbox"/> Available RAM Slots	<input type="checkbox"/> SMC Version	<input type="checkbox"/> Battery Capacity
<input type="checkbox"/> Hard Drive Size	<input type="checkbox"/> SMART Status	<input type="checkbox"/> Boot Drive Full	
<input checked="" type="checkbox"/> Operating System	<input type="checkbox"/> Service Pack	<input type="checkbox"/> Active Directory Status	<input type="checkbox"/> Master Password Set
<input type="checkbox"/> FileVault Status	<input checked="" type="checkbox"/> SWU		
<input type="checkbox"/> Purchased/Leased	<input type="checkbox"/> PO Number	<input type="checkbox"/> PO Date	<input type="checkbox"/> Vendor
<input type="checkbox"/> Warranty Expires	<input type="checkbox"/> Lease Expires	<input type="checkbox"/> AppleCare ID	<input type="checkbox"/> Purchase Price
<input type="checkbox"/> Life Expectancy	<input type="checkbox"/> Purchasing Account	<input type="checkbox"/> Purchasing Contact	
<input type="checkbox"/> Active Network Interface	<input type="checkbox"/> Computer Sleep	<input type="checkbox"/> DNS Servers	<input type="checkbox"/> IP Geo-Location

This pane allows you to choose the attributes displayed in your search results when you view your search in one of the following reporting formats:

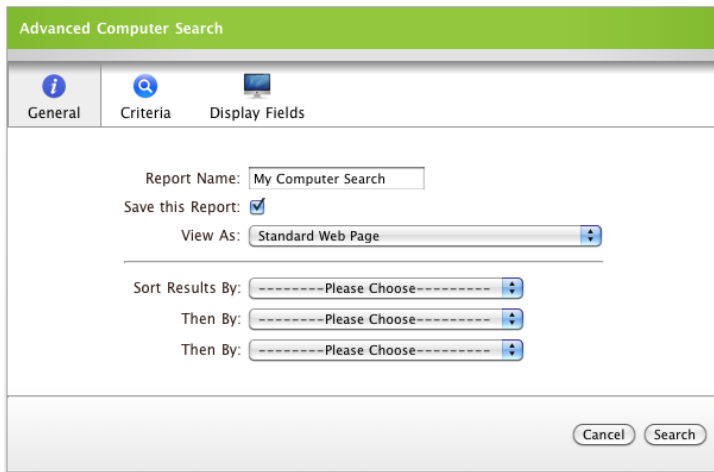
- Standard Webpage
- CSV
- Tab
- XML

You can change the default selections by changing your Inventory Display preferences. For more information on changing Inventory Display preferences, see the “Inventory Display Preferences” section.

### To perform an advanced computer search:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.  
The **Computers** link is selected by default.
3. Click the **Advanced Search** link.

4. If you want to save your search, enter a name for the report and select **Save this Report**.



5. Using the **View As** pop-up menu, choose the format in which you want to view the report.
6. If you want the results to be sorted, choose how you want them sorted using the **Sort Results By** pop-up menus.
7. Click the **Criteria** tab, and narrow your search by clicking the **Add (+)** button next to each search type that corresponds to the information that you want to use.  
A list of searchable items is displayed.
8. Click the items that you want to use in your search, and further specify the search criteria using the fields provided.
9. If you are viewing the report in a supported format, click the Display Fields pane and select the checkbox next to each attribute that you want displayed in your search results.
10. Click the **Search** button.



## Viewing Computer Search Results

By default, computer search results are displayed in Standard Webpage format. You can view the search results in any of the following alternate formats:

- Standard Webpage
- Computer Details (PDF)
- Computer Details Multipage (PDF)
- Computer Overview (PDF)
- Network Overview (PDF)
- Hardware Change Report (PDF)
- Software Change Report (PDF)
- Application Difference Report (PDF)
- Application Distribution Report (PDF)
- OS Distribution Report (PDF)
- System Security Report (PDF)
- CSV
- Tab
- XML

For simple computer searches, choose one of these options from the **View Results As** pop-up menu at the bottom of the results list. For advanced computer searches, choose one of these options from the **View As** pop-up menu on the General pane of the advanced search interface.


**Note:** The attributes displayed in simple computer search results are determined by your Inventory Display preferences. See the “Managing Inventory Attributes” section for more information. The attributes displayed in advanced computer search results are determined by the settings on the Display Fields pane of the advanced search interface. For more information, see “Performing Advanced Computer Searches”.

### Computer Details (PDF)

The Computer Details report displays an overview of each search result, one record per page. The Overview section contains information pertaining to physical location, hardware, and storage. The pie chart on the right side shows the percentage of the boot volume that is full. Matches for any licensed software are displayed in the licensed software section.

The rest of the report shows a list of non-suppressed applications. Since each computer record is limited to one page, the number of applications that are not displayed is noted at the bottom of the page.

Computer Details Report Generated for My Company




**BART** 02/25/2007 at 2:27 PM

---

**Overview**

Asset Tag	125883
Make/Model	Apple 13-inch MacBook
Serial Number	4H6382HGVMN
OS	Mac OS X 10.4.8
Boot Drive	[62% Full]
Processor Speed	2. GHz x2
Total RAM:	2 GB
Optical Drive	MATSHITA DVD-R UJ-857
Network	00.17.f2.2c.1b.1c [10/100/1000]



---

**Licensed Software**

Microsoft Office 2004

---

**Applications**

Acquisition.app	132.7
AirPort Disk Utility.app	1.0
AirPort Utility.app	5.0
Dis. Disc. & In. & Remov...	2.2

## Computer Details Multipage (PDF)


This report contains the same information as the Computer Details report, but it includes a complete list of applications as well.

## Computer Overview (PDF)

The Computer Overview report provides a simple report that details a limited number of attributes. This report displays the following fields for each computer:

- Computer Name
- Operating System
- User Information (including real name, username, and email address)
- Computer Model
- Computer Serial Number
- Processor Information
- RAM
- Hard Drive Size

Computer Overview Report Generated for My Company



Computer	OS	User	Model	Serial #	Processor	RAM	HD
JAMF-196	Mac OS X 10.3.9	Ahmad Jamal (ajamal) - ajamal@jamfsoftware.com	Power Mac G4 (QuickSilver)	XB240014MRN	867 MHz x1	512 MB	38.18 GB
JAMF-212	Mac OS X 10.4.5	Andre Previn (aprevin) - aprevin@jamfsoftware.com	iMac (Flat Panel)	QT306ZPB3U	800 MHz x1	512 MB	55.9 GB
JAMF-258	Mac OS X 10.3.5	Antonio Jobim (ajobim) - ajobim@jamfsoftware.com	iMac (Flat Panel)	W8306ZEBN3U	800 MHz x1	512 MB	55.9 GB
JAMF-522	Mac OS X 10.4.5	Art Blakey (ablakey) - ablakey@jamfsoftware.com	iMac Intel	QP606123U2S	2. GHz x2	1 GB	233.76 GB
JAMF-1864	Mac OS X 10.4.3	Art Pepper (apepper) - apepper@jamfsoftware.com	iMac G5	W844634XPNY	1.8 GHz x1	512 MB	74.53 GB
JAMF-524	Mac OS X 10.3.9	Art Taylor (ataylor) - ataylor@jamfsoftware.com	PowerBook G4 (15-inch 1.5/1.33 GHz)	W84340AFQHY	1.5 GHz x1	512 MB	74.53 GB
JAMF-254	Mac OS X 10.4.7	Bill Evans (bevans) - bevans@jamfsoftware.com	iMac (Flat Panel)	W8306ZDSN3U	800 MHz x1	512 MB	55.9 GB
JAMF-526	Mac OS X 10.4.7	Billy Martin (bmartin) - bmartin@jamfsoftware.com	MacBook Pro	W860914AVJ3	2. GHz x2	1 GB	93.16 GB
JAMF-246	Mac OS X 10.4.5	Billy Strayhorn (bstrayhorn) - bstrayhorn@jamfsoftware.com	iMac (Flat Panel)	W8306Z98N3U	800 MHz x1	512 MB	55.9 GB
JAMF-245	Mac OS X 10.3.5	Billy Taylor (btaylor) - btaylor@jamfsoftware.com	Power Mac G4 (QuickSilver)	XB302004MRN	867 MHz x1	512 MB	38.18 GB
JAMF-240	Mac OS X 10.3.9	Blossom Dearie (bdearie) - bdearie@jamfsoftware.com	17-inch iMac (Flat Panel)	QT2393M3N0S	800 MHz x1	256 MB	74.53 GB
JAMF-233	Mac OS X 10.2.8	Brad Mehldau (bmehldau) - bmehldau@jamfsoftware.com	iMac (version = 2.1)	W8306ZB3-N3U-ifi1	800 MHz x1	512 MB	
JAMF-2182	Mac OS X 10.4.6	Cannonball Adderley (cadderley) - cadderley@jamfsoftware.com	MacBook Pro	W86342A0VWY	2. GHz x2	1 GB	93.16 GB
JAMF-456	Mac OS X 10.4.6	Carl Allen (callen) - callen@jamfsoftware.com	Mac mini	YM524140RH5	1.42 GHz x1	1 GB	74.53 GB
JAMF-248	Mac OS X 10.3.4	Cedar Walton (cwalton) - cwalton@jamfsoftware.com	eMac	G8252521N8M	700 MHz x1	512 MB	38.16 GB
JAMF-344	Mac OS X 10.3.5	Charlie Haden (chaden) - chaden@jamfsoftware.com	iMac (Flat Panel)	W8306ZC4N3U	800 MHz x1	512 MB	55.9 GB


## Network Overview (PDF)

The Network Overview report breaks down your search results into six sections that address the following information:

- Computers per building
- Computers per department
- Total count of each unique operating system
- Total count of each unique computer model

- Total count of each version of /usr/sbin/jamf
- Count of errors that took place in the 12 hours before the report was printed

Network Overview Generated for My Company



Computers per Building		Operating Systems		/usr/sbin/jamf versions	
Hong Kong	11	Mac OS X 10.3.9	10	5.0	56
LA	15	Mac OS X 10.4.2	5		
na	30	Mac OS X 10.4.3	8		
		Mac OS X 10.4.5	8		
		Mac OS X 10.4.6	2		
		Mac OS X 10.4.7	23		

Computers per Department		Models		Errors in the last 12 hours	
Copy Writers	13	Apple 13-inch MacBook	2		
Finance	21	Apple 17-inch Mac (Flat Panel)	2		
PrePress	22	Apple iBook G3 (Early 2003)	1		
		Apple iMac (Flat Panel)	6		
		Apple iMac G5	2		
		Apple iMac G5 (Sight)	3		
		Apple iMac mini	5		
		Apple iMac mini	1		
		Apple MacBook Pro	3		
		Apple Power Mac G4 (AGP Graphics)	1		
		Apple Power Mac G4 (MD)	7		
		Apple Power Mac G4 (QuickSilver)	10		
		Apple Power Mac G5	10		
		Apple Power Macintosh G5 (Late 2005)	2		
		Apple PowerBook G4 (15-inch 1.5/1.33 GHz)	1		


## Hardware Change Report (PDF)

The Hardware Change report displays the changes that have taken place to the hardware configurations on your network over time. This information is especially useful when tracking down unauthorized changes.

The following hardware attributes are detailed in this report:

- NIC Speed
- Optical Drive
- Make
- Model
- Serial Number
- Processor Speed
- Number of Processors
- Total RAM
- Open RAM Slots
- Hard Drive Percentage Full

Report Generated for Internal Development



Hardware Changes for jamf0012


Report Date	NIC Speed	Optical	Make	Model	Serial #	Speed	Procs	RAM	Open	HD
2007-05-13 11:35:47.0	10/100/1000	MATSHITA DVD-R UJ-857	Apple	13-inch MacBook	4H6382H9VMN	2. GHz	2	1 GB	0	111.79 GB
2007-05-11 16:04:50.0	10/100/1000	MATSHITA DVD-R UJ-857	Apple	13-inch MacBook	4H6382H9VMN	2. GHz	2	2 GB	0	111.79 GB

Any changes to the hardware configurations that took place between reports will be highlighted in red. By comparing this data with the report dates in the first column, you will be able to determine the approximate date of the change.

## Software Change Report (PDF)

The Software Change report displays the changes that have taken place to the software installed on your computers over time. Anytime an application, font, or plug-in is added or removed from a computer, a record is logged. Changes to the operating system will also be displayed.

Software Change Report Generated for Internal Development



Software Changes for jam0012

Changes on 2007-05-13 16:04:57.0			
App Added	Microsoft Word	11.3.2	/Applications/Microsoft Office 2004/Microsoft Word
App Added	Microsoft PowerPoint	11.3.2	/Applications/Microsoft Office 2004/Microsoft PowerPoint
App Added	Microsoft Messenger.app	5.1.1	/Applications/Microsoft Office 2004/Microsoft Messenger.app
App Added	Microsoft Entourage	11.3.3	/Applications/Microsoft Office 2004/Microsoft Entourage
App Added	Microsoft Excel	11.3.2	/Applications/Microsoft Office 2004/Microsoft Excel
App Removed	QuarkXPress	QuarkXPress version	/Applications/QuarkXPress 6.0/QuarkXPress

## Application Difference Report (PDF)

The Application Difference report compares the software that is actually installed on a computer to what the JSS projects should exist on the computer.

There are two prerequisites to run this report:


- All of your packages must be indexed.
- Each computer you are generating the report for must contain Autorun data for the configuration and packages that should be installed.

The JSS references Autorun data to generate this report. Once it determines which packages should be installed on a computer, the JSS references the index of packages that are actually installed and generates a record of what the computer should look like.

Each Application Difference report is broken down into four sections that detail the following information:

- Overview of the computer
- A list of any unauthorized applications
- A list of any missing applications
- A list of any mismatched applications (versions are different)

Application Difference Report Generated for My Company



**JAMF-IMG** Data from 02/26/2007 at 9:30 PM

**Computer Overview**

Make/Model	Apple 13-inch MacBook	
Serial Number	4H6383FDU9D	
OS	Mac OS X 10.4.8	

**4 Unauthorized Applications**

MacBook EFI Firmware Update.app	1.0	
Parallels Transporter.app	2.0	Build 1078
Parallels Image Tool.app	2.5	
Parallels Desktop.app	2.5	


**2 Mis-Matched Applications**

iTunes.app	7.0.2	6.0.4
QuickTime Player.app	7.1.3	7.0.4 Pro

## Application Distribution Report (PDF)

The Application Distribution report displays a count of applications on your network, broken down by version.


For example, the data in the following screen shot reflects 19 copies of Adobe Photoshop from Creative Suite 1 and 215 copies of Adobe Photoshop from Creative Suite 2. We can see that only one person has updated to version 9.0.2, with 192 people using version 9.0.1 and 22 people using 9.0.

Application Distribution Report Generated for My Company 

Application Name	Copies	Total
<b>Adobe Photoshop CS.app</b>		
8.0 (8.0x119)	19	
	<b>Total Copies:</b>	<b>19</b>
<b>Adobe Photoshop CS2.app</b>		
9.0 (9.0x196)	22	
9.0.1 (9.0.1x294)	192	
9.0.2 (9.0.2x312) [20]	1	
	<b>Total Copies:</b>	<b>215</b>
<b>Adobe Reader 6.0.app</b>		
6.0	14	
6.0.2	1	
6.0.3	1	
6.0.4	1	
	<b>Total Copies:</b>	<b>17</b>

## Operating System Distribution Report (PDF)

The Operating System Distribution report displays a total count of each unique operating system on your network. It also breaks down the results for each department and building.

OS Distribution Report Generated for My Company 

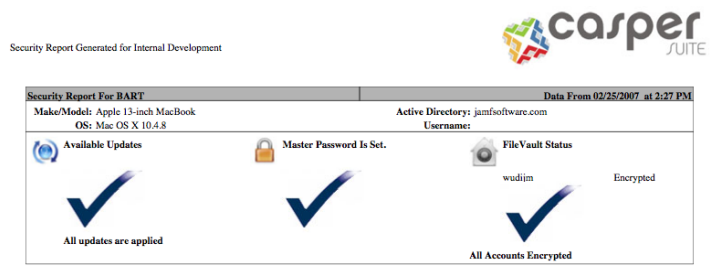
Operating System Name	Copies
Mac OS 9.1	1
Mac OS 9.2	9
Mac OS X 10.2.4	2
Mac OS X 10.2.6	3
Mac OS X 10.2.8	4
Mac OS X 10.3.2	4
Mac OS X 10.3.3	1
Mac OS X 10.3.4	2
Mac OS X 10.3.5	12
Mac OS X 10.3.6	1
Mac OS X 10.3.7	7
Mac OS X 10.3.8	3
Mac OS X 10.3.9	17
Mac OS X 10.4.2	18
Mac OS X 10.4.3	25
Mac OS X 10.4.4	1
Mac OS X 10.4.5	15
Mac OS X 10.4.6	4
Mac OS X 10.4.7	312
Mac OS X 10.4.8	2
Mac OS X Server 10.3.9	1
Mac OS X Server 10.4.3	1
Mac OS X Server 10.4.7	2
Mac OS X Server 10.4.9	1
Microsoft Windows XP Professional 5.1.2600	63
<b>Total Count:</b>	<b>511</b>

## System Security Report (PDF)

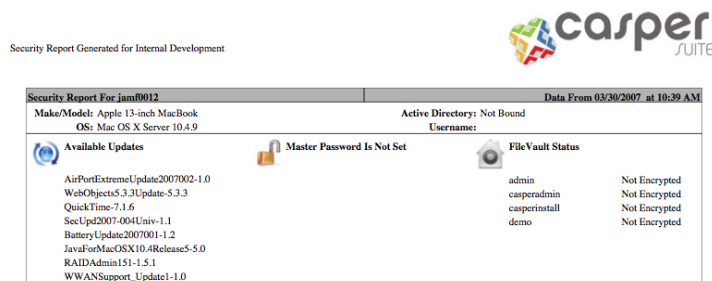
The System Security report displays security-related information for each computer. This report is broken down into four sections that detail the following information:

- Overview of the computer (including Active Directory status)
- List of available software updates
- Existence of a master password on the computer
- FileVault status for each account on the computer

The report for a computer that meets the criteria in each section will display blue checkmarks beneath the sections:



The report for a computer that does not meet the criteria will display the items that do not meet the criteria in the relevant section:



## CSV

This format exports your search results into a CSV file that you can open in Microsoft Excel and other spreadsheet applications.

## Tab

This format exports your search results into a tab-delimited text file that you can open in Microsoft Excel and other spreadsheet applications.

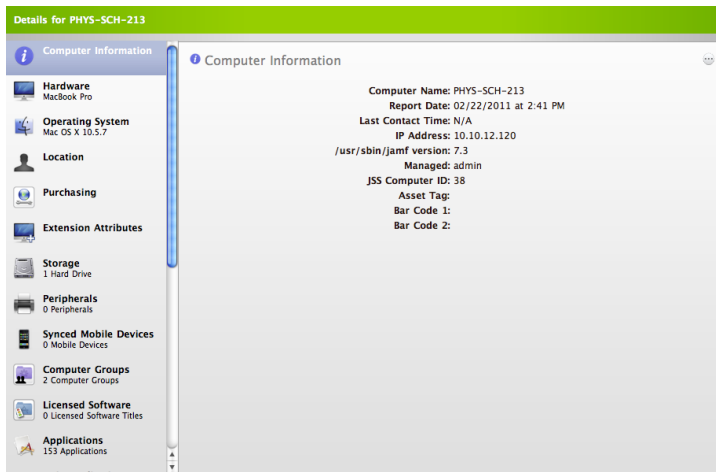
## XML

This format exports your search results into an XML file. XML files are commonly used to move data between applications.

## Viewing Computer Details

After performing a computer search, you can view a Details report for any search result by clicking the **Details** link across from it.

Details reports are broken down by category. Clicking a category in the sidebar displays related information in the category pane. Some panes allow you to perform actions, such as editing information, viewing history, and adding components.



The following table describes each category pane and the actions that you can perform from it:

Category	Description	Actions that you can perform
<b>Computer Information</b>	General information about the computer, including computer name, IP address, asset tag, management account, and date/time of last inventory report	Edit computer information Run a remote command (remote lock, remote unenroll, and remote wipe)
<b>Hardware</b>	Hardware information, including make, model, and MAC address(es)	Edit hardware information View hardware/software history
<b>Operating System</b>	Information about the operating system, including system and version number	--
<b>Location</b>	Information about the computer's physical location on the network	Edit location information Perform LDAP lookup View location history
<b>Purchasing</b>	Purchasing information for the computer, including PO details, warranty information, and purchasing contact	Edit purchasing information Perform GSX lookup
<b>Extension Attributes</b>	Extension attributes collected from the computer	Edit values for non-script extension attributes
<b>Storage</b>	Storage information for each drive	--

Category	Description	Actions that you can perform
<b>Peripherals</b>	A list of peripherals associated with the computer	Add peripheral Delete peripheral View peripheral details
<b>Synced Mobile Devices</b>	Information about mobile devices synced with the computer	View mobile device details
<b>Computer Groups</b>	A list of groups that the computer is a member of	--
<b>Licensed Software</b>	A list of licensed software titles installed on the computer	--
<b>Applications</b>	A list of applications installed on the computer	View application details
<b>UNIX Applications</b>	A list of UNIX applications installed on the computer	View UNIX application details
<b>Fonts</b>	A list of fonts installed on the computer	--
<b>Plug-ins</b>	A list of plug-ins installed on the computer	--
<b>Management History</b>	A list of management commands run on the computer	Update management history Cancel a remote command that is pending
<b>Package Receipts</b>	A list of packages installed or cached by the Casper Suite A list of packages installed by Installer.app or Software Update	--
<b>Software Updates</b>	A list of available software updates	--
<b>Local User Accounts</b>	A list of local user accounts and information about them, including username, real name, UID, and Home directory	--
<b>Printers</b>	A list of printers mapped to the computer	--
<b>Services</b>	A list of active services	--
<b>UNIX Reports</b>	Results for the following UNIX commands run by Recon: uptime - Length of time since last reboot w - List of user that are logged in top - Snapshot of processes that are running	--
<b>Attachments</b>	A list of files attached to the inventory record	Upload attachments

**Note:** For instructions on how to suppress applications, fonts, plug-ins, UNIX executables, or accounts from inventory reports, see the “Suppressing Software from Reports” section.



# Searching Peripherals

Once peripherals are added to the JAMF Software Server (JSS), they can be viewed for inventory or reporting purposes.

This section explains how to:

- Perform simple and advanced peripheral searches
- View peripheral search results
- View peripheral details

## Performing Simple Peripheral Searches

A simple peripheral search functions like a search engine, allowing you to locate a general range of results quickly and easily.

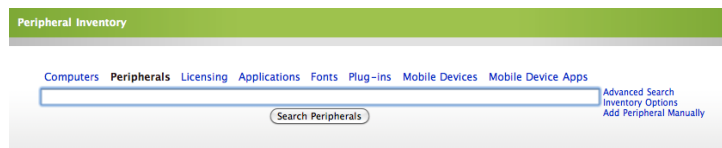
Simple searches can be performed based on the following attributes of a peripheral:

- Peripheral type
- Customizable peripheral fields
- Bar code
- Username
- Real name
- Email address
- Phone number
- Position
- Department
- Building
- Room
- Name of the computer the peripheral is attached to

**Note:** Performing an empty search (with no criteria in the search field) returns all of the peripherals in your database.

**To perform a simple peripheral search:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Peripherals** link.



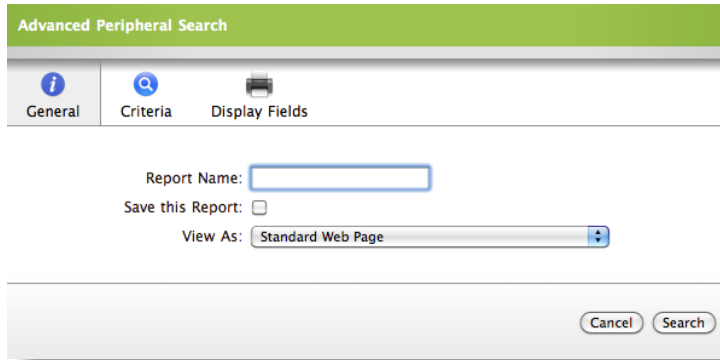
4. Enter one or more search terms into the search field.
5. Click the **Search Peripherals** button, or press the Enter key.

# Performing Advanced Peripheral Searches

When used to search for peripherals and create reports, advanced searches offer a variety of powerful options. The advanced peripheral search interface consists of three navigation panes: General, Criteria, and Display Fields.

A detailed description of the information on each pane follows:

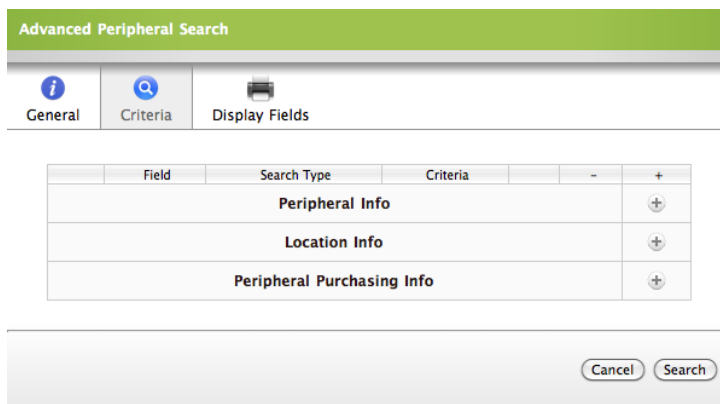
## General Pane



This pane allows you to choose a reporting format and save the report so you can access it in the future. If you choose to save a report, you can perform the same search at a later date.

Saved peripheral searches can be accessed on the Peripheral Inventory pane. You can edit or delete a saved peripheral search by clicking the disclosure triangle next to the search and then clicking the **Edit** or **Delete** link.

## Criteria Pane



This pane allows you to specify the attributes on which to base your search. These options are broken down into the following categories:

- Peripheral Info
- Location Info
- Purchasing Info

## Display Fields Pane

Advanced Peripheral Search

General Criteria Display Fields

Username  Real Name  Email Address  Department  
 Building  Room  Phone  Position  
 Live LDAP Lookups

Purchased/Leased  PO Number  PO Date  Vendor  
 Warranty Expires  Lease Expires  AppleCare ID  Purchase Price  
 Life Expectancy  Purchasing Account  Purchasing Contact

Cancel Search

This pane allows you to specify the attributes displayed in your search results.

You can change the default selections by changing your Inventory Display preferences. For more information on changing Inventory Display preferences, see the “Inventory Display Preferences” section.

### To perform an advanced peripheral search:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Peripherals** link.
4. Click the **Advanced Search** link.
5. If you want to save your search, enter a name for the report and select the **Save this Report** checkbox.

Advanced Peripheral Search

General Criteria Display Fields

Report Name:

Save this Report:

View As:

Cancel Search

6. Using the **View As** pop-up menu, choose the format in which you want to view the report.
7. Click the **Criteria** tab, and narrow your search by clicking the **Add (+)** button next to each search type that corresponds to the information that you want to use.  
A list of searchable items is displayed.
8. Click the items that you want to use in your search, and further specify the search criteria using the fields provided.

9. Click the **Display Fields** tab and select the checkbox next to each attribute that you want displayed in your search results.
10. Click the **Search** button.

## Viewing Peripheral Search Results

By default, peripheral search results are displayed in Standard Webpage format. You can view the search results in any of the following alternate formats:

- CSV
- Tab
- XML

For simple peripheral searches, choose one of these options from the **View Results As** pop-up menu at the bottom of the results list. For advanced peripheral searches, choose one of these options from the **View As** pop-up menu on the General pane of the advanced search interface.

**Note:** The attributes displayed in simple peripheral search results are determined by your Inventory Display preferences. See the “Managing Inventory Attributes” section for more information. The attributes displayed in advanced peripheral search results are determined by the settings on the Display Fields pane of the advanced search interface. For more information, see “Performing Advanced Peripheral Searches”.

### CSV

This format exports your search results into a CSV file that you can open in Microsoft Excel and other spreadsheet applications.

### Tab

This format exports your search results into a tab-delimited text file that you can open in Microsoft Excel and other spreadsheet applications.

### XML

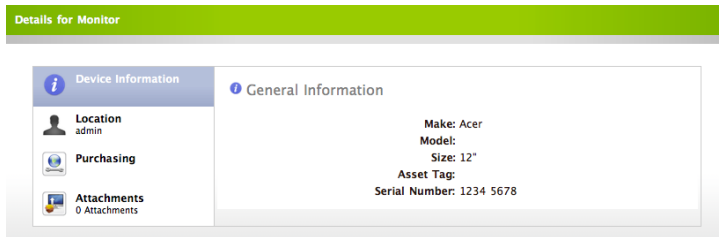
This format exports your search results into an XML file. XML files are commonly used to move data between applications.

## Viewing Peripheral Details

After performing a peripheral search, you can view details for any peripheral returned in the search by clicking the **Details** link across from it.

Peripheral reports are broken down into four sections:

- Device Information
- Location
- Purchasing
- Attachments



# Searching Software Inventory

Once you acquire computers, you can search and view installed applications, fonts, and plug-ins.

This section explains how to:

- Perform simple and advanced software searches
- View software search results

## Performing Simple Software Searches

A simple software search functions like a search engine, allowing you to locate a general range of results quickly and easily.

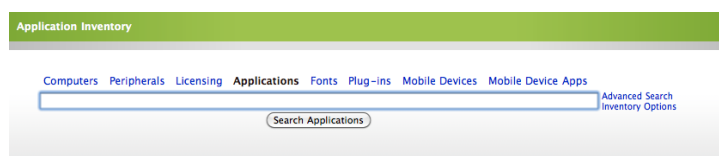
Simple searches can be performed based on the following attributes of a software record:

- Application Title
- Application Version

**Note:** Performing an empty search (with no criteria in the search field) does not return any results. Search criteria are required to search for software.

**To perform a simple software search:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Applications, Fonts, or Plug-ins** link.



4. Enter one or more search terms into the search field.
5. Click the **Search** button, or press the Enter key.

## Performing Advanced Software Searches

Advanced software searches offer you a variety of powerful options. The advanced software search interface consists of three navigation panes: General, Criteria, and Display Fields.

A detailed description of the information on each pane follows:

## General Pane

The screenshot shows the 'General' pane of the 'Advanced Application Search' window. It features a green header bar with the title 'Advanced Application Search'. Below the header is a navigation bar with three tabs: 'General' (selected), 'Criteria', and 'Display Fields'. The main area contains a 'Report Name' text input field, a 'Save this Report' checkbox, and a 'View As' dropdown menu currently set to 'Standard Web Page'. At the bottom right, there are 'Cancel' and 'Search' buttons.

This pane allows you to choose a reporting format and save the report so you can access it in the future. If you choose to save a report, you can perform the same search at a later date.

Saved software searches can be accessed on the Computer Inventory pane. You can edit or delete a saved software search by clicking the disclosure triangle next to the search and then clicking the **Edit** or **Delete** link.

## Criteria Pane

The screenshot shows the 'Criteria' pane of the 'Advanced Application Search' window. It features a green header bar with the title 'Advanced Application Search'. Below the header is a navigation bar with three tabs: 'General', 'Criteria' (selected), and 'Display Fields'. The main area contains search criteria fields: 'Platform' with a dropdown menu set to 'Any', 'Application Name' with a 'like' dropdown and an input field, and 'Application Version' with a 'like' dropdown and an input field. At the bottom right, there are 'Cancel' and 'Search' buttons.

This pane allows you to specify the attributes on which to base your search. These options are broken down into the following categories:

- Platform
- Application Title
- Application Version

## Display Fields Pane

Advanced Application Search

General Criteria **Display Fields**

Application Path  Size  Copyright  Date Modified  
 Bundle ID  Permissions  Registered To  Company  
 Serial Number 1  Serial Number 2

Info Link  JSS Computer ID  Asset Tag  Platform  
 Computer Name  Bar Code  Last Contact Time  Last Report Date  
 Managed  Jamf Binary Version  IP Address

Username  Real Name  Email Address  Department  
 Building  Room  Phone  Position  
 Live LDAP Lookups

Make  Model  MAC Address  NIC Speed  
 Optical Drive  Boot ROM  Serial Number  Processor Speed  
 Number of Processors  Processor Type  Processor Architecture  Total RAM  
 Available RAM Slots  SMC Version  Battery Capacity

Hard Drive Size  SMART Status  Boot Drive Full

Operating System  Service Pack  Active Directory Status  Master Password Set  
 FileVault Status  Number of Available Updates

Purchased/Leased  PO Number  PO Date  Vendor  
 Warranty Expires  Lease Expires  AppleCare ID  OS AppleCare ID  
 OS Maintenance Expires  Purchase Price  Life Expectancy  Purchasing Account  
 Purchasing Contact

Cancel Search

This pane allows you to specify the attributes displayed in your search results when you view your search in one of the following reporting formats:

- Standard Webpage
- CSV
- Tab
- XML

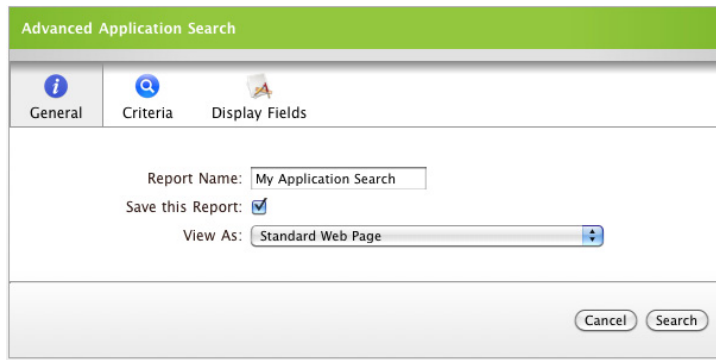
You can change the default selections by changing your Inventory Display preferences. For more information on changing Inventory Display preferences, see the “Inventory Display Preferences” section.

### To perform an advanced software search:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Applications, Fonts, or Plug-ins** link.
4. Click the **Advanced Search** link.
5. If you want to save your search, enter a name for the report and select the **Save this Report** checkbox.



- Using the **View As** pop-up menu, choose the format in which you want to view the report.



- Click the **Criteria** tab, and narrow your search by clicking the **Add (+)** button next to each search type that corresponds to the information that you want to use.  
A list of searchable items is displayed.
- Select each item that you want to use in your search, and further specify the search criteria using the fields provided.
- Click the **Display Fields** tab, and select the checkbox next to each attribute that you want displayed in your search results.
- Click the **Search** button.

## Viewing Software Search Results

By default, software search results are displayed in Standard Webpage format. You can view the search results for advanced software searches in any of the following alternate formats by choosing from the **View As** pop-up menu on the General pane of the advanced search interface:

- CSV
- Tab
- XML

**Note:** The attributes displayed in advanced software search results are determined by the settings on the Display Fields pane of the advanced search interface. For more information, see “Performing Advanced Software Searches”.

### CSV

This format exports your search results into a CSV file that you can open in Microsoft Excel and other spreadsheet applications.

### Tab

This format exports your search results into a tab-delimited text file that you can open in Microsoft Excel and other spreadsheet applications.

## XML

This format exports your search results into an XML file. XML files are commonly used to move data between applications.

# Performing Mass Actions on Computer Search Results

Mass actions are a quick way to perform the following tasks on the results of a computer search:

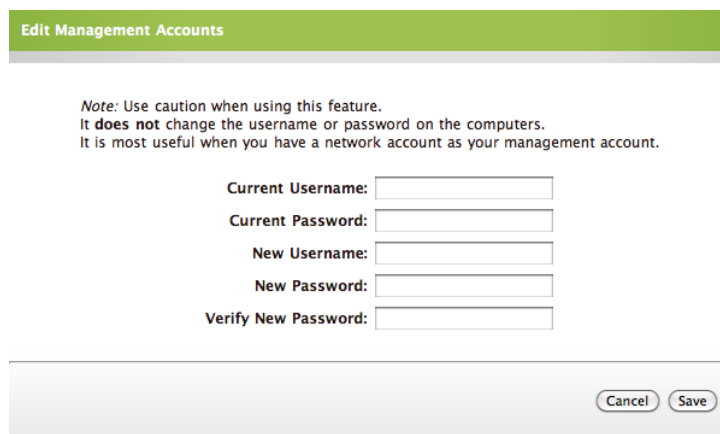
- Edit management accounts.
- Edit the building, department, or servers.
- Edit and delete Autorun data.
- Look up and populate purchasing information from Apple's Global Service Exchange (GSX).
- Email users.
- Delete from the JAMF Software Server (JSS).

## Mass Editing Management Accounts

This allows you to change management account information for all results of a computer search. This is useful when the management account is from a directory service and the account has been changed.

**To mass edit management accounts:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Choose "Edit Management Accounts" from the **Take Action on Results** pop-up menu. Then, click **Go**.
5. Enter the username and password for the current management account.



**Edit Management Accounts**

*Note: Use caution when using this feature. It does not change the username or password on the computers. It is most useful when you have a network account as your management account.*

Current Username:

Current Password:

New Username:

New Password:

Verify New Password:

Cancel Save

6. Enter the username and password for the new management account. Then, enter the password again to verify it.
7. Click the **Save** button.

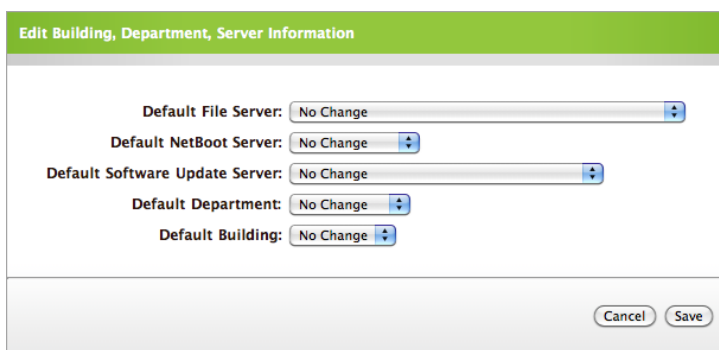
8. Click **Continue** to confirm the change.

## Mass Editing Building, Department, or Servers

This allows you to edit location information and change the primary distribution point, NetBoot Server, and Software Update server for all results of a computer search.

**To mass edit the building, department, or servers:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Choose "Edit Building, Department, or Servers" from the **Take Action on Results** pop-up menu. Then, click **Go**.
5. Use the pop-up menus to specify new location and server information as needed.



The screenshot shows a dialog box titled "Edit Building, Department, Server Information". It contains five dropdown menus, each with "No Change" selected. The dropdowns are: Default File Server, Default NetBoot Server, Default Software Update Server, Default Department, and Default Building. At the bottom right of the dialog are "Cancel" and "Save" buttons.

6. Click the **Save** button.
7. Click **Continue** to confirm the change.

## Mass Editing and Mass Deleting Autorun Data

This allows you to edit or delete Autorun data for all results of a computer search.

**To mass edit or mass delete Autorun data:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Choose "Edit Autorun Data" from the **Take Action on Results** pop-up menu. Then, click **Go**.

5. If you want to edit the Autorun data, configure new settings as needed and click the **Apply Changes** button.

If you want to delete the Autorun data, click the **Delete Autorun Data for these Computers** button and click **OK** when prompted.

**Edit Autorun Data**

**Install**

Target Drive: Macintosh HD

Erase Target Drive

Configuration: Empty

Reboot To Target Drive When Done

Local Username:

Local Password:

**JAMF Software Server Options**

Store on JSS  Cache Packages

Run Automatically  Ignore Delay

Distribution Point: phineas.jamfsw.corp (afp://phineas.jamfsw.corp/CasperShare)

Delete Autorun Data for these Computers Cancel Apply Changes

6. Click **Continue** to confirm the changes.

## Mass Look up Purchasing Information from GSX

This allows you to look up and populate purchasing information from Apple's Global Service Exchange (GSX).

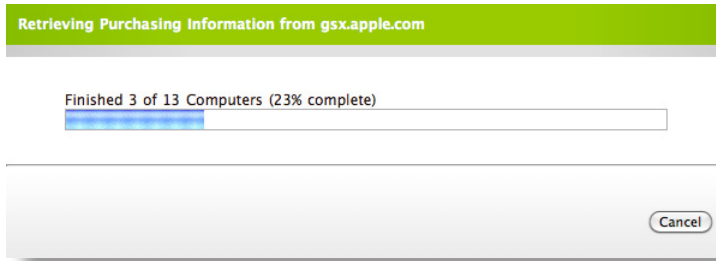
To utilize this feature, a GSX connection must be set up in the JSS. For more information on setting up this connection, see the section entitled "Integrating with GSX".

**Note:** GSX lookups may not always return complete purchasing information. The lookup only returns information available in GSX.

### To perform a mass GSX lookup:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.

4. Choose “Look up Purchasing Info in GSX” from the **Take Action on Results** pop-up menu. Then, click **Go**. The progress of the lookup is displayed onscreen.



5. When the results are displayed, click the **Update Records** button to populate the information in the JSS. Then, click **Continue** to confirm.  
If the results state that the JSS is already up-to-date, click the **Cancel** button.

## Mass Emailing Users

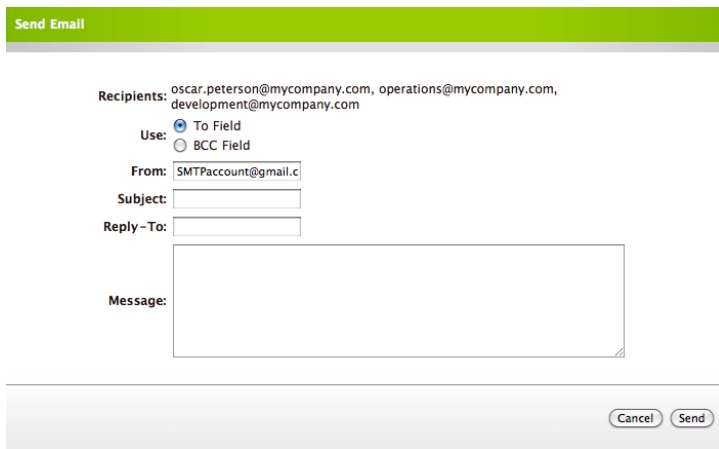
Mass emails are a convenient way to notify users of an upcoming software upgrade, a full drive, or another issue.

Mass emails are sent from the SMTP server that is specified in the JSS. If you have not specified an SMTP server, see the section entitled “Enabling Email Notifications” for instructions on how to do so.

### To mass email users:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Choose “Send Email” from the **Take Action on Results** pop-up menu. Then, click **Go**.

5. Use the options and fields provided to compose the email message.  
The email address you send the message from must be associated with the SMTP server in the JSS. Replies are also sent to this address unless you specify otherwise.



The screenshot shows a 'Send Email' dialog box with a green header. The 'Recipients' field contains 'oscar.peterson@mycompany.com, operations@mycompany.com, development@mycompany.com'. The 'Use:' section has two radio buttons: 'To Field' (selected) and 'BCC Field'. The 'From:' field contains 'SMTPAccount@gmail.c'. There are empty input fields for 'Subject:' and 'Reply-To:'. A large text area labeled 'Message:' is below these fields. At the bottom right, there are 'Cancel' and 'Send' buttons.

6. Click the **Send** button.
7. Click **Continue** to confirm.

## Mass Deleting Computers

You can remove computers from your inventory by deleting them from the JSS.

### To mass delete computers from the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Choose "Delete Computers" from the **Take Action on Results** pop-up menu. Then, click **Go**.
5. Click the **Delete Permanently** button; or if peripherals are associated with one or more of the computers, click the **Delete Computers Only** or **Delete Computers and Peripherals** button.
6. Click **Continue** to confirm the deletion.

# Editing Computer Records

The JAMF Software Server (JSS) allows you to edit the following information:

- General information, including the management account
- MAC address(es)
- Location information
- Purchasing information
- Non-script extension attributes

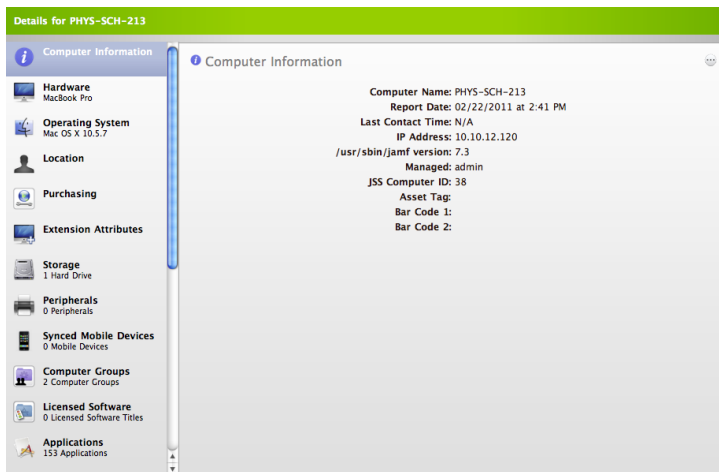
**To edit a computer record:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Click **Details** across from the computer record you want to edit.
5. Click the category you want to edit in the categories list.

The following categories contain editable information:


- Computer Information
- Hardware
- Location
- Purchasing
- Extension Attributes

6. Click the **Ellipsis**  button to display the editable fields.

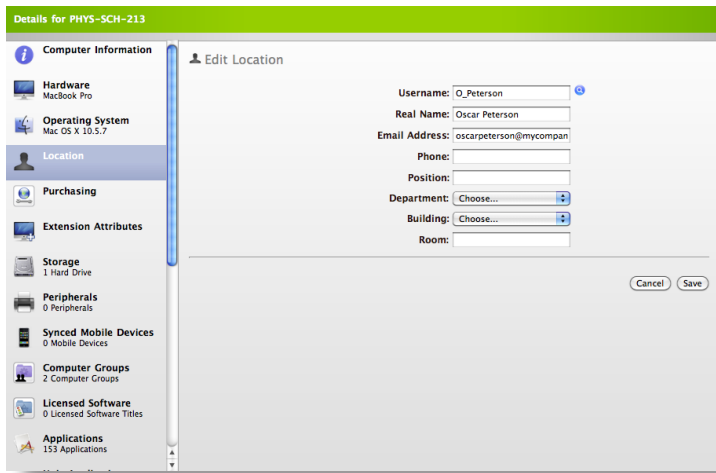




7. Add or modify information as needed.

If you are editing location or purchasing information, click the **Search**  icon to perform an LDAP or GSX lookup. This populates the fields with information from an LDAP server or Apple's Global Service Exchange (GSX).

**Note:** The lookup feature is only available if an LDAP server and/or GSX connection is set up in the JSS. For more information on setting up these connections, see the "Integrating with LDAP Servers" and "Integrating with GSX" sections.



8. Click **Save**.

# Deleting Computers from the JSS

You can remove a computer from your inventory by deleting it from the JAMF Software Server (JSS).

## To delete a computer from the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Click **Delete** across from the computer record.
5. Click the **Delete Permanently** button; or if peripherals are associated with the computer, click the **Delete Computers Only** or **Delete Computers and Peripherals** button.

# Creating Computer Groups

Computer groups offer an easy way to identify and manage clients that share common attributes or meet custom criteria. You can use these groups to assign computers to a policy's scope and track clients for reporting purposes.

The JAMF Software Server (JSS) allows you to create two kinds of computer groups: smart computer groups and static computer groups. Smart computer groups are based on inventory attributes and have dynamic group membership. This means that group membership changes automatically anytime a change in criteria or client inventory occurs. Conversely, static computer groups are hardcoded and have fixed memberships that can only be changed by an administrator.

Only enrolled computers can be members of a computer group.

This section explains how to create two kinds of computer groups:

- A smart computer group
- A static computer group

## To create a smart computer group:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Smart Computer Groups** link.
4. Click the **Create Smart Group** button in the toolbar.
5. Enter a name for the group in the **Computer Group Name** field.

ComputerGroup Name:

Send Email Notification on Change:

Field	Search Type	Criteria	-	+
Computer Information				+
Location Information				+
Hardware Information				+
Storage Information				+
OS Configuration Information				+
Software Information				+
Purchasing Information				+
Receipts Information				+

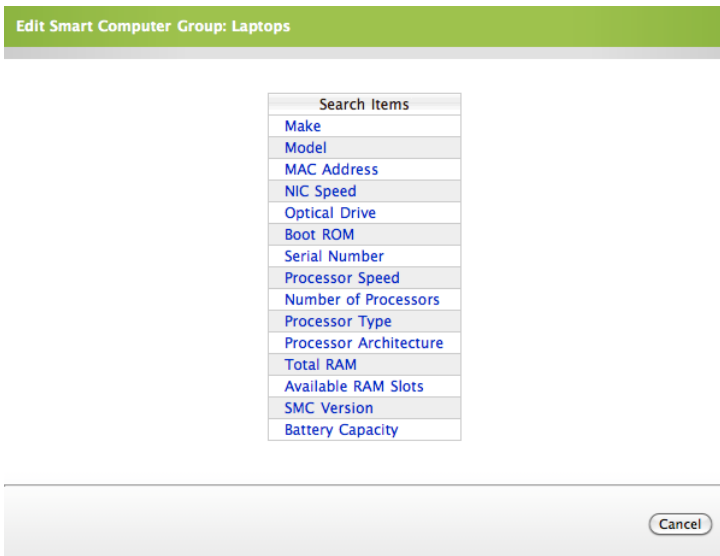
Cancel Save

- To send an email notification to administrators when membership changes occur, select the **Send Email Notification on Change** option.

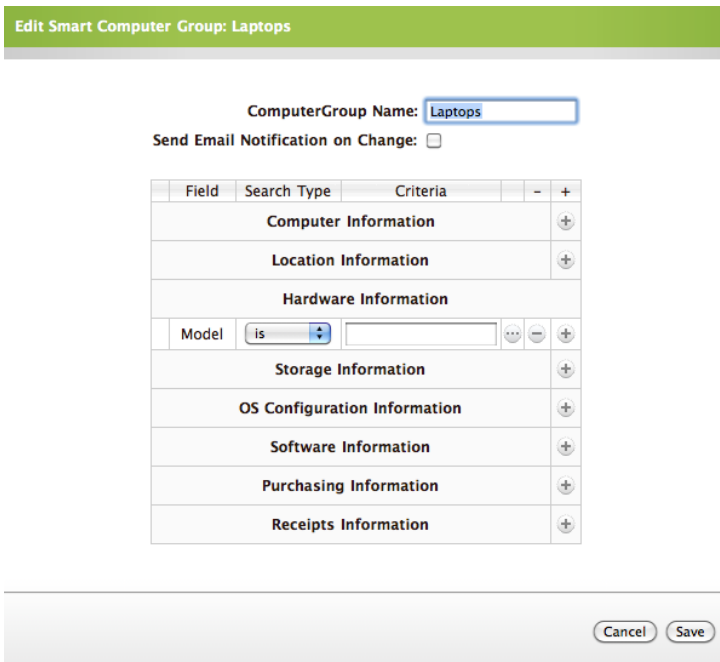
The JSS sends email notifications to the email addresses for accounts that have smart computer group email privileges enabled.

**Note:** An SMTP server must be set up in the JSS to send email notifications. For information on how to set up an SMTP server, see the “Enabling Email Notifications” section of this guide.

- Click the **Add (+)** button next to the category on which you want to base the group.
- Click the item on which you want to base the group.



- Specify group criteria by choosing a value from the **Search Type** pop-up menu and entering criteria in the text field.



10. Repeat steps 7 through 9 as needed.
11. Click the **Save** button.

**To create a static computer group:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Static Computer Groups** link.
4. Click the **Create Static Group** button in the toolbar.
5. Enter a name for the group in the **Computer Group Name** field.

The screenshot shows a dialog box titled "Edit Static Computer Group:". It contains a text input field labeled "Computer Group Name". Below this is a table with the following data:

Computer Name	User	Department	Building	
MyCompany0001				<input type="checkbox"/>
MyCompany0002				<input type="checkbox"/>
MyCompany0003				<input type="checkbox"/>
MyCompany0004				<input type="checkbox"/>
MyCompany0005				<input type="checkbox"/>

At the bottom right of the dialog box are two buttons: "Cancel" and "Save".

6. Select the checkbox next to each computer you want to include, and then click the **Save** button.

# Suppressing Software from Reports

Inventory reports may include a large number of insignificant software titles. You can suppress one or more software titles from the following categories:

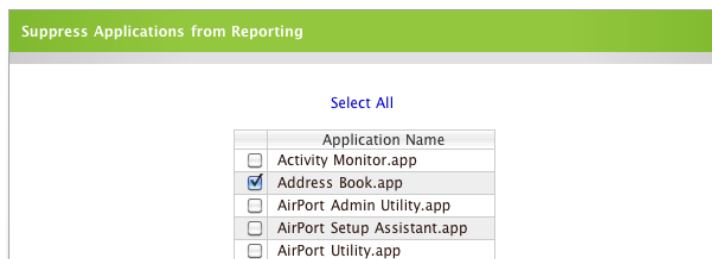
- Applications
- Fonts
- Plug-ins
- UNIX Executables
- Accounts

This section explains how to:

- Suppress software
- Unsuppress software

## To suppress software from reports:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. In the **Suppress Inventory Items** category, click the link that indicates the item(s) you want to suppress.
5. Select the checkbox next to each title you want to suppress, or click the **Select All** link to suppress all of the titles.



6. Click the **Suppress Selected** button at the bottom of the page.

## To unsuppress software from reports:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. In the **Unsuppress Inventory Items** category, click the link that indicates the item(s) you want to suppress.
5. Select the checkbox next to each title you want to unsuppress, or click the **Select All** link to suppress all of the titles.
6. Click the **Unsuppress Selected** button at the bottom of the page.

# Viewing Receipts

The JAMF Software Server (JSS) generates a receipt when changes are made to the following items in a computer's inventory record:

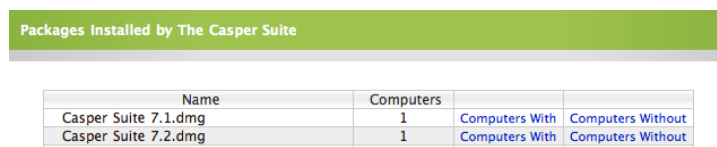
- Packages installed by the Casper Suite
- Packages installed by `Installer.app` or Apple's Software Update
- Packages the Casper Suite has cached and is waiting to install
- Updates available through Software Update
- Local user accounts that reside in NetInfo on client computers
- Services running on client computers

In order for the JSS to collect these receipts, the appropriate receipt type must be enabled. This can be done on the Settings pane in the JSS using the **Inventory Options** link.

You can also create smart computer groups based on client computers that do or do not have certain receipts.

## To view receipts:

1. Log in to the JSS with a web browser.
2. Click the **Logs** tab.
3. Click the link for the type of receipt that you want to view.  
This displays a list of the receipts on your network.



Packages Installed by The Casper Suite			
Name	Computers	Computers With	Computers Without
Casper Suite 7.1.dmg	1	<a href="#">Computers With</a>	<a href="#">Computers Without</a>
Casper Suite 7.2.dmg	1	<a href="#">Computers With</a>	<a href="#">Computers Without</a>

4. Click the **Computers With** link to display a list of computers that have the receipt.

**Note:** When viewing receipts for Software Updates, you can click the **Computers With** link to see a list of client computers that have the update available.

5. Click the **Computers Without** link to see a list of client computers that do not have the receipt.

# Managing Custom Reports

You can add custom reports to the JSS to extend your inventory reporting capabilities.

These reports are available when using the Inventory pane in the JAMF Software Server (JSS) to search or browse computers. A link for each custom report is displayed near the bottom of the page under the Export Options heading.

The Casper Suite comes with several templates that you can use to create custom reports. These templates are simple JSP files. They are located in:

```
/Library/JSS/Tomcat/webapps/ROOT/WEB-INF/reporting/
```

**Note:** If you upgraded from Casper Suite v8.1 or earlier, the custom report templates are located in:

```
/Library/Tomcat/webapps/ROOT/WEB-INF/reporting/
```

Before modifying these templates, be sure to read and respect the comments in the files.

This section explains how to create, edit, and delete a custom report.

## To create a custom report:

1. Create a JSP file (using one of the templates or otherwise) and place it in the following location on the server:

```
/Library/JSS/Tomcat/webapps/ROOT/WEB-INF/reporting/
```

**Note:** If you upgraded from Casper Suite v8.1 or earlier, place the file in this location:

```
/Library/Tomcat/webapps/ROOT/WEB-INF/reporting/
```

2. Place any image files for the report (.gif, .jpg, etc.) in the following location:

```
/Library/JSS/Tomcat/webapps/ROOT/reporting_images/
```

**Note:** If you upgraded from Casper Suite v8.1 or earlier, place the image files in this location:

```
/Library/Tomcat/webapps/ROOT/reporting_images/
```

3. Place any CSS (Cascading Style Sheet) files for the report in the following location:

```
/Library/JSS/Tomcat/webapps/ROOT/reporting_theme/
```

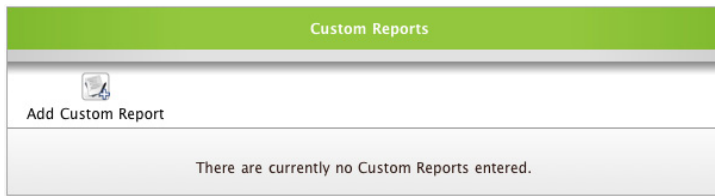
**Note:** If you upgraded from Casper Suite v8.1 or earlier, place the CSS files in this location:

```
/Library/Tomcat/webapps/ROOT/reporting_theme/
```

4. Log in to the JSS with a web browser.
5. Click the **Settings** tab.



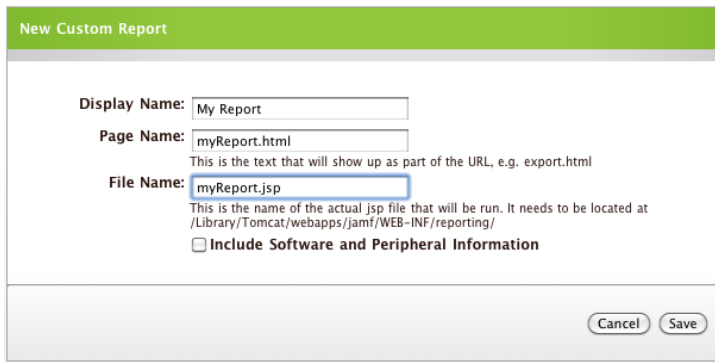
6. Click the **Inventory Options** link.
7. Click the **Custom Reports** link.
8. Click **Add Custom Report** in the toolbar.



9. Enter a display name for the report. For example, "My Report".
10. In the **Page Name** field, enter a name for the page that will display in your web browser each time you create a report.  
This name does not need to match the name of the JSP file.

**Note:** This name cannot contain spaces.

11. Enter the name of the JSP file in the **File Name** field.  
This must match the name of the JSP file exactly.



12. Select the **Include Software and Peripheral Information** checkbox to include software and peripheral information in the report.

**Note:** Selecting this option may delay the reporting process since it contains more information.

13. Click the **Save** button.

#### To edit a custom report:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Custom Reports** link.
5. Click the **Edit Report** link across from the report you want to edit.

6. Make changes as needed.
7. Click the **Save** button.

**To delete a custom report:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Custom Reports** link.
5. Click the **Delete Report** link.
6. Click **Delete Custom Report** to confirm.

---

# Imaging

## Overview of the Imaging Process

This section provides information about each component of the imaging process.

### Configurations

Configurations are sets of packages, scripts, printers, and directory bindings that make up an image. Configurations allow you to quickly specify what needs to be installed on a computer and make updates without rebuilding an entire image.

### Smart Configurations

Smart configurations give you the ability to create similar configurations quickly by creating configurations that inherit the components of other configurations. You can then assign additional packages, scripts, printers, and directory bindings as needed.

### Compiled Configurations

Compiled configurations speed up the imaging process by building a single DMG that includes each component in a configuration.

### Partitioning

In addition to packages, scripts, printers, and directory bindings, configurations can contain partitioning information.

Secondary partitions can be dynamically sized based on the target drive and can receive the following payloads:

- A configuration
- A Restore partition (Casper Imaging automatically converts an OS package to a Restore partition.)
- A Winclone image
- Nothing

As a safety mechanism, drives that contain multiple pre-configured partitions are not repartitioned; however, secondary partitions can be set up to re-image the partition if it already exists.

## Restore Partitions

Restore partitions are hidden partitions that allow you to re-image a computer using less network overhead. These partitions function as an alternative to NetBoot or USB/FireWire drives.

In lab environments, Restore partitions allow for fully automated re-imaging of computers. They can also cache packages and scripts locally to reduce the stress on your distribution points.

# Managing Configurations

This section explains how to:

- Create configurations
- Create smart configurations
- Compile configurations
- Delete configurations

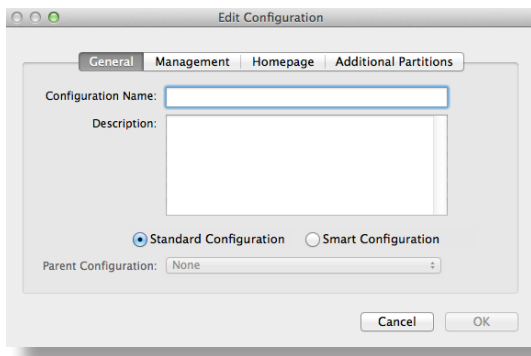
## Creating Configurations

This section explains how to use Casper Admin or the JAMF Software Server (JSS) to:

- Create a configuration
- Set up partitioning

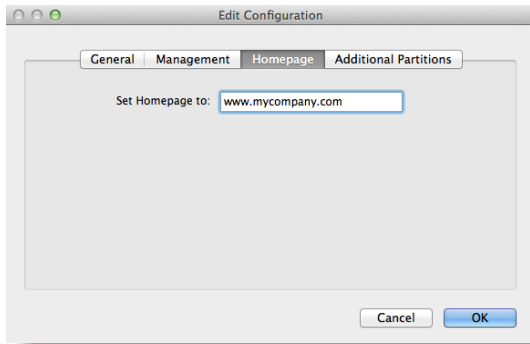
**To create a configuration using Casper Admin:**

1. Open Casper Admin.
2. Click the **New Config** button in the toolbar.
3. Enter a name for the configuration.



4. (Optional) Enter a description of the configuration.
5. If you want to set a default homepage for the clients:
  - a. Click the **Homepage** tab.
  - b. Enter the web address for the homepage.

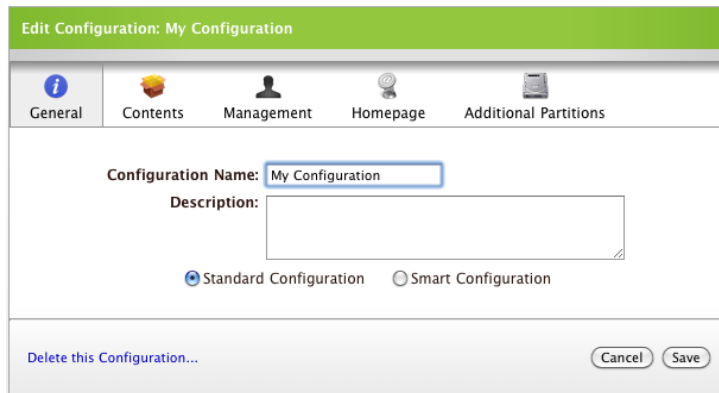
c. Click **OK**.



6. To add packages, scripts, printers, and directory bindings, drag them from the list in the main pane to the configuration in the sidebar.

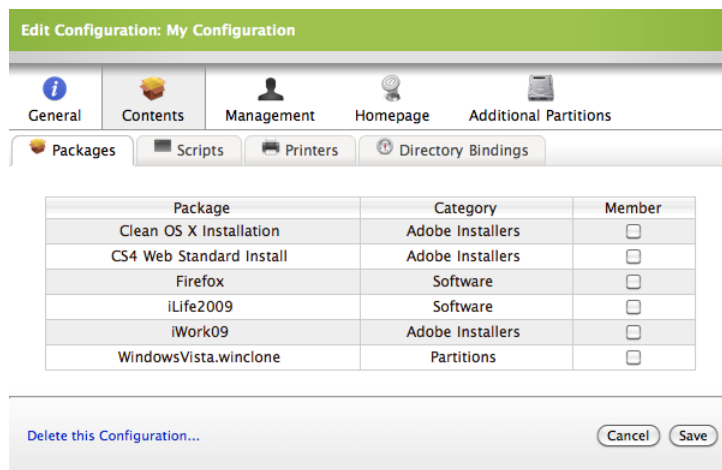
**To create a configuration using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Config** button in the toolbar.
5. Enter a name for the configuration.
6. (Optional) Enter a description of the configuration.

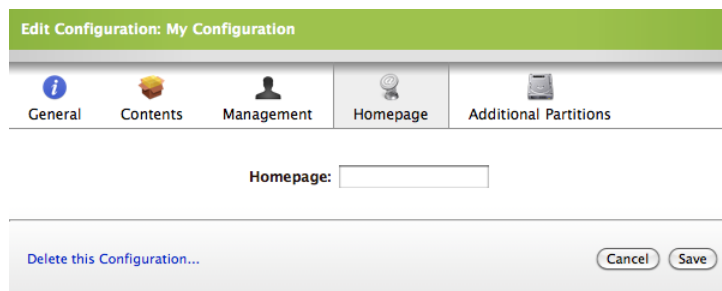


7. Click the **Contents** tab and use the **Packages**, **Scripts**, **Printers**, and **Directory Bindings** tabs to locate the items you want to add to the configuration.

To add an item, select the checkbox next to it.



8. If you want to set a default homepage for the clients:
  - a. Click the **Homepage** tab.
  - b. Enter the web address for the homepage in the **Homepage** field.



9. Click the **Save** button.

#### To set up partitioning for a configuration using Casper Admin:

1. Open Casper Admin.
2. Create or edit the configuration to partition.
  - To create a new configuration, click the **New Config** button in the toolbar.
  - To edit an existing configuration, select the configuration in the sidebar.
3. Click the **Additional Partitions** tab.
4. Click the **Add (+)** button.
5. Enter a name for the partition in the **Partition Name** field.
6. Enter the size you want the partition to be in the **Size** field.
7. Enter the maximum percentage of space that the partition should take up on the target drive.

8. If you want to deploy a configuration to the partition:
  - a. Choose "Journaled HFS+" from the **Format** pop-up menu.
  - b. Choose the configuration that you want to install from the **Install the Configuration** pop-up menu.
  - c. If you want this partition to be re-imaged on subsequent images of the primary partition, select the **Re-image this partition if it already exists** option.
  - d. To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.
  - e. Click **OK**.

9. If you want to deploy a Restore partition to the partition:
  - a. Choose "Journaled HFS+" from the **Format** pop-up menu.
  - b. Select the **This is a Restore Partition** checkbox.
  - c. Choose an OS package from which to create the Restore partition.

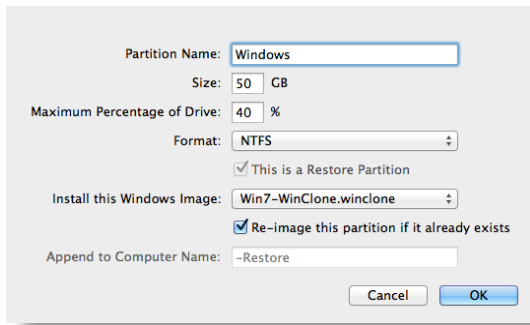
**Note:** Casper Admin identifies any package that has a priority of 1 as an OS package.

- d. To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.
- e. Click **OK**.

10. If you want to deploy a Winclone image to the partition:
  - a. Choose "NTFS" from the **Format** pop-up menu.
  - b. Choose the image that you want to install.
  - c. Select the **Re-image this partition if it already exists** option if you want the partition to be re-imaged on subsequent images of the primary partition.



d. Click **OK**.



11. Repeat steps 2 through 10 for each additional partition.

### To set up partitioning for a configuration using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Create or edit the configuration to partition.
  - To create a new configuration, click the **New Config** button in the toolbar.
  - To edit an existing configuration, select the configuration in the sidebar.
5. Click the **Additional Partitions** tab.
6. Click the **Add New Partition** link.
7. Enter a name for the partition, and then enter the size that you want it to be.
8. Enter the maximum percentage space that the partition should take up on the target drive.
9. If you want to deploy a configuration to the partition:
  - a. Choose "Journaled HFS+" from the **Format** pop-up menu.
  - b. Choose the configuration that you want to install.
  - c. If you want this partition to be re-imaged on subsequent images of the primary partition, select the **Re-image this partition if it already exists** option.
  - d. To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.

- e. Click **OK**.

Edit Configuration: My Configuration

General Contents Management Homepage Additional Partitions

Partition Name: Secondary

Size: 20 GB

Maximum Percentage of Drive: 20 %

Format: Journaled HFS+

This is a Restore partition

Configuration: My Configuration

Re-image this Partition if it already exists

Append to Computer Name: -Secondary

OK

Delete this Configuration... Cancel Save

10. If you want to deploy a Restore partition to the partition:
- Choose "Journaled HFS+" from the **Format** pop-up menu.
  - Select the **This is a Restore Partition** checkbox.
  - Choose the OS package from which the Restore partition should be created.

**Note:** Casper Admin identifies any package that has a priority of 1 as an OS package.

- To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.
- Click **OK**.

Edit Configuration: My Configuration

General Contents Management Homepage Additional Partitions

Partition Name: Restore

Size: 10 GB

Maximum Percentage of Drive: 10 %

Format: Journaled HFS+

This is a Restore partition

Package: Clean OS X Installation

Re-image this Partition if it already exists

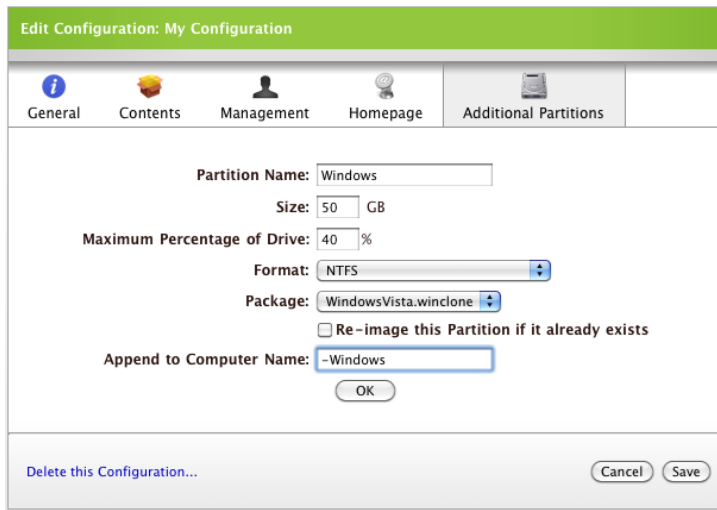
Append to Computer Name: -Restore

OK

Delete this Configuration... Cancel Save

11. If you want to deploy a Winclone image to the partition:
- Choose "NTFS" from the **Format** pop-up menu.
  - Choose the image that you want to install.

- c. If you want the partition to be re-imaged on subsequent images of the primary partition, select the **Re-image this partition if it already exists** option.
- d. Click **OK**.



12. Repeat steps 4 through 11 for each additional partition.
13. Click the **Save** button.

## Creating Smart Configurations

Smart configurations are based on other configurations. When you create a smart configuration, the configuration it is based on is called the standard configuration.

Smart configurations inherit the following components from their standard configuration:

- Packages
- Scripts
- Printers
- Directory bindings
- Homepage
- Partitions

Making changes to a standard configuration automatically updates the smart configuration to reflect the changes.

This section explains how to create a smart configuration using Casper Admin or the JSS.

**To create a smart configuration using Casper Admin:**

1. Open Casper Admin.
2. Click the **New Config** button in the toolbar.

3. Enter a name for the configuration.
4. (Optional) Enter a description of the configuration.
5. Select the **Smart Configuration** button.
6. Choose the configuration on which you want to base the smart configuration, and then click **OK**.
7. Add packages, scripts, printers, and directory bindings to the configuration, if necessary.

**Note:** To display only items unique to the smart configuration (the items you added in step 7), click the **Hide Items from Parent Configuration** button. To turn off this feature, click the **Hide Items from Parent Configuration** button again to depress it.

#### To create a smart configuration using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Config** button in the toolbar.
5. Enter a name for the configuration.
6. (Optional) Enter a description of the configuration.
7. Select the **Smart Configuration** button.
8. Choose the configuration on which you want to base the smart configuration, and then click **OK**.
9. Click the **Contents** tab and add packages, scripts, printers, and directory bindings to the configuration if necessary.
10. Click **Save**.

## Compiling Configurations

The compilation process installs the contents of a configuration to a single DMG, and then makes a block copy of the configuration. You can choose to make the DMG a compressed or an uncompressed file.

The time it takes to complete the compilation process varies with the amount of data in the configuration. For the fastest results, use a wired connection.

#### To compile a configuration using Casper Admin:

1. Open **Casper Admin**.
2. In the sidebar, select a configuration and click the **Compile** button.
3. Choose to create a compressed or an uncompressed DMG.
4. Enter credentials for the local administrator account.

5. Click **OK**.

**Note:** You may be prompted to authenticate multiple times during this process.

## Deleting Configurations

If there are clients using Autorun with a configuration you need to delete, it is recommended that you delete the entire configuration from the JSS. This gives you the option to update the Autorun data using a new configuration.

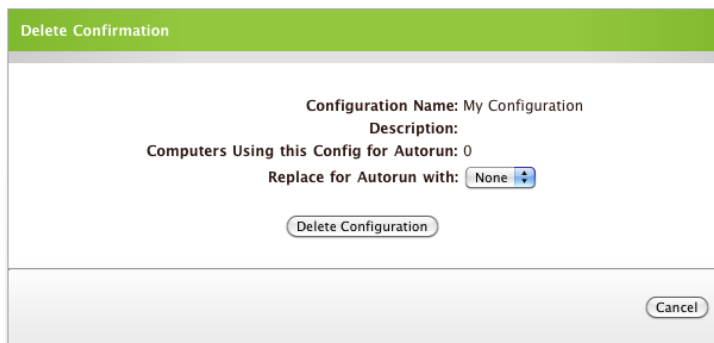
This section explains how to delete a configuration using Casper Admin or the JSS.

### To delete a configuration using Casper Admin:

1. Open Casper Admin.
2. In the sidebar, select the configuration that you want to delete and click the **Delete** button in the toolbar.
3. Click **OK** to confirm.

### To delete a configuration using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. In the sidebar, select the configuration that you want to delete and click the **Delete the Configuration** link.
5. To assign a new configuration that should be used for Autorun data, choose the configuration from the **Replace for Aurorun with** pop-up menu.



6. Click the **Delete Configuration** button.

# Imaging Drives

Before imaging a drive, you must boot to a startup disk other than the target drive. Some of the most common options for booting to a different startup disk are:

- NetBoot/NetInstall67
- A USB or FireWire drive
- A Restore partition

The JAMF Software Resource Kit includes a utility called the Casper NetInstall Creator. This utility creates a NetInstall image that has Casper Imaging automatically configured for you.

A Restore partition is a hidden partition configured to open Casper Imaging and automatically re-image a computer without intervention.

Imaging a drive for the first time automatically acquires the computer.

This section explains how to:

- Image a drive
- View imaging logs using the JSS

## To image a drive:

1. Boot to a startup disk other than the target drive.
2. Open Casper Imaging.
3. Choose the drive that you want to image from the **Target Drive** pop-up menu.
4. Select the **Erase <target drive>** checkbox.

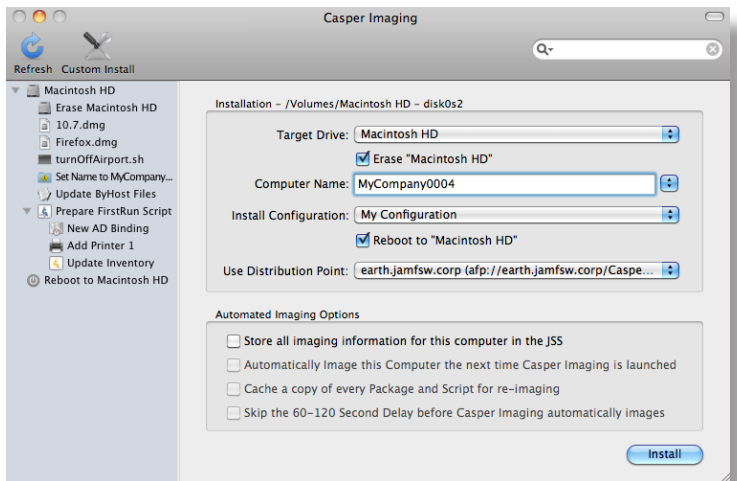
**Warning:** Selecting this option will cause all data on the target drive to be lost.

5. Enter a name for the computer in the **Computer Name** field.
6. Choose a configuration from the **Install Configuration** pop-up menu.
7. Select the **Reboot to <target drive>** checkbox.
8. Choose a distribution point from the **Use Distribution Point** pop-up menu.

To use a local drive, choose "Choose Local Drive" and then choose the local drive.

The local drive must be an external drive that is replicated in Casper Admin. (For more information, see the "Replicating FireWire or USB Drives" section in "Managing Distribution Points".)

9. Click **Install**.



**To view Imaging logs using the JSS:**

1. Log in to the JSS using a web browser.
2. Click the **Logs** tab.
3. Click the **Casper Imaging Logs** link.
4. Click the **View Log** link across from the log that you want to view.

# Customizing the Imaging Process

The imaging process is made up of the following components:

- Packages
- Scripts
- Printers
- A local account
- Directory bindings
- An Open Firmware/EFI password
- Network settings

Although configurations already contain most of these components, you can fully customize the imaging process by modifying each component as needed.

This section explains how to:

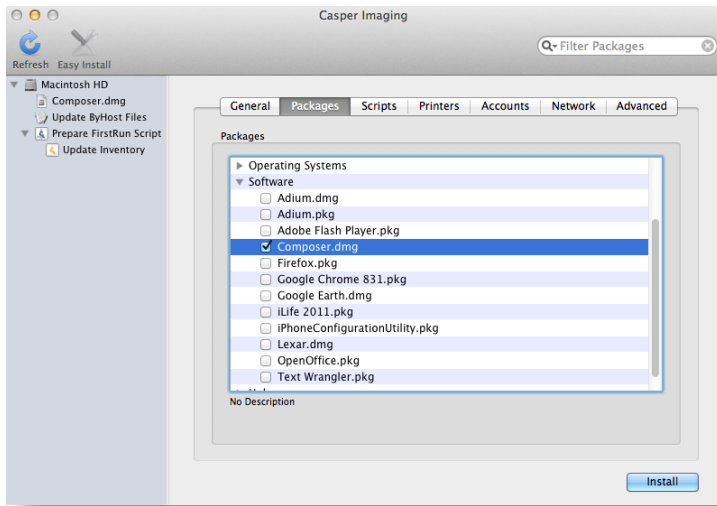
- Change the selected packages
- Change the selected scripts
- Change the selected printers
- Create a new local account
- Change the selected directory bindings
- Set an Open Firmware/EFI password

**To change the selected packages:**

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Packages** tab.

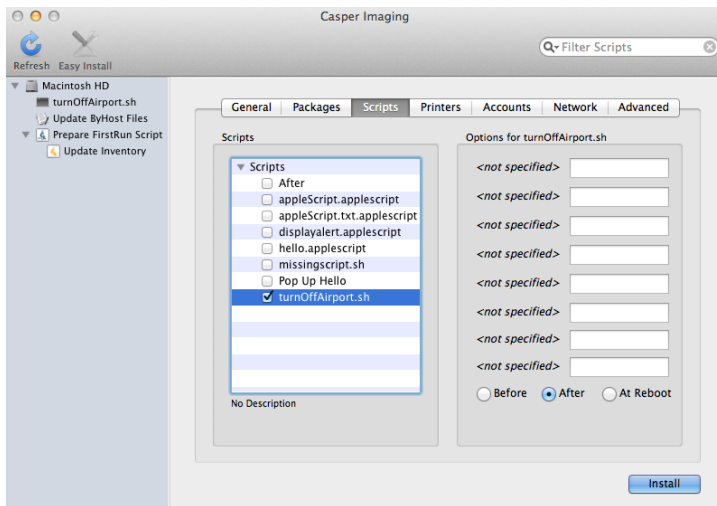


- In the list of packages, locate the packages you want to add or remove and select the checkbox next to each one.



#### To change the selected scripts:

- Open Casper Imaging.
- Click the **Custom Install** button in the toolbar.
- Click the **Scripts** tab.
- In the list of scripts, locate the scripts you want to add or remove and select the checkbox next to each one.

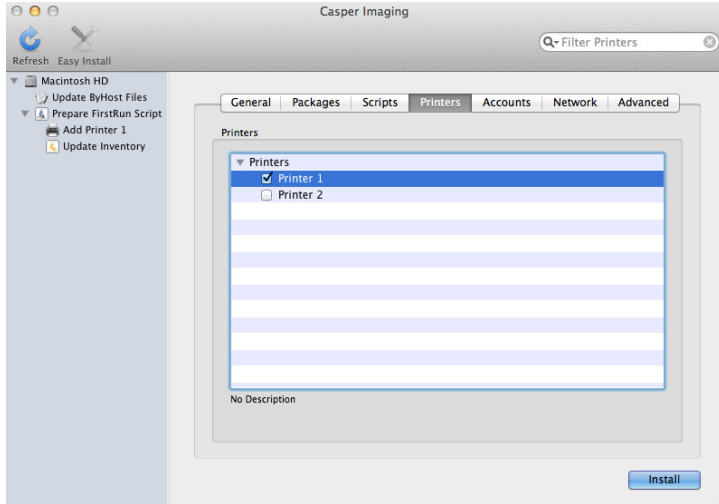


- Enter custom parameters and select a priority for each script using the **Before**, **After**, and **At Reboot** options.

#### To change the selected printers:

- Open Casper Imaging.

2. Click the **Custom Install** button in the toolbar.
3. Click the **Printers** tab.
4. In the list of printers, locate the printers you want to add or remove and select the checkbox next to each one.



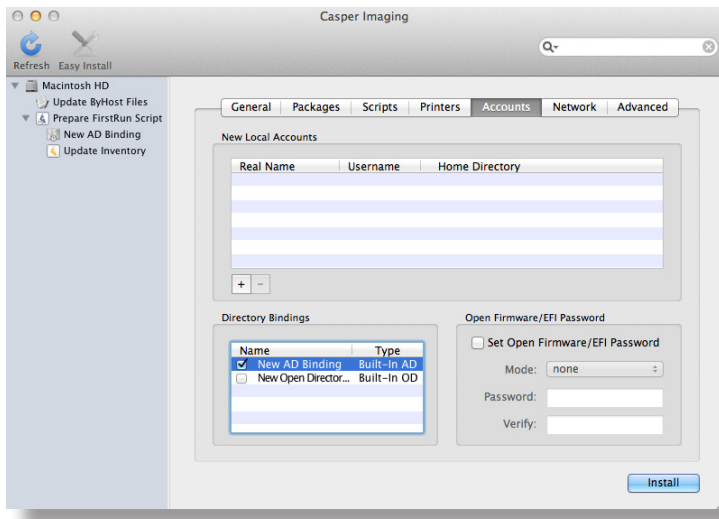
#### To create a new local account:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Accounts** tab.
4. Click the **Add (+)** button below the list of new local accounts.
5. Enter the new account information in the dialog that appears and click **OK**.

#### To change the selected directory bindings:

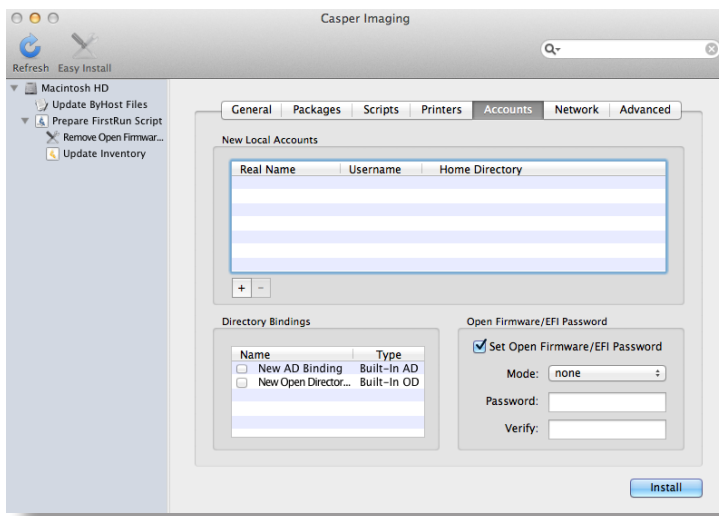
1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Accounts** tab.

4. In the list of directory bindings, select the checkbox next to each binding you want to add or remove.



#### To set the Open Firmware/EFI password:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Accounts** tab.
4. Select the **Set Open Firmware/EFI Password** checkbox.
5. Choose "Command" from the **Mode** pop-up menu.
6. Enter and verify the password for your account.



## Computer-Specific Network Settings

In order to change the network settings for a computer, Casper Imaging must be able to locate a network configuration that has the same settings (for instance, manually, using DHCP with a manual IP address, using DHCP, or using BootP) as the computer.

For example, if a computer requires a manually entered IP address, the configuration must require the same.

If only a few computers require a certain network configuration (or your OS package does not have one of the network configuration types listed in Casper Imaging), you can build a package that contains the following file:

```
/Library/Preferences/SystemConfiguration/preferences.plist
```

You should take this file from a computer that has the network configuration type you are looking for, such as manually or using DHCP with a manual IP address.

This section explains how to:

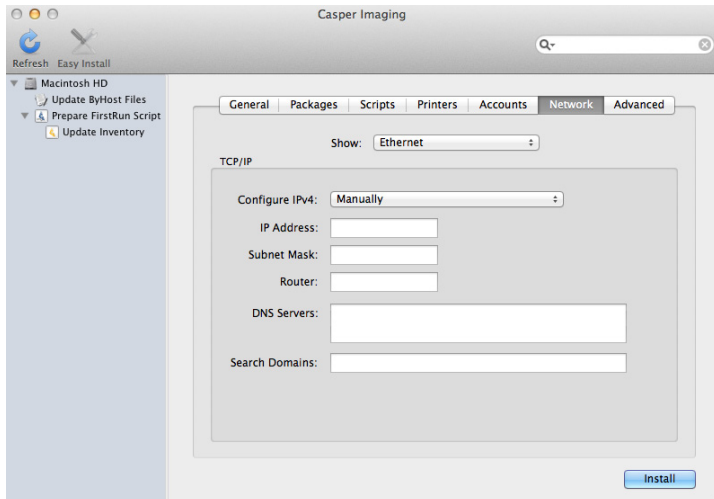
- Change the network settings
- Set the Apple Remote Desktop info fields
- Reset or fix permissions after imaging
- Display the Mac OS X Setup Assistant on the first boot

### To change the network settings:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Network** tab.
4. Choose "Ethernet" or "Airport" from the **Show** pop-up menu.

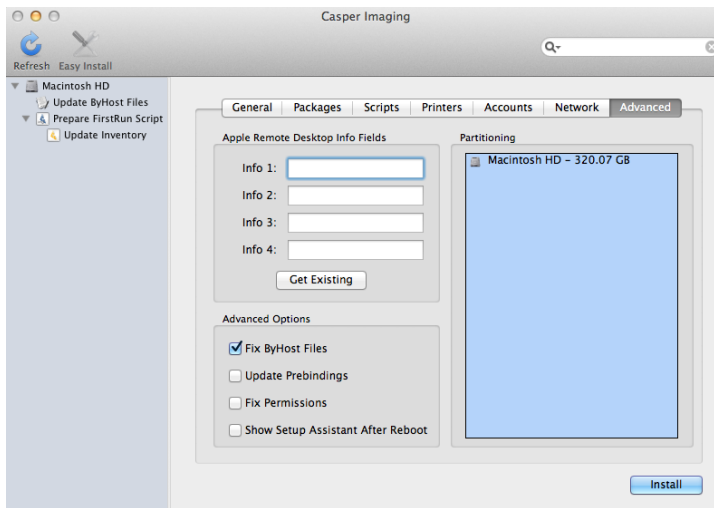
5. Choose the network configuration type from the **Configure IPv4** pop-up menu, and then make the necessary changes.

**Note:** Any fields left blank will not be modified when Casper Imaging updates the settings.



#### To set the Apple Remote Desktop info fields:

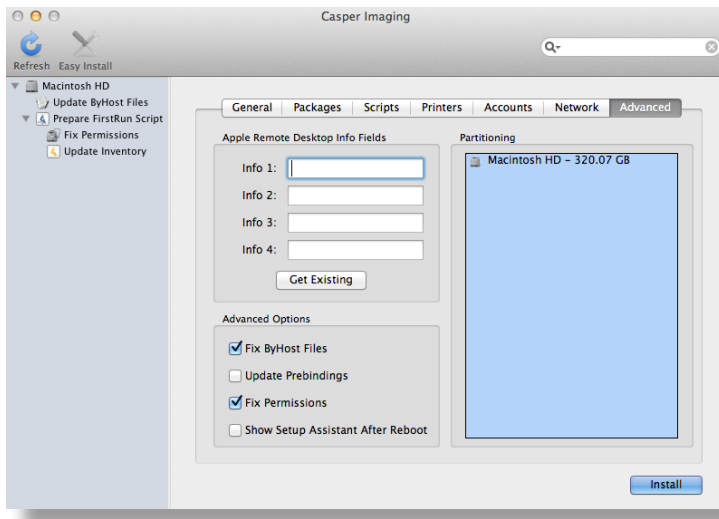
1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Advanced** tab and specify any relevant information.



#### To reset or fix permissions after imaging:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.

3. Click the **Advanced** tab and select the **Fix Permissions** checkbox.



To display the Mac OS X Setup Assistant on the first boot:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Advanced** tab and select the **Show Setup Assistant After Reboot** checkbox.

**Note:** If you do not select the **Show Setup Assistant After Reboot** checkbox, Casper Imaging will make sure the file exists in:

```
/private/var/db/.AppleSetupDone
```

# Managing Autorun Preferences

Autorun preferences allow you to control delay, load balancing, and caching settings the Autorun feature in Casper Imaging. The following list explains each preference setting:

- **Delay**—The minimum number of seconds that Casper Imaging waits before automatically imaging a computer.  
During this delay, a pane is displayed that allows you to cancel reformatting of the drive if necessary.
- **Random additional delay**—The number of seconds added to the delay.  
Setting an additional delay can relieve stress from the distribution point when a large deployment is staggered over a period of time.
- **Enable Load Balancing for distribution points**—Randomly assigns distribution points for each computer if the distribution point has a backup.  
This does not guarantee distribution points will balance perfectly as the balancing is done client-side.
- **Leave this much space available when caching packages**—Caches packages locally until the specified amount of space remains on the client.  
This only takes place if Casper Imaging is configured to cache packages during the Autorun process. See the “Using the Autorun Feature” section for more information.
- **Compare Cached Packages using**—Specifies whether file size, modification date, or checksum is used to ensure the latest copy of a package.  
This only takes place if Casper Imaging is configured to cache packages during the Autorun process. See the “Using the Autorun Feature” section for more information.

To set Autorun preferences:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Autorun Preferences** link.
4. On the pane that is displayed, set Autorun preferences as needed.

**Autorun Preferences**  
Preferences for how Casper Imaging's Autorun feature behaves.

Delay:  seconds

Random additional delay:  seconds

Enable Load Balancing for distribution points:

Leave this much space available when caching packages:  MB

Compare Cached Packages using:  File Size  
 Modification Date  
 Checksum (Slow)

5. Click the **Save** button.

# Using the Autorun Feature

The Autorun feature allows you to automatically re-image computers according to a schedule. This reduces the amount of time and interaction required to prepare a lab or classroom for use.

The Autorun preferences allow you to configure delay, load balancing, and caching options for the Autorun feature. See the section entitled “Managing Autorun Preferences” for more information.

This section explains how to:

- Store Autorun data for a computer
- Create Autorun data for a computer
- Bypass the Autorun feature
- Edit Autorun data for a computer
- Delete Autorun data for a computer

You can also edit and delete Autorun data for multiple computers at one time. See the “Performing Mass Actions on Computer Search Results” section for more information.

## To store Autorun data:

1. Open Casper Imaging on the computer you want to store Autorun data for.
2. Configure imaging options for the computer, and then select the **Store all imaging information for this computer in the JSS** checkbox.
3. Enter the password for the local account if prompted and click **OK**.
4. To automatically re-image the computer the next time Casper Imaging is launched, select the **Automatically image this computer the next time Casper Imaging is launched** checkbox.
5. To reduce network traffic during subsequent re-images, select the **Cache a copy of every package and script for re-imaging** checkbox.  
This prompts Casper Imaging to keep a copy of each package and script.
6. To bypass the delay that takes place before the imaging process begins, select the **Skip the 60–120 Second delay before Casper Imaging automatically images** checkbox.

**Note:** Once Autorun data is stored for the computer, it is imaged automatically when Casper Imaging is launched.

## To create Autorun data for a computer:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.



4. Click **Autorun** across from the computer record.
5. On the Install pane, specify installation information and set imaging options.

**Note:** Re-imaging a computer with Autorun data does not modify the management information on the computer.

6. Use the six remaining tabs (**Packages, Scripts, Printers, Accounts, Network, and Advanced**) to specify any additional information as needed.
7. Click the **Save** button.

#### To bypass the Autorun feature:

To temporarily bypass the Autorun feature, hold down the Shift key when you open Casper Imaging.

#### To edit Autorun data for a computer:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Click **Autorun** across from the computer record you want to edit.
5. On the Install pane, add or modify the information as needed.

**Autorun Data for MyCompany0005**

Install Packages Scripts Printers Accounts Network Advanced

**Installation**

Target Drive:

Erase Target Drive

Computer Name:

Install Configuration:

Reboot To Target Drive When Done

Use Distribution Point:

**Local Authentication to allow Casper Imaging to run Automatically**

Local Username:

Local Password:

**JAMF Software Server Options**

Store all imaging information for this computer in the JSS

Automatically Image this Computer the next time Casper Imaging is launched

Cache a copy of the every Package and Script for re-imaging

Skip the 60-120 Second Delay before Casper Imaging automatically images

6. Use the six remaining tabs (**Packages, Scripts, Printers, Accounts, Network, and Advanced**) to specify any additional information as needed.
7. Click the **Save** button.

**To delete Autorun data for a computer:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced computer search.
4. Click **Autorun** across from the computer record.
5. Click the **Remove Autorun Data for this Computer** button.

Autorun Data for MyCompany0005

Install Packages Scripts Printers Accounts Network Advanced

**Installation**

Target Drive:

Erase Target Drive

Computer Name:

Install Configuration:

Reboot To Target Drive When Done

Use Distribution Point:

**Local Authentication to allow Casper Imaging to run Automatically**

Local Username:

Local Password:

**JAMF Software Server Options**

Store all imaging information for this computer in the JSS

Automatically Image this Computer the next time Casper Imaging is launched

Cache a copy of the every Package and Script for re-imaging

Skip the 60-120 Second Delay before Casper Imaging automatically images

6. Click the **Delete Permanently** button to confirm.

# PreStage Imaging

PreStage imaging allows you to image computers or groups of computers automatically as you add them to your network. When you create a PreStage, you pre-configure the imaging process to include information that you want to use to image the computers.

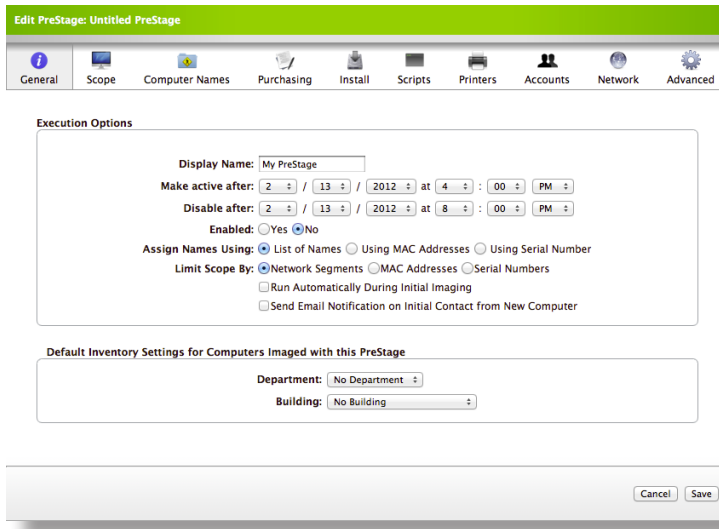
Using a PreStage automatically acquires newly imaged computers and enrolls any computers that are associated with an administrator account that has SSH access to the computer.

This section explains how to create, view logs for, edit, and delete a PreStage.

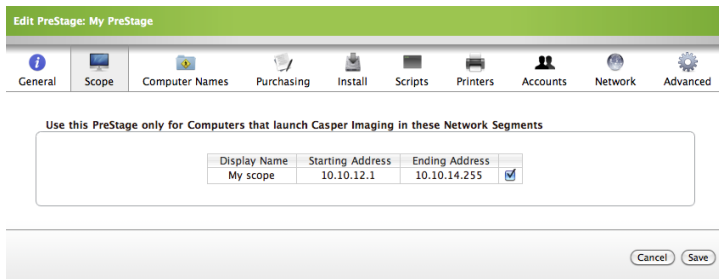
## To create a PreStage:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **PreStage Imaging** link.
4. Click the **Create PreStage** button in the toolbar.
5. Enter a display name for the PreStage.
6. Set the date and time you want the PreStage to become active using the **Make active after** pop-up menus.
7. Set the date and time you want to PreStage to expire using the **Disable after** pop-up menus. If you don't want the PreStage to expire, set a date far ahead in the future, such as "12/30/2020".
8. Choose how you want the PreStage to assign names to the computers:
  - If you select the **List of Names** option, you can provide a list of computer names from which names are assigned.
  - If you select the **Using MAC Addresses** option, names are assigned according to each computer's MAC address.
  - If you select the **Using Serial Number** option, names are assigned according to each computer's serial number.
9. Choose whether to limit the scope of the PreStage to computers in certain network segments, with specific MAC addresses, or with certain serial numbers.

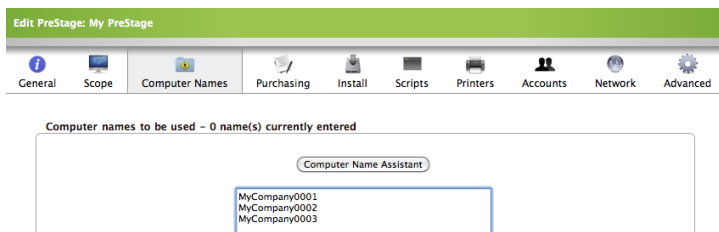
- If you want Casper Imaging to automatically image the computer during the initial imaging, select the **Run Automatically During Initial Imaging** checkbox.



- To receive an email notification when a new computer is imaged using the PreStage, select the **Send Email Notification on Initial Contact from New Computer** checkbox.
- Click the **Scope** tab.
- Based on how you chose to limit the scope in step 9, select the network segments to which the PreStage should be made available or enter the MAC addresses or serial numbers for the computers.

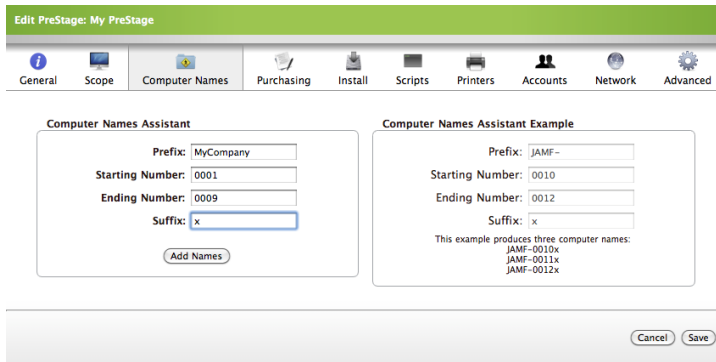


- Click the **Computer Names** tab.
- If you chose to assign names to the computers using a list of names in step 8, do one of the following:
  - Manually enter a list of computer names in the blank field provided.

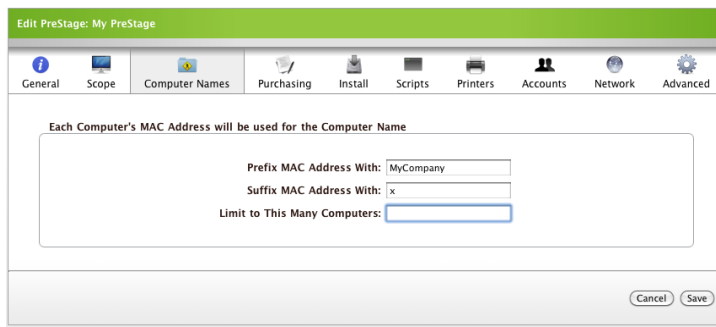


- If the names are in numerical order, perform the following steps to have the JSS populate the list for you:
  - Click the **Computer Name Assistant** button.

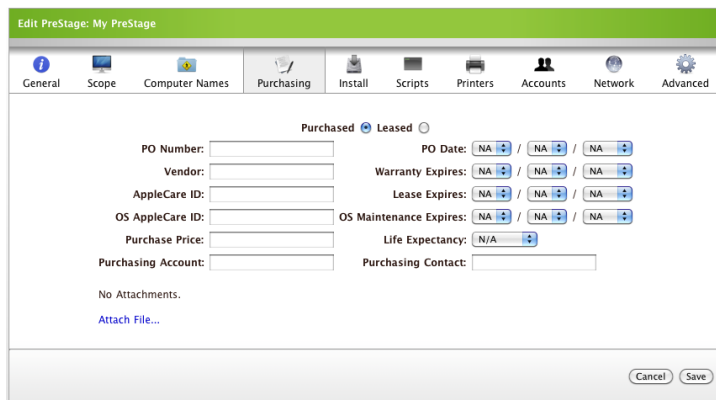
- b. Enter a prefix, starting number, ending number, and suffix in the fields provided.
- c. A sample entry is displayed for your reference.
- d. Click the **Add Names** button.



16. If you chose to assign names to the computers using MAC addresses in step 8, enter a prefix and suffix for the MAC addresses and enter the maximum number of computers the PreStage should be used for. If there is no definite number, enter a large number, such as "99999".



17. If you want new computers to include purchasing information on their inventory reports, click the **Purchasing** tab and enter the information you want them to include.



18. Use the Install, Scripts, Printers, Accounts, Network, and Advanced panes to enter any additional imaging information. To make this information available for the computers in the future, click the **Install** tab and select the **Store all imaging information for this computer in the JSS** checkbox.

19. Click **Save**.

**To view logs for a PreStage:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **PreStage Imaging** link.
4. Click the **View Status** link across from the PreStage.
5. Click the **View Log** link across from the log that you want to view.

**To edit a PreStage:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **PreStage Imaging** link.
4. Click the **Edit** link across from the PreStage you want to modify and make the necessary changes.
5. Click **Save**.

**To delete a PreStage:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **PreStage Imaging** link.
4. Click the **Delete** link across from the PreStage that you want to delete.
5. Click **Delete** to confirm.

# Target Mode Imaging

Target Mode Imaging (TMI) is an alternative method for imaging large quantities of computers when using the network is not optimal. For example, MacBook Airs that do not have built-in ethernet but come with high-speed Thunderbolt ports can be imaged in mass using TMI. This method of imaging is faster than using USB Ethernet dongles, especially when using Thunderbolt.

Instead of running Casper Imaging on every computer by booting to a NetBoot image or an external drive, you can run Casper Imaging on a host computer and connect other computers that are booted to target disk mode.

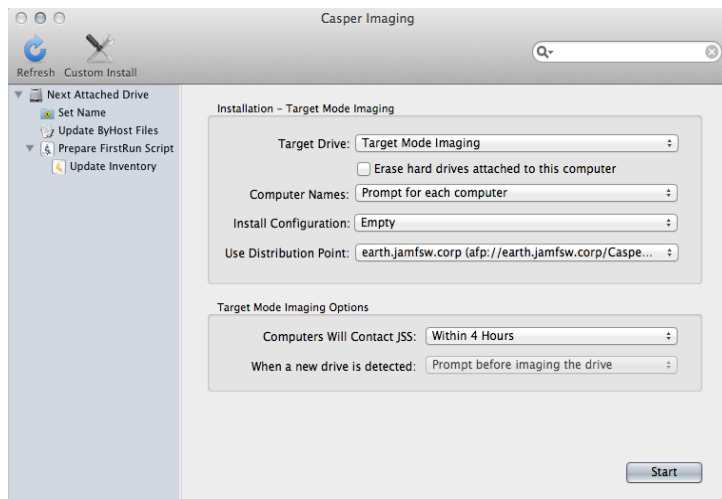
TMI automatically acquires newly imaged computers.

TMI requires a host computer with a FireWire or Thunderbolt port and target computers that support target disk mode.

## To use TMI:

1. On the host computer, open Casper Imaging.
2. Choose "Target Mode Imaging" from the **Target Drive** pop-up menu.
3. To erase the target drives, select the **Erase hard drives attached to this computer** checkbox.

**Warning:** Selecting this option will cause all data on the target drives to be lost.



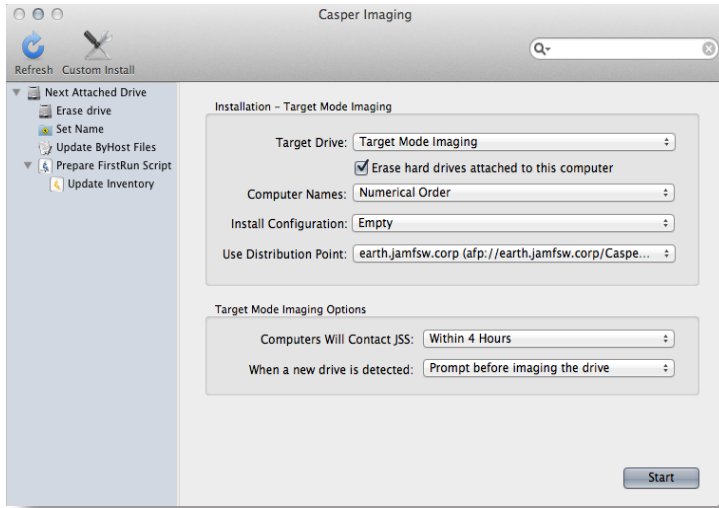
4. Specify how you want to name target computers by choosing an option from the **Computer Name** pop-up menu.

Choosing "Numerical order", "Use MAC Address", or "Use serial number" prompts you to enter a prefix and suffix. For "Numerical order", you must also enter a start number.

Choosing "Upload CSV file" prompts you to choose a CSV file. The CSV file must meet the following specifications:

- The first column contains the target computers' serial numbers or MAC addresses. Acceptable delimiters for MAC addresses are a period, a colon, or no delimiter.
- The second column contains the target computers' names.

5. Choose a configuration from the **Install Configuration** pop-up menu.



6. Choose a distribution point from the **Use Distribution Point** pop-up menu.

To use a local drive, choose "Choose Local Drive" and then choose the local drive.

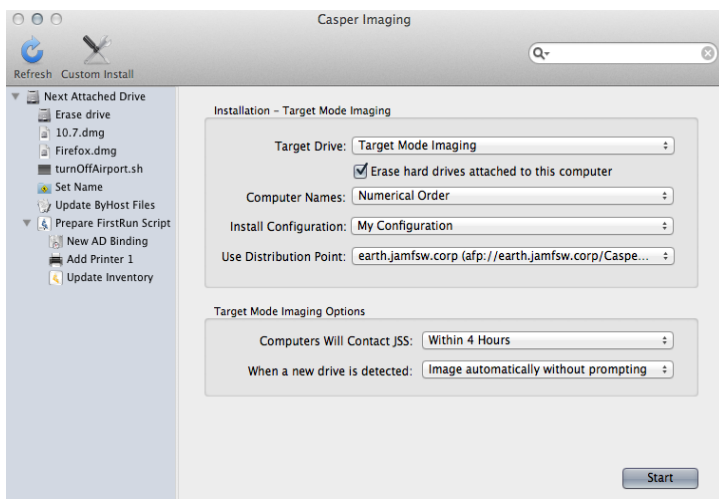
The local drive must be an external drive that is replicated in Casper Admin. (For more information, see the "Replicating FireWire or USB Drives" section in "Managing Distribution Points".)

7. If target computers will not be started up to contact the JSS immediately after imaging, specify an approximate contact time by choosing an option from the **Computers Will Contact JSS** pop-up menu.

8. To automatically image subsequent drives when they are connected to the host computer, choose "Image automatically without prompting" from the **When a new device is detected** pop-up menu.

By default, Casper Imaging displays a prompt before imaging each drive.

9. Click **Start**.





10. Boot a target computer to target disk mode.  
To do this, turn on the computer and immediately press and hold down the T key.
11. Use a FireWire or Thunderbolt cable to connect the target computer to the host computer, and then click **OK** if prompted.  
Casper Imaging immediately starts imaging the drive.
12. When the imaging process is complete, disconnect the target computer.
13. Repeat steps 10-12 for each target computer.

# Patch Management

## Running Software Update

You can automate Apple's Software Update on your client computers so that Software Update installs updates in the background without disturbing users.

In OS X v10.4 and later, Apple allows you to host your own software update server internally. This reduces bandwidth by downloading packages once per server instead of once per computer. It also allows you to control and approve updates using the Server Admin application on Mac OS X Server before you make them available.

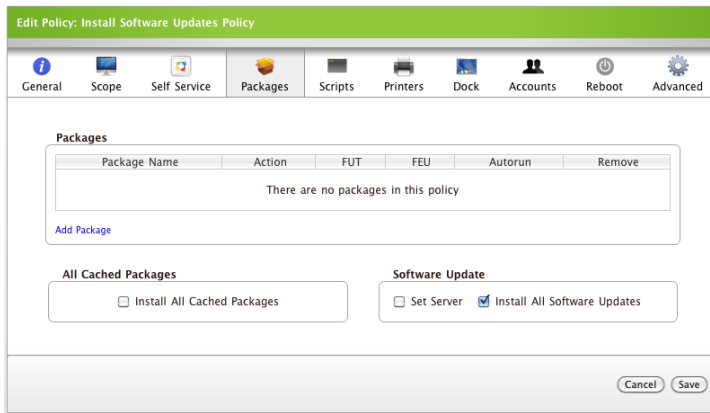
Before using a policy to run Software Update on client computers from an internally hosted software update server, you must add one or more software update servers to the JAMF Software Server (JSS). For instructions on adding software update servers, see the "Software Update Servers" section.

This section explains how to run Software Update using a policy or Casper Remote.

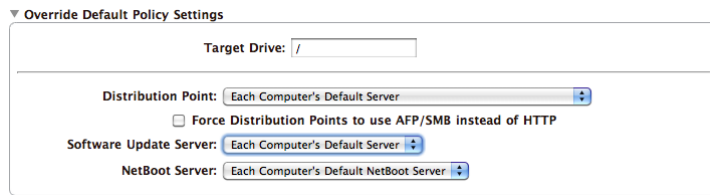
### To run Software Update using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.

- Click the **Packages** tab and select the **Install All Software Updates** checkbox.



- If you have an alternate software update server configured in your environment and you want to install the updates from this server instead of from apple.com, select the **Set Server** checkbox. If you have multiple alternate software update servers configured, choose which one you want to install:
  - Select the **Set Server** checkbox.
  - Click the **General** tab.
  - Click the disclosure triangle next to **Override Default Policy Settings**.
  - Select a server from the **Software Update Server** pop-up menu.



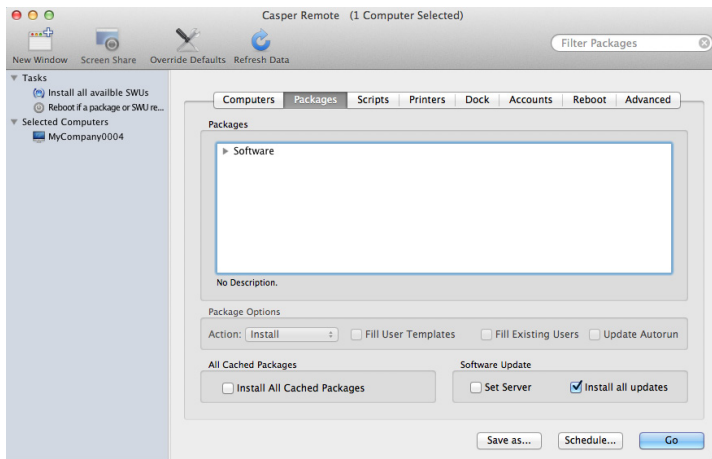
- If an update requires client computers to reboot, the computers will do so by default. To change this setting or assign specific reboot criteria, click the **Reboot** tab and make the necessary changes.
- Click **Save**.

Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

### To run Software Update using Casper Remote:

- Open Casper Remote.
- In the **Computers** list, locate the clients you want to receive the software updates and select the checkbox next to each one.

3. Click the **Packages** tab and select the **Install All Updates** checkbox.



4. If you have an alternate software update server configured in your environment and you want to install the updates from this server instead of from apple.com, select the **Set Server** checkbox.
5. If an update requires client computers to reboot, they will do so by default. To change this setting or specify reboot criteria, click the **Reboot** tab and make the necessary changes.
6. Click **Go**.

Once you complete these steps, Casper Remote applies the update to client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote applies all available updates.
4. Casper Remote reboots the clients, if necessary. (This step is based on any reboot settings you may have configured.)
5. Casper Remote logs out of each client and ends the SSH connection.

# Installing Adobe CS3/CS4 Updaters

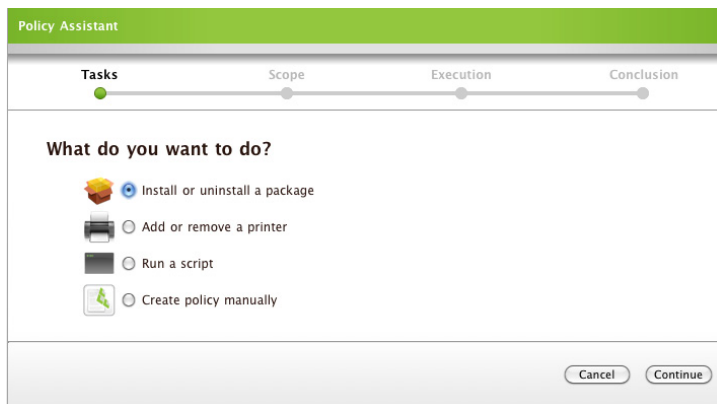
The Casper Suite allows you to deploy Adobe CS3 or CS4 Updaters without repackaging them.

Once you identify the DMG as an Adobe Updater, you can deploy it like any other package. For more information on adding a DMG of an Adobe CS3/CS4 Updater, see the section entitled “Managing Packages”.

This section explains how to install an Adobe Updater using a policy or Casper Remote.

## To configure a policy to install an Adobe Updater using the Policy Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.
5. Select the **Install or uninstall a package** option and click **Continue**.



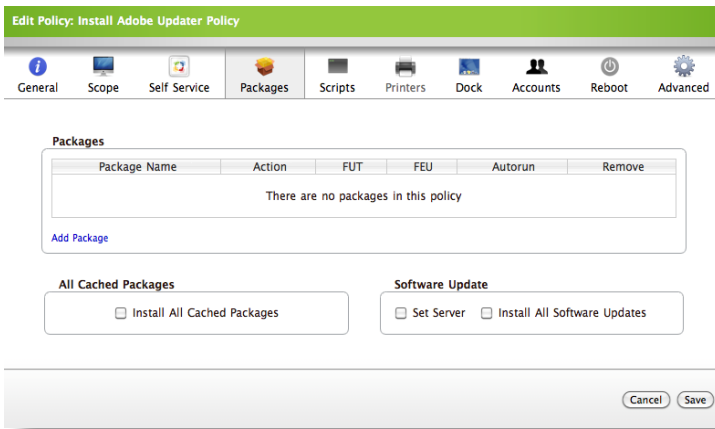
6. Follow the instructions on each pane to configure the rest of the policy.

Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

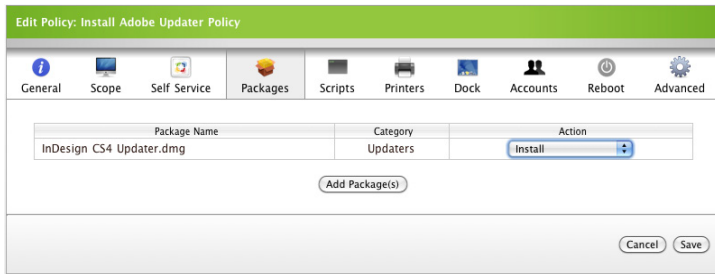
## To manually configure a policy to install an Adobe Updater:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.

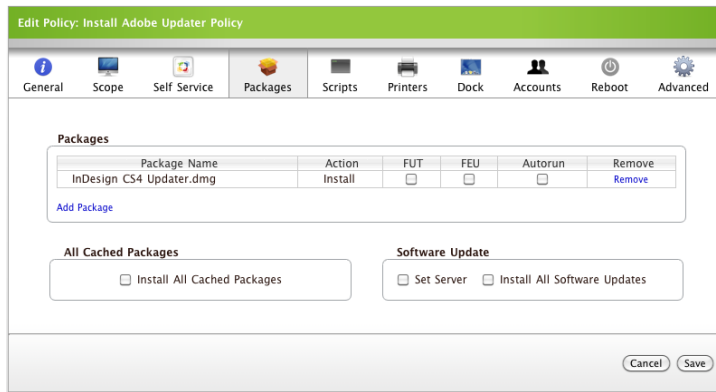
- To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
  6. Assign the policy to a category using the **Category** pop-up menu.
  7. Choose a trigger from the **Triggered By** pop-up menu.
  8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
  9. Click the **Scope** tab and assign computers or user groups to the scope.
  10. Click the **Packages** tab and click the **Add Package** link.



11. Locate the updater you want to install and choose "Install" from the **Action** pop-up menu across from it.
12. Click the **Add Package(s)** button.



13. Click **Save**.



Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

**To install an Adobe Updater using Casper Remote:**

1. Open Casper Remote.
2. In the **Computers** list, locate the clients on which you want to install the updater and select the checkbox next to each one.
3. Click the **Packages** tab.
4. In the **Packages** list, locate the updater you want to deploy and select the checkbox next to it.
5. Click **Go**.

Once you complete these steps, Casper Remote deploys the updater to client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote installs the Adobe Updater.
4. Casper Remote logs out of each client and ends the SSH connection.

# Software Distribution

## Installing Packages

The Casper Suite supports deployment for the following package formats:

- DMG
- PKG
- MPKG (self-contained)
- Adobe CS3 or CS4 Installer

Make sure the software is packaged in one of these formats before you begin.

The first step to deploying a package is to upload the package using the Casper Admin application and assign it to a category. You can now configure custom deployment settings and modify the attributes of the package if necessary. For more information about uploading packages and customizing deployment settings, see the “Managing Packages” section of this guide.

Next, create a policy or use the Casper Remote application to deploy the package. Before choosing the method that you want to use, read the “Policies” section and consider the benefits of each method.

Once a package is deployed, client computers pull it from their default distribution point. Clients without default distribution point pull packages from the master distribution point. If HTTP is enabled on the distribution point, clients download the package over HTTP or HTTPS; if HTTP is not enabled, clients utilize Apple Filing Protocol (AFP) or Server Message Block (SMB) to obtain the packages. If you deploy the package using a policy, you can change these settings in the “Override Default Settings” section on the General pane when you edit or manually configure the policy.

Once client computers obtain the package, it is installed in the background to avoid disturbing users.

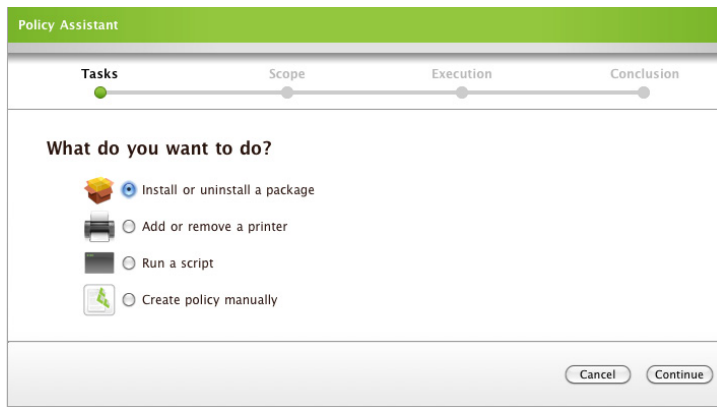
This section explains how to install a package using a policy or Casper Remote.

### To configure a policy to install a package using the Policy Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.



5. Select the **Install or uninstall a package** option and click the **Continue** button.



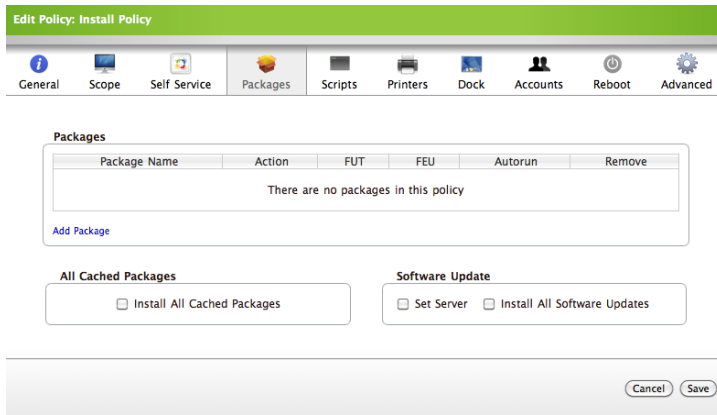
6. Follow the onscreen instructions to configure the rest of the policy.

Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

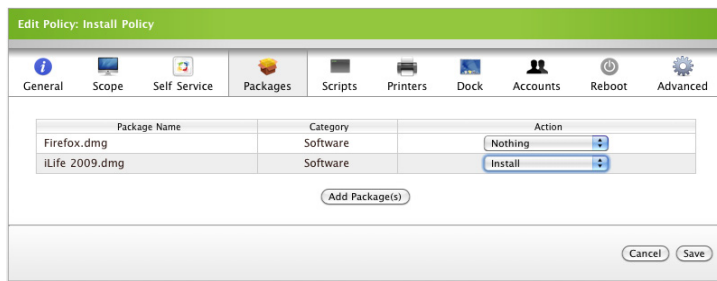
#### To manually configure a policy to install a package:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.

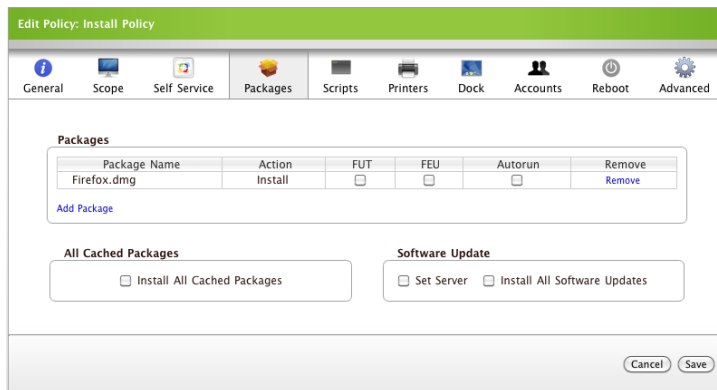
10. Click the **Packages** tab and click the **Add Package** link.



11. Locate the package you want to install and choose "Install" from the **Action** pop-up menu across from it.
12. Click the **Add Package(s)** button.



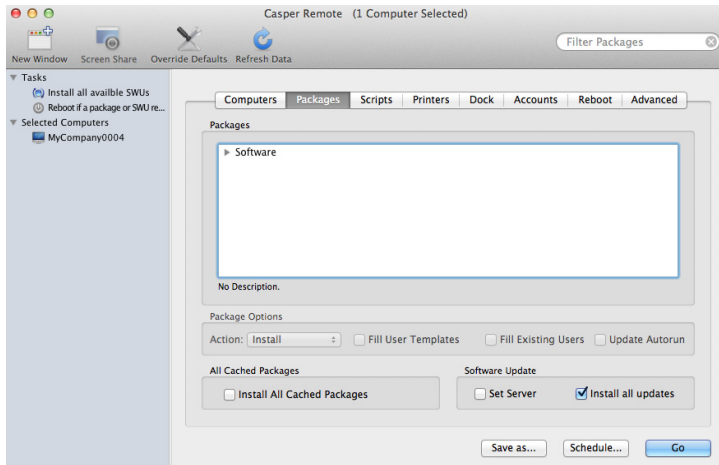
13. Click **Save**.



Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

## To install a package using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the clients you want to install the package to and select the checkbox next to each one.
3. Click the **Packages** tab.
4. In the **Packages** list, locate the package you want to install and select the checkbox next to it.
5. Click **Go**.



Once you complete these steps, Casper Remote installs the package on client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote installs the package.
4. Casper Remote logs out of each client and ends the SSH connection.

# Caching Packages

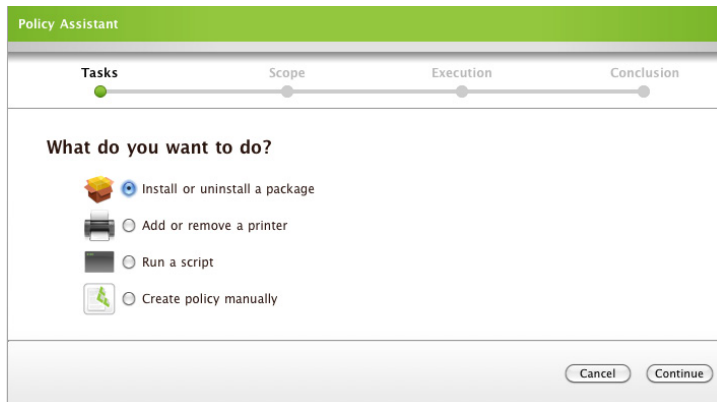
Caching packages allows client computers to download a series of packages over time without installing them right away. This reduces the use of bandwidth but still allows you to make packages available to users simultaneously.

The same prerequisites and settings used to install packages also apply when caching packages.

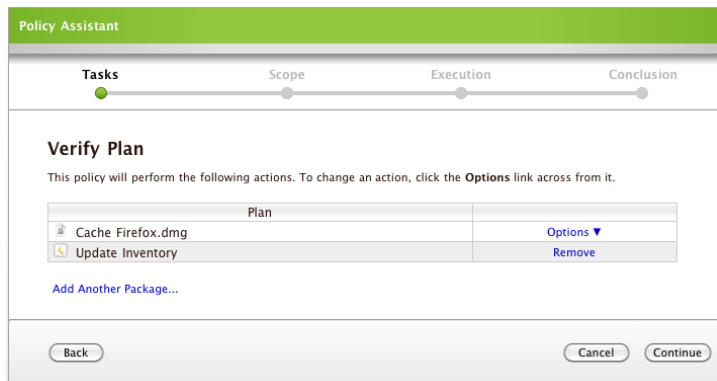
This section explains how to cache a package using a policy or Casper Remote.

## To configure a policy to cache a package using the Policy Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.
5. Select the **Install or uninstall a package** option and click the **Continue** button.



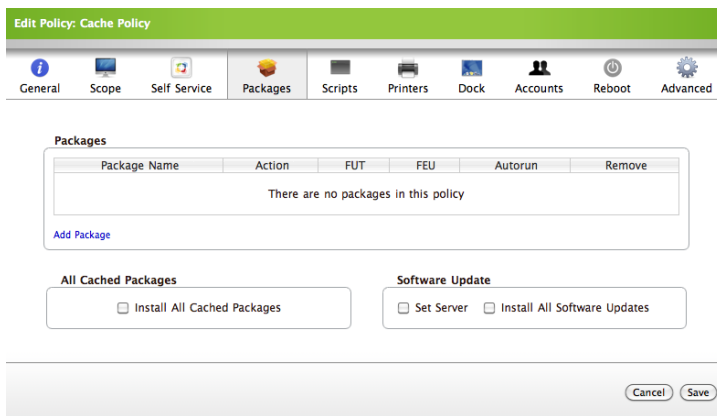
6. Follow the onscreen instructions until you get to the Verify Plan pane. Then, click **Options** and choose "Cache" from the menu.



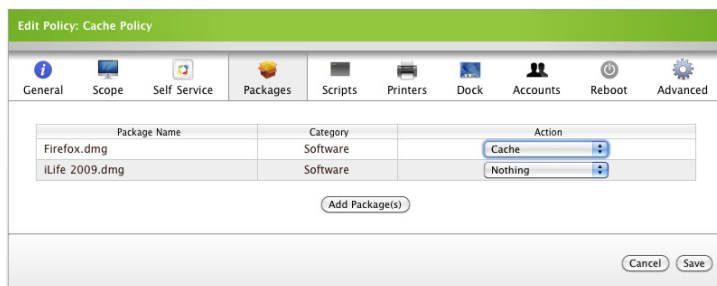
- Click the **Continue** button and follow the instructions on each pane to configure the rest of the policy. Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

**To manually configure a policy to cache a package:**

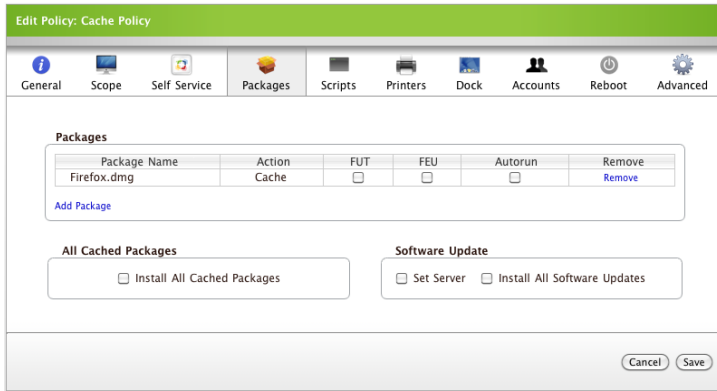
- Log in to the JSS with a web browser.
- Click the **Management** tab.
- Click the **Policies** link.
- Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
- Enter a display name for the policy.
- Assign the policy to a category using the **Category** pop-up menu.
- Choose a trigger from the **Triggered By** pop-up menu.
- Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
- Click the **Scope** tab and assign computers or user groups to the scope.
- Click the **Packages** tab and click the **Add Package** link.



- Locate the package you want to cache and choose "Cache" from the **Action** pop-up menu across from it.
- Click the **Add Package(s)** button.



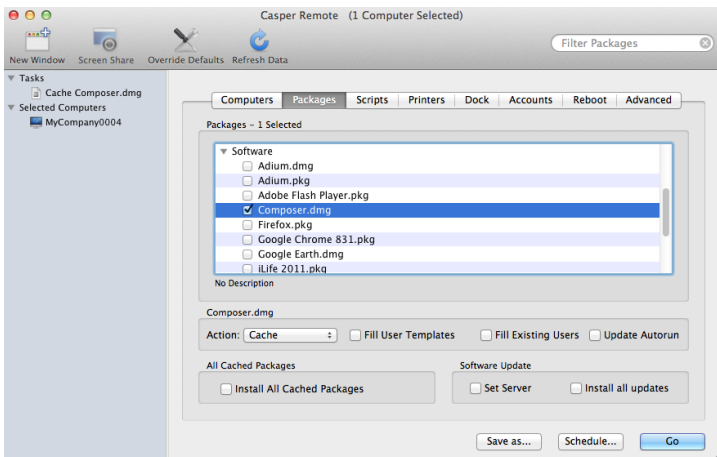
13. Click Save.



Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

**To cache a package using Casper Remote:**

1. Open Casper Remote.
2. In the **Computers** list, locate the clients that you want to cache the package and select the checkbox next to each one.
3. Click the **Packages** tab.
4. In the **Packages** list, locate the package you want to cache and select the checkbox next to it.
5. Choose "Cache" from the **Action** pop-up menu.
6. Click **Go**.



Once you complete these steps, Casper Remote caches the package on client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote caches the package in the following directory:  
/Library/Application Support/JAMF/Waiting Room/
4. Casper Remote logs out of each client and ends the SSH connection.

# Installing Cached Packages

You can choose to install one or all of the packages cached on a client computer.

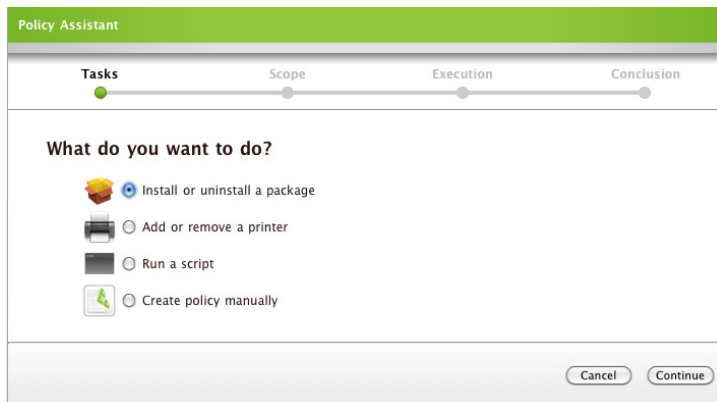
The same prerequisites and settings used to install packages also apply when installing cached packages.

This section explains how to use a policy or Casper Remote to:

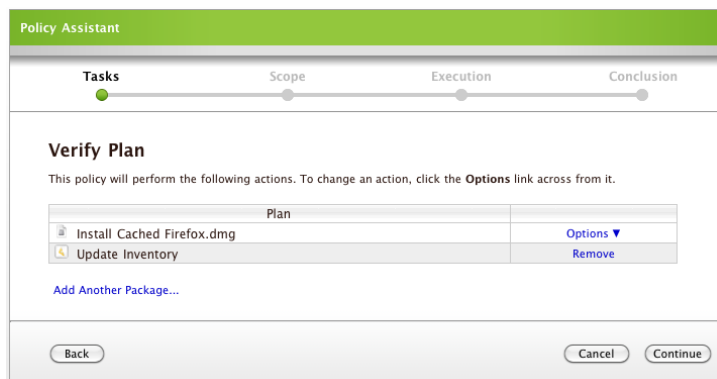
- Install a cached package
- Install all cached packages

**To configure a policy to install a cached package using the Policy Assistant:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.
5. Select the **Install or uninstall a package** option and click the **Continue** button.



6. Follow the onscreen instructions until you get to the Verify Plan pane. Then, click **Options** and choose "Install Cached" from the menu.



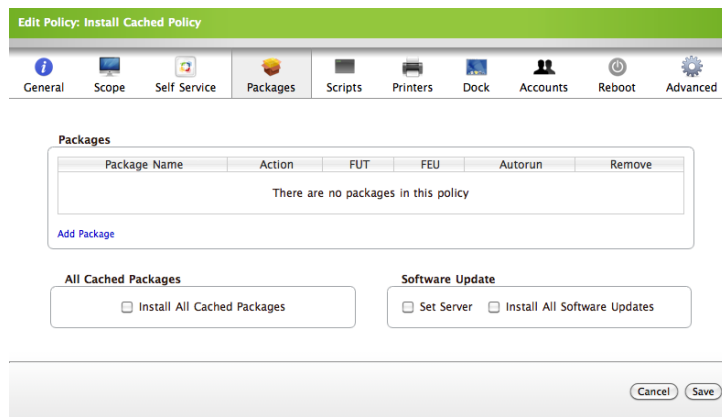


7. Click the **Continue** button and follow the instructions on each pane to configure the rest of the policy.

Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

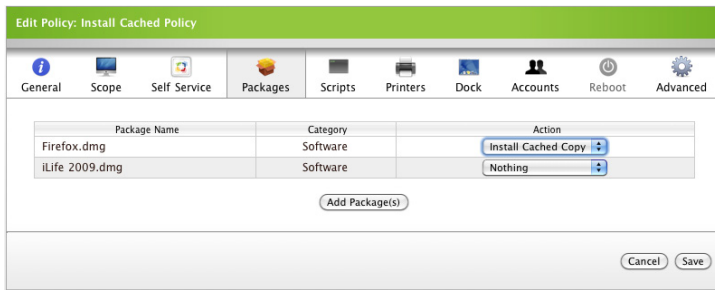
### To manually configure a policy to install a cached package:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Packages** tab and click the **Add Package** link.

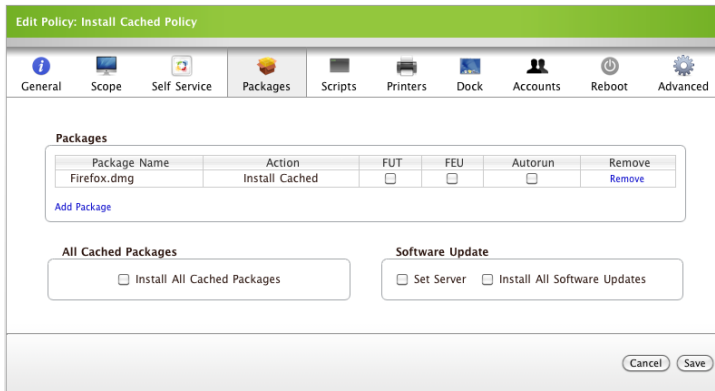


11. Locate the package you want to install and choose "Install Cached Copy" from the **Action** pop-up menu across from it.

12. Click the **Add Package(s)** button.



13. Click **Save**.

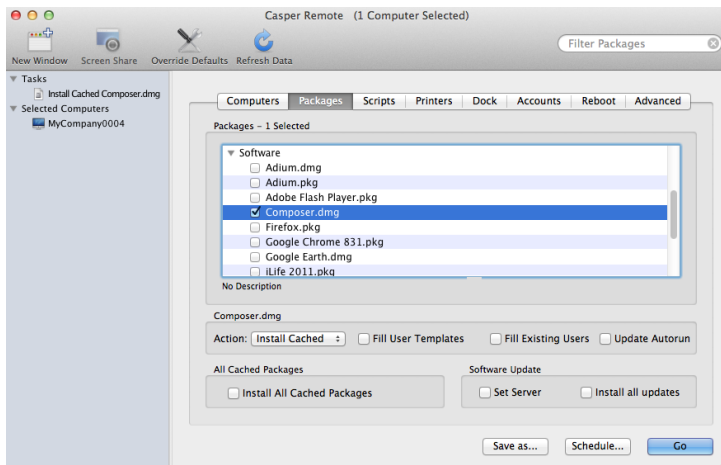


Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

### To install a cached package using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the clients that you want to install the package and select the checkbox next to each one.
3. Click the **Packages** tab.
4. In the **Packages** list, locate the package you want to install and select the checkbox next to it.
5. Choose "Install Cached" from the **Action** pop-up menu.

## 6. Click Go.



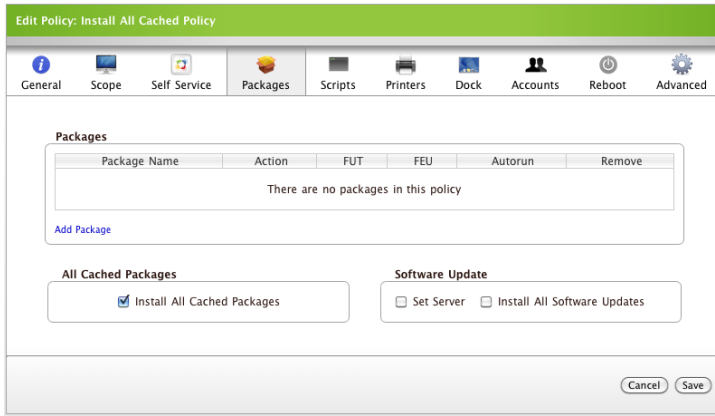
Once you complete these steps, Casper Remote installs the cached package by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote installs the cached package from the following directory:  
/Library/Application Support/JAMF/Waiting Room/
4. Casper Remote logs out of each client and ends the SSH connection.

### To install all cached packages using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Packages** tab and select the **Install All Cached Packages** checkbox.

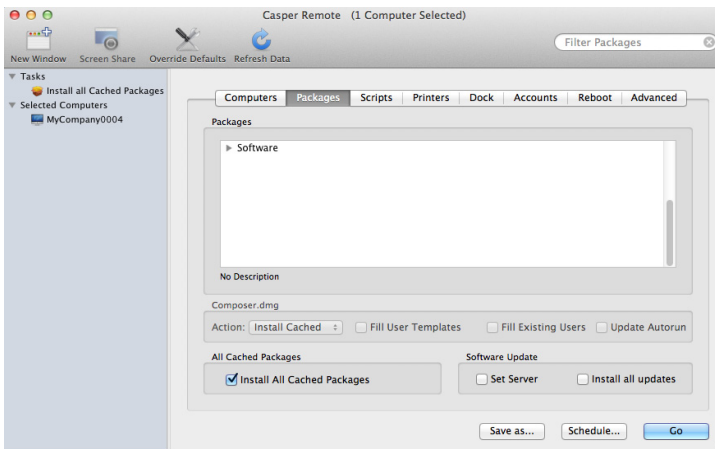
11. Click **Save**.



Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To install all cached packages using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the clients that you want to install the cached packages and select the checkbox next to each one.
3. Click the **Packages** tab and select the **Install All Cached Packages** checkbox.
4. Click **Go**.



Once you complete these steps, Casper Remote installs the cached packages by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote installs the cached packages from the following directory:  
/Library/Application Support/JAMF/Waiting Room/
4. Casper Remote logs out of each client and ends the SSH connection.

# Uninstalling Packages

You can uninstall a package from one or more client computers if the package was uploaded to the Casper Admin application prior to deployment.

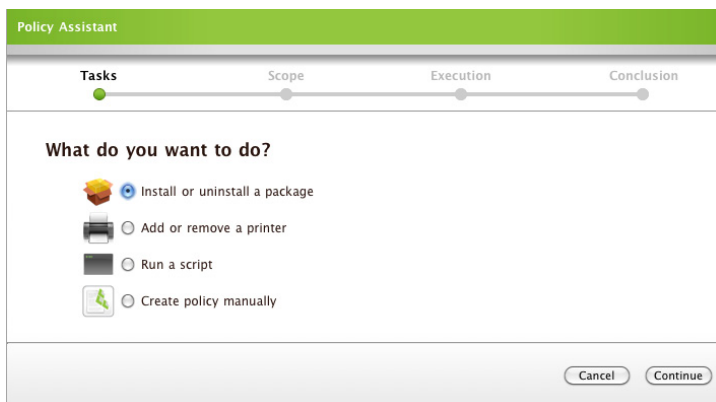
Before using the instructions in this section, index the package and enable the **Allow Uninstall** option. For instructions on how to do this, see both the “Indexing Packages” and “Changing Package Attributes” sections in this guide.

**Note:** You do not need to index the package and enable the **Allow Uninstall** option if you are uninstalling an Adobe CS3/CS4 Installer.

This section explains how to uninstall a package using a policy or Casper Remote.

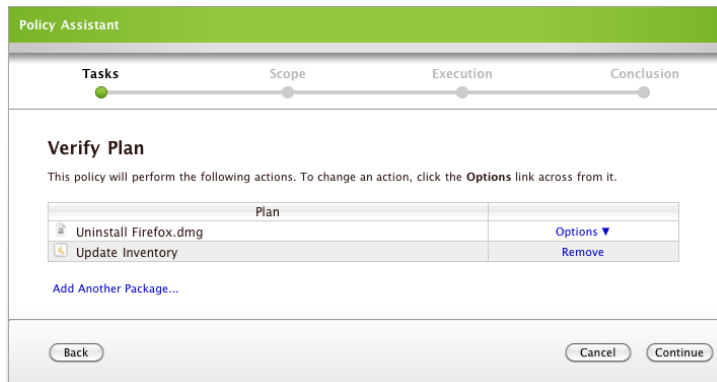
## To configure a policy to uninstall a package using the Policy Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.
5. Select the **Install or uninstall a package** option and click the **Continue** button.



6. Follow the onscreen instructions until you get to the Verify Plan pane. Then, click **Options** and choose "Uninstall" from the menu.

If the package is not indexed and/or the **Allow Uninstall** option is not enabled, the **Uninstall** option is not displayed.



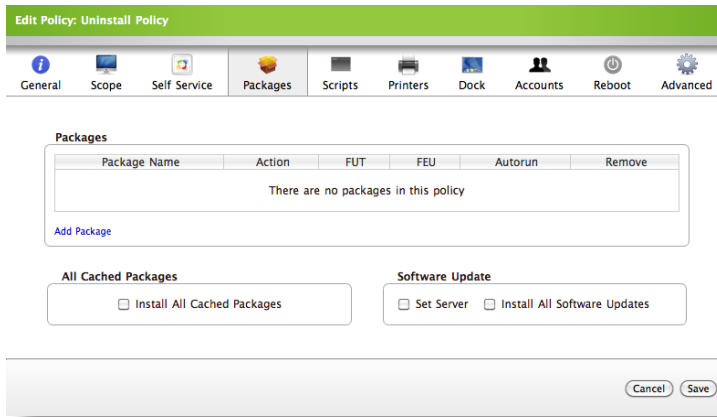
7. Click the **Continue** button and follow the instructions on each pane to configure the rest of the policy.

Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

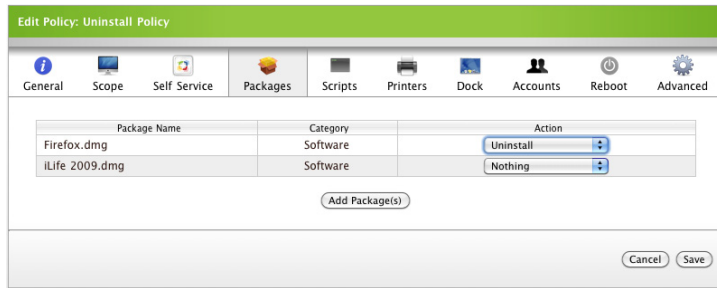
#### To manually configure a policy to uninstall a package:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.

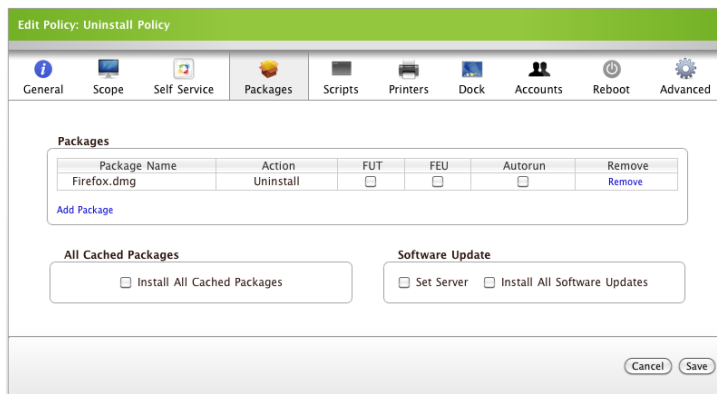
10. Click the **Packages** tab and click the **Add Package** link.



11. Locate the package you want to cache and choose "Uninstall" from the **Action** pop-up menu across from it.  
If the package is not indexed and/or the **Allow Uninstall** option is not enabled, the **Uninstall** option is not displayed.
12. Click the **Add Package(s)** button.



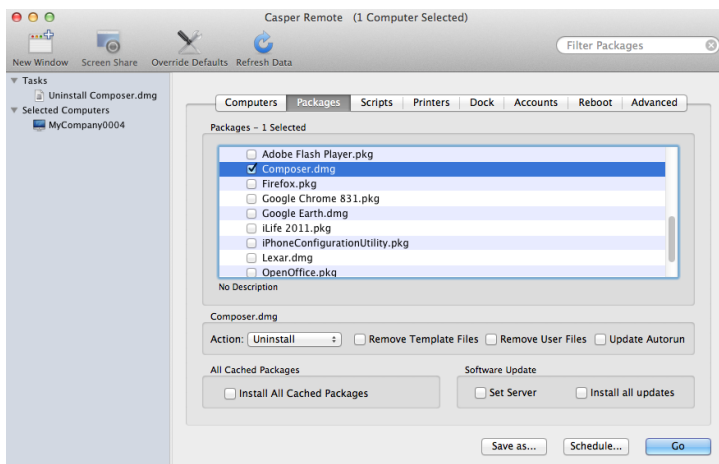
13. Click **Save**.



Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

## To uninstall a package using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the clients that you want to remove the package from and select the checkbox next to each one.
3. Click the **Packages** tab.
4. In the **Packages** list, locate the package you want to uninstall and select the checkbox next to it.
5. Choose "Uninstall" from the **Action** pop-up menu below the list of packages.  
If the package is not indexed and/or the **Allow Uninstall** option is not enabled, the **Uninstall** option is not displayed.
6. Click **Go**.



Once you complete these steps, Casper Remote uninstalls the package from client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote uninstalls the package.
4. Casper Remote logs out of each client and ends the SSH connection.



# Using the Self Healing Feature

In order to utilize the Self Healing feature, you must enforce Self Healing on your client computers.

Before you enforce Self Healing, make sure the following requirements are met:

- The package that contains the triggering file is indexed. (For more information, see the “Indexing Packages” section.)
- The Self Healing feature is enabled. (For more information, see the “Enabling the Self Healing Feature” section.)
- Each client computer on which you want to enforce Self Healing has Autorun data that includes the package that contains the triggering file. (For more information on creating Autorun data, see the section entitled “Using the Autorun Feature”.)

After you enforce Self Healing, a log of each Self Healing event is stored in the JAMF Software Server (JSS).

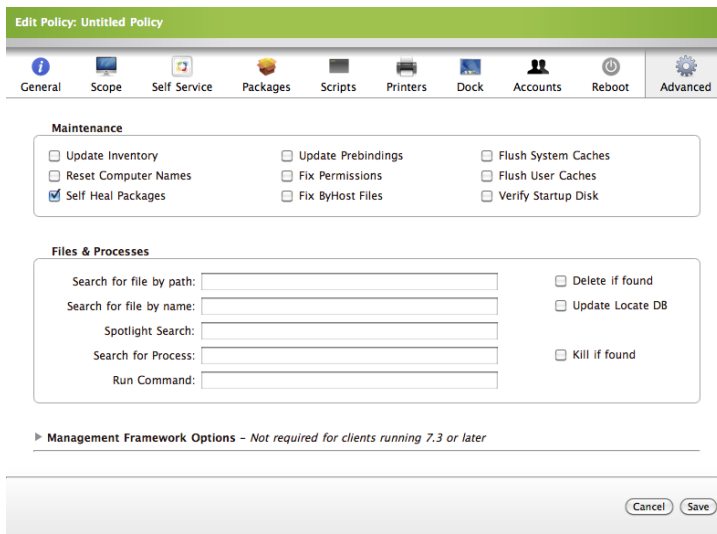
This section explains how to:

- Enforce Self Healing using a policy or Casper Remote
- View Self Healing logs

## To enforce Self Healing using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Advanced** tab and select the **Self Heal Packages** checkbox.

11. Click **Save**.



Client computers run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

**To enforce Self Healing using Casper Remote:**

1. Open Casper Remote.
2. In the **Computers** list, locate the clients that you want to enforce Self Healing and select the checkbox next to each one.
3. Click the **Advanced** tab.
4. Select the **Self Heal Packages** checkbox and click **Go**.

**To view Self Healing logs:**

1. Log in to the JSS with a web browser.
2. Click the **Logs** tab.
3. Click the **Self Healing Logs** link to display a list of Self Healing logs.
4. Click the **View Logs** link across from a log to see additional information.

---

# Remote Control

## Overview of Remote Control

The Casper Suite integrates screen sharing through the Casper Remote application. Casper Remote automates the tools built into Mac OS X to allow screen sharing sessions between computers.

Screen sharing sessions are tunneled through an SSH connection. These sessions are centrally authenticated and logged and do not require special software to be installed on client computers. For added security, you can configure the screen sharing server to run only for the duration of the session.

# Requirements

To share the screen of another computer, the computer you want to share screens with must meet the following requirements:

- SSH is activated on the computer.
- The computer is enrolled with the JAMF Software Server (JSS).
- The computer is able to contact the JSS at the DNS name or IP address specified in the Preference window in Casper Remote.

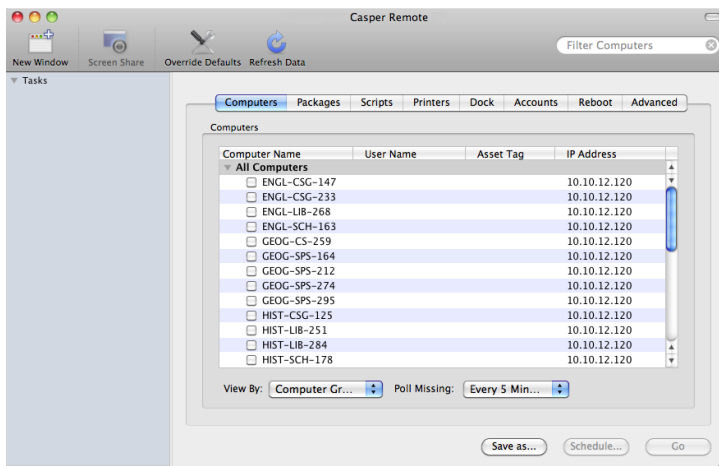
In addition, you must use an account with screen sharing privileges to log in to Casper Remote.

# Using Screen Sharing

This section explains how to share the screen of another computer on your network.

## To share the screen of another computer:

1. Open Casper Remote.
2. Enter credentials for a JSS user account that has screen sharing privileges and then click **OK**.
3. In the **Computers** list, select the computer whose screen you want to share. (You do not need to select the checkbox next to the name of the computer.)



4. Click the **Screen Share** button in the toolbar.
5. If both your computer and the client computer have Mac OS X 10.7 or later, you are prompted to choose a screen sharing option.
  - Choose "Ask to share the display" to allow the user to see the screen sharing session.
  - Choose "Connect to a virtual display" to hide the screen sharing session.

Depending on your screen sharing privileges, users may need to accept a screen sharing request before you can share their screen.

# How Screen Sharing Works

Casper Remote performs the following steps to create a secure connection for screen sharing:

1. Casper Remote creates an SSH connection to the client computer.
2. Casper Remote checks the computer for the most current version the following file:  
`/usr/sbin/jamf`  
If the file is out of date or missing, Casper Remote installs the most current version over secure copy or HTTP depending on your preference settings.
3. Casper Remote checks the computer for the following file and verifies that it contains the correct information:  
`/Library/Preferences/com.jamfsoftware.jss.plist`  
If the file does not exist or contains incorrect information, Casper Remote automatically creates the file.
4. The jamf binary verifies that the account used to initiate the connection has screen sharing privileges.
5. If necessary, the user is prompted to accept the screen sharing session.
6. The JSS logs the connection.
7. Casper Remote starts the Screen Sharing service.
8. Casper Remote creates a temporary account with limited privileges and uses it for the screen sharing session.
9. Casper Remote starts the Screen Sharing application and connects to the computer over an SSH connection.
10. When the Screen Sharing window is closed, Casper Remote deletes the temporary account, stops the screen sharing service if it was started, and logs out of the SSH connection.  
If the SSH connection is terminated before these tasks take place, a launch daemon performs them within 60 seconds.

# Settings and Security Management

## Managed Preferences

Managed Preferences allow you to specify the value for each key in a domain. These settings are stored in the directory service node for each account or client computer.

The JAMF Software Server (JSS) reads Managed Preference templates from manifest files bundled with the JSS. You can also upload manifest, or PLIST, files to create new Managed Preferences or import manifests from the Manifest Destiny project hosted at <https://code.google.com/hosting/>.

Managed Preferences are assigned to computers and users using Managed Preference profiles. This allows you to change the scope of Managed Preferences or disable a large number of Managed Preferences quickly.

Managed Preferences can be applied at the following levels:

- User-level enforced
- User-level every login
- User-level at next login only
- System-level enforced
- Unmanaged

If you've applied Managed Client Extension settings (MCX) in Apple's Workgroup Manager, you may be familiar with the following levels:

- Always
- Often
- Once
- Always (Applied to a computer object)
- Unset

The following table shows each level, its Workgroup Manager counterpart, whether it requires a custom application to be observed, and how it is applied.

Casper Suite Managed Preference Levels	Workgroup Manager Managed Preference Levels	Requires Application Level Support	Applied At
User-level enforced	Always	Yes	Login with a login hook
User-level every login	Often	No	Login with a login hook
User-level at next login only	Once	No	Login with a login hook
Computer-level enforced	Always (Applied to a computer object)	Yes	Reboot with a startup script
Unmanaged	Unset	No	Login or reboot

This section explains how the Casper Suite’s Managed Preferences may affect MCX settings from third-party providers. It also explains domains, keys, and values as they relate to Managed Preferences.

This section also explains how to:

- Enable Managed Preferences
- Create a Managed Preference profile
- Create a Managed Preference from a template
- Duplicate a Managed Preference
- Upload a manifest or PLIST file
- Import a Managed Preference from Manifest Destiny
- Create a Managed Preference manually

## Compatibility with Third-Party MCX Providers

In some cases, Managed Preferences from the Casper Suite can interfere with or be interfered with by MCX settings from a third-party provider. Tested third-party providers include:

- Open Directory (Built-in binding)
- Active Directory (Built-in binding)
- Likewise
- ADmitMac
- Centrify



The following table shows how Managed Preferences (in OS X v10.6 and later) affect MCX settings from third-party providers.

	Open Directory	Active Directory	Likewise	ADmitMac	Centrify
Local Home	Works together	Works together	Works together	Works together	Works together
Network Home	Works together	Works together	N/A	Works together	N/A
Mobile Home	Nothing applied from JSS	Works together	Nothing applied from JSS	Nothing applied from JSS	Nothing applied from JSS

## Understanding Domains, Keys, and Values

Most applications written for Mac OS X store preferences in a property list or PLIST file. Each PLIST file represents a domain that contains multiple keys and values.

For example, each user has a PLIST file that determines the appearance of their Dock. This file is located in the user home directory in:

```
/Library/Preferences/com.apple.dock.plist
```

In this example, the domain for the file is:

```
com.apple.dock
```

The key that determines if the Automatically hide and show the Dock feature is enabled is:

```
autohide
```

There is a command-line utility called Defaults that allows you to read and write PLIST files. Apple's Developer Tools also contain an application called Property List Editor that allows you to view and edit PLIST files.

Using the information from the previous example, the preferences settings on your account can be displayed by executing the following command from Terminal:

```
defaults read com.apple.dock autohide
```

This command returns the value of the `autohide` key for the `com.apple.dock` domain.

If the command returns a "0", the feature is not enabled. If the command returns a "1", the feature is enabled.

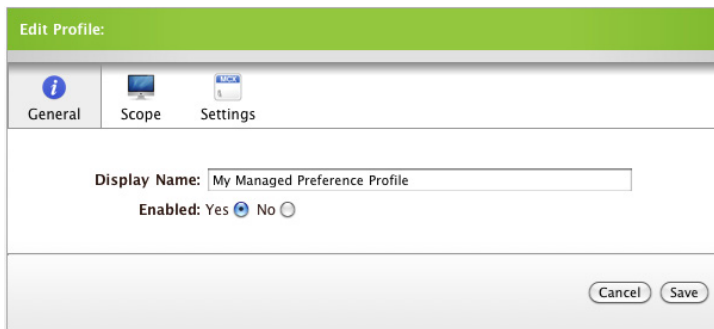
### To enable Managed Preferences:

1. Log in to the JSS with a web browser.

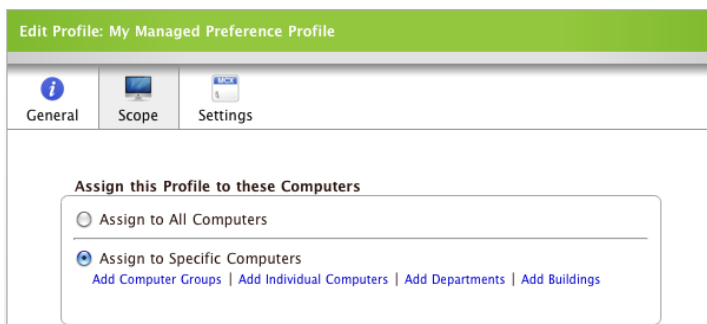
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. To apply Managed Preferences at computer level:
  - a. Click the **Startup Item** tab.
  - b. Select the **Create startup item** checkbox.
  - c. Select the **Apply Computer Level Enforced Managed Preferences** checkbox.
5. To apply Managed Preferences at user level:
  - a. Click the **Login/Logout Hooks** tab.
  - b. Select the **Create login and logout hooks** checkbox.
  - c. Select the **Apply User Level Managed Preferences** checkbox.
6. Click the **Save** button.

**To create a Managed Preference profile:**

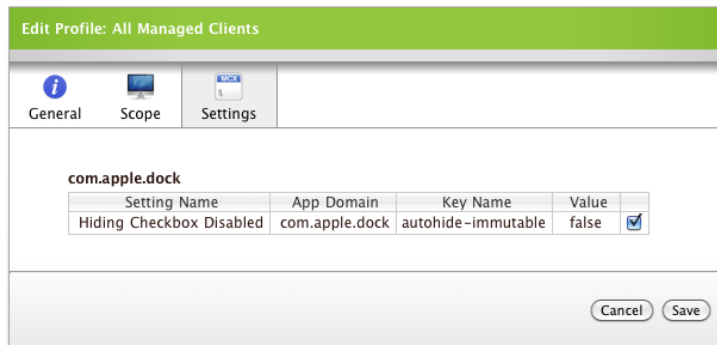
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Managed Preferences** link.
4. Click the **Create Managed Preference profile** button.
5. Enter a display name for the profile.
6. Select **Yes** to enable it.



7. Click the **Scope** tab and assign computers or user groups to the scope.

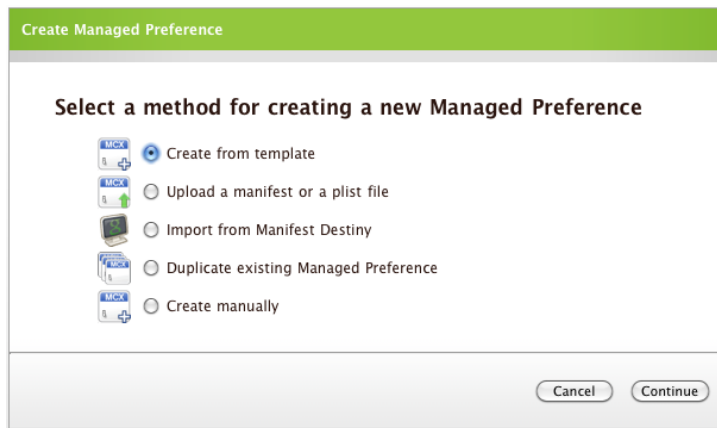


8. Click the **Settings** tab.
9. Select the checkbox across from the preferences you want to include in the profile and click the **Save** button.

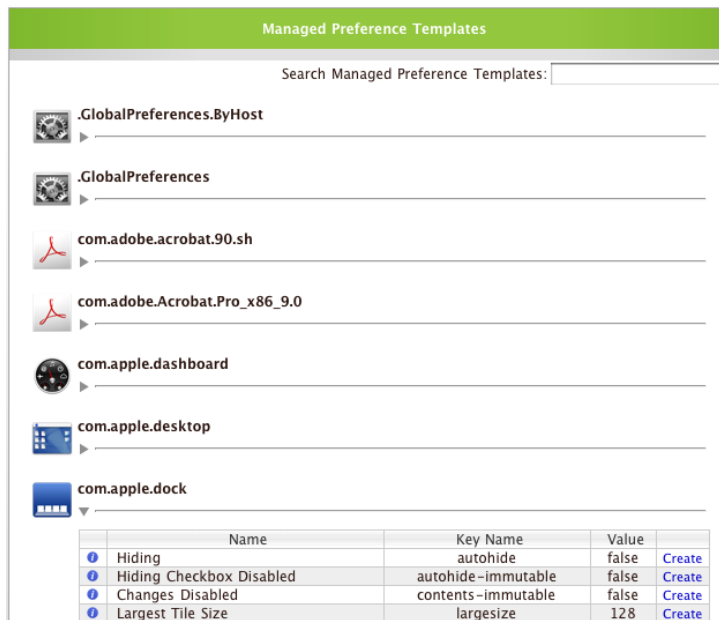


#### To create a Managed Preference from a template:

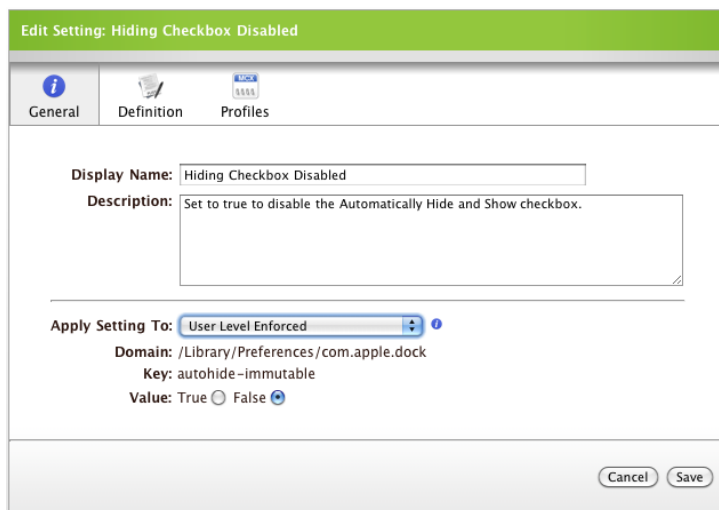
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Managed Preferences** link.
4. Click the **Create Managed Preference** button.
5. Select the **Create from template** option and click the **Continue** button.



- Click the disclosure triangles to locate the Managed Preference you want to create and click the **Create** link across from it.



- Choose a level at which to apply the preference from the **Apply Setting To** pop-up menu.
- Select a value for the preference.

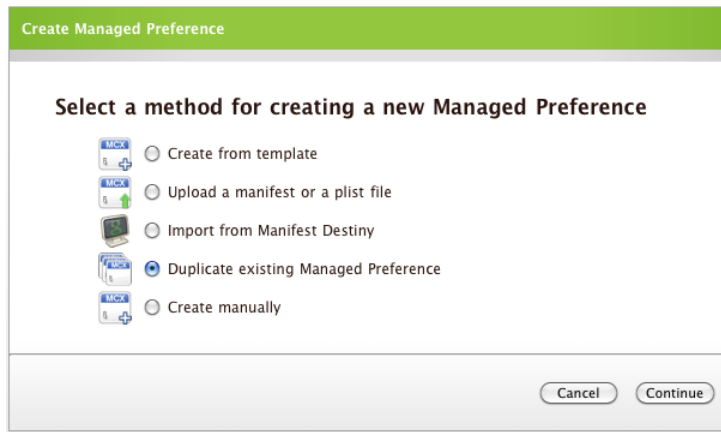


- Click the **Profiles** tab and select the checkbox across from the profile(s) you want to assign the preference to.
- Click the **Save** button.

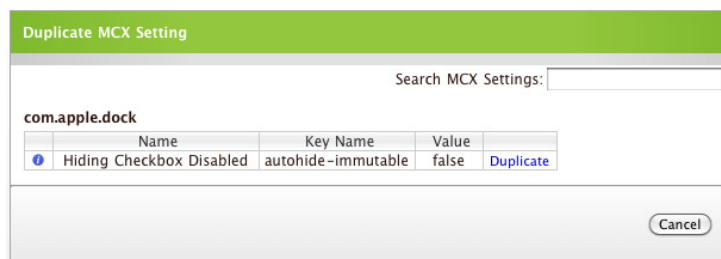
#### To duplicate a Managed Preference:

- Log in to the JSS with a web browser.
- Click the **Management** tab.

3. Click the **Managed Preferences** link.
4. Click the **Create Managed Preference** button.
5. Select the **Duplicate existing Managed Preference** option and click the **Continue** button.



6. Click the **Duplicate** link across from the preference you want to duplicate.

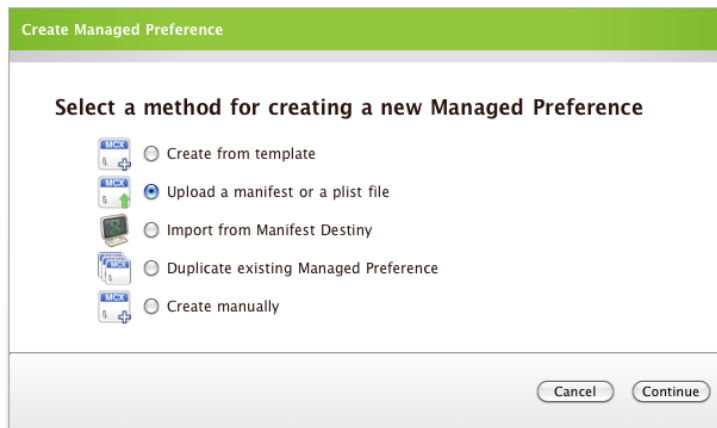


7. Make changes if necessary.
8. Click the **Save** button.

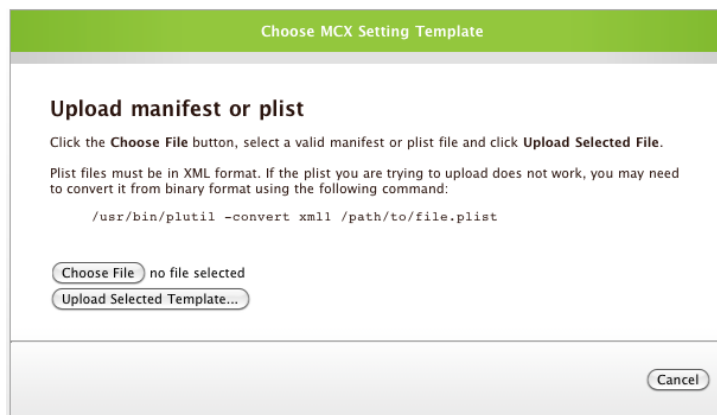
**To upload a manifest or PLIST file:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Managed Preferences** link.
4. Click the **Create Managed Preference** button.

5. Select the **Upload a manifest or plist file** option and click the **Continue** button.



6. Click the **Choose File** button.

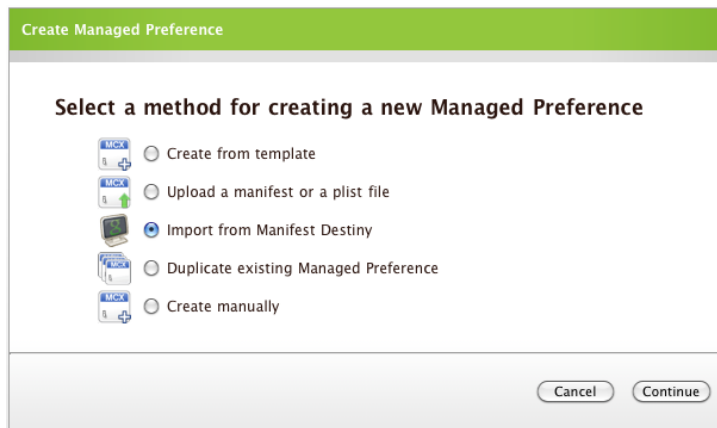


7. Select the file you want to upload, and then click the **Upload Selected Template** button.
8. Click **Save**.

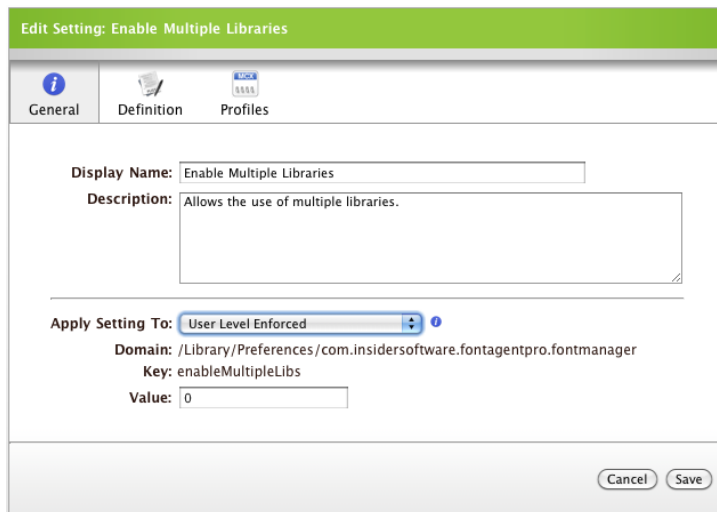
#### To import a Managed Preference from Manifest Destiny:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Managed Preferences** link.
4. Click the **Create Managed Preference** button.

5. Select the Import from **Manifest Destiny** option and click the **Continue** button.



6. Click the disclosure triangles to locate the Managed Preference you want to create, and click the **Create** link across from it.
7. Choose a level at which to apply the preference from the **Apply Setting To** pop-up menu.
8. Select a value for the preference.

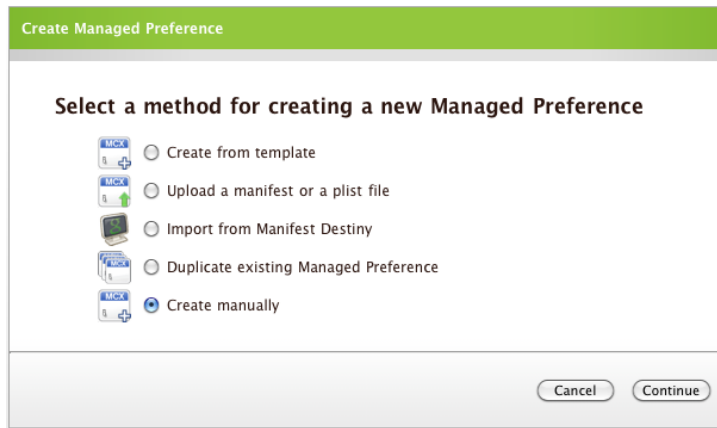


9. Click the **Profiles** tab and select the checkbox across from each profile you want to assign the preference to.
10. Click the **Save** button.

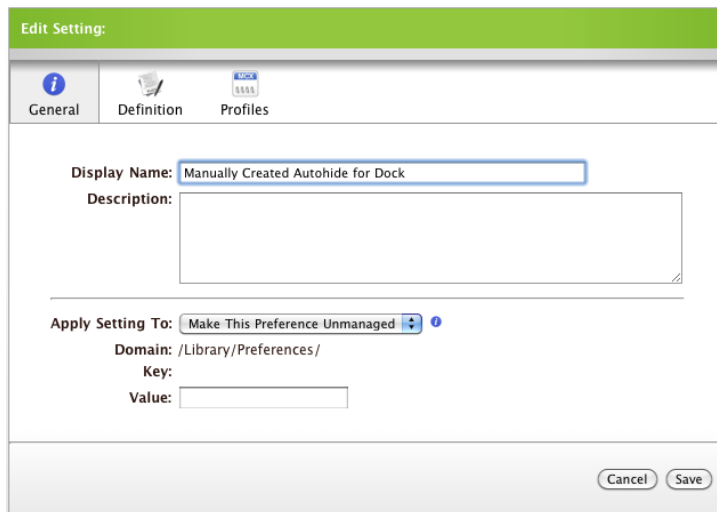
#### To create a Managed Preference manually:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Managed Preferences** link.
4. Click the **Create Managed Preference** button.

5. Select the **Create manually** option and click the **Continue** button.



6. Enter a display name for the preference.
7. (Optional) Enter a description of the preference.



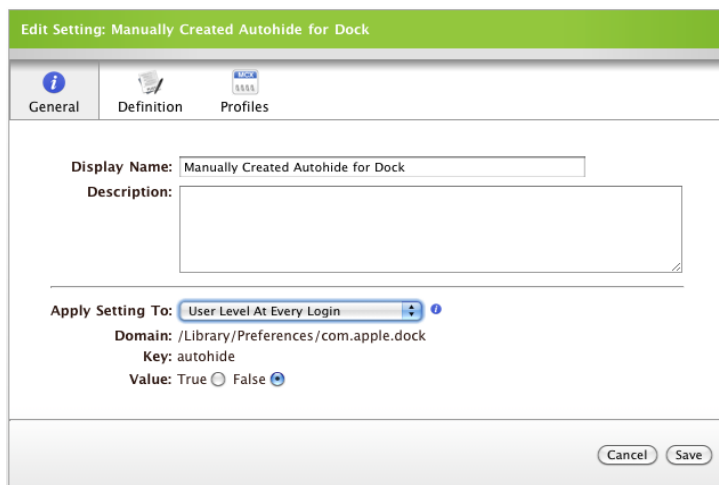
8. Click the **Definition** tab and select **Allowed** or **Not Allowed** for each level.

**Note:** Most custom settings only work when they are applied at user level or user-level enforced. Managed Preferences applied at system-level enforced require applications be custom written for them.

9. Enter the domain. For example, "com.apple.dock".
10. Enter the key name. For example, "autohide".
11. Choose a key type from the **Key Type** pop-up menu.
12. Click the **General** tab.
13. Choose a level at which to apply the preference from the **Apply Setting To** pop-up menu.



14. Select a value for the preference.



15. Click the **Profiles** tab and select the checkbox across from each profile you want to apply the preference to.
16. Click the **Save** button.

# Managing Mac OS X Configuration Profiles

The JAMF Software Server (JSS) allows you to create, install, update, and remove Mac OS X configuration profiles.

## About Mac OS X Configuration Profiles

Mac OS X configuration profiles are XML files (.mobileconfig) that define groups of settings for computers and users. You create a configuration profile to apply to computers (computer-level) or users (user-level). Each level has a unique set of payloads and a few that are common to both. The settings are applied at the specified level when the profile is installed.

To install a configuration profile, you assign computers or users to its scope. Computer-level profiles are installed when computers in the scope contact the JSS. User-level profiles are installed when users in the scope log in to their computers with credentials for a directory account and a login hook is present.

## Requirements

To install a Mac OS X configuration profile, you need:

- Computers with OS X v10.7 or later
- An Apple Push Notification service (APNs) certificate uploaded to the JSS  
See the “Apple Push Notification Service Certificate” section in “Configuring the Computer Management Framework” for more information.
- The following security options enabled in the JSS:
  - Certificate-based communication
  - Push notifications for OS X v10.7 or later clientsSee the “Security” section in “Configuring the Computer Management Framework” for more information.
- *(For user-level profiles only)* Client computers that are bound to a directory service  
Tested directory bindings include:
  - Active Directory
  - Open Directory
  - ADmitMacSee “Creating Directory Bindings” for more information.
- *(For user-level profiles only)* Login hooks configured in your environment  
See the “Login and Logout Hooks” section in “Configuring the Computer Management Framework” for more information on creating login hooks with the Casper Suite.

## Creating and Installing Mac OS X Configuration Profiles

The JSS allows you to create configuration profiles using an interface similar to Apple's Profile Manager. When you are done creating the profile, you can install it by assigning computers or users to the scope.

**Note:** Some payloads and settings available in Profile Manager cannot be configured with the JSS.

Before creating a configuration profile, you should have basic knowledge of configuration profile payloads and settings and how they affect computers. Most payloads and settings are explained in Apple's Profile Manager Help documentation, available at:

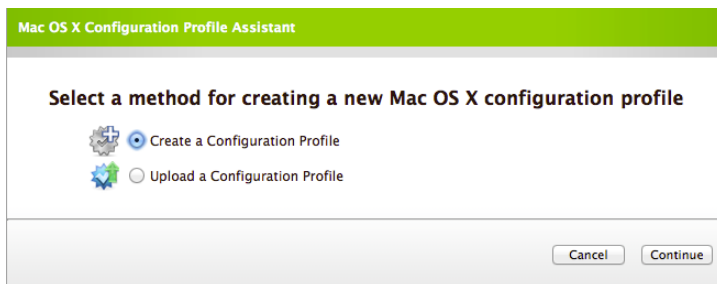
<https://help.apple.com/profilemanager/mac/10.7/#>

Some configuration profiles settings can only be configured with the JSS. For more information on these settings, see the following Knowledge Base article:

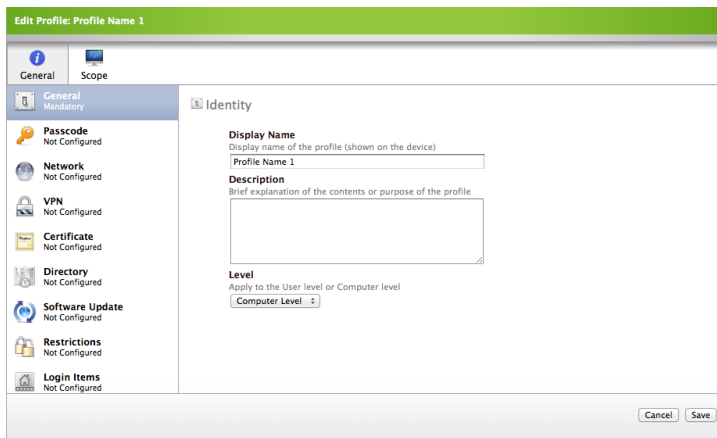
<https://jamfnation.jamfsoftware.com/article.html?id=217>

**To create and install a Mac OS X configuration profile using the JSS:**

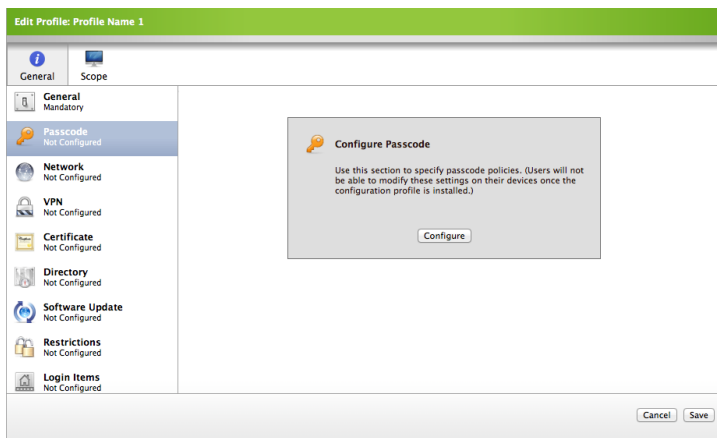
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Configuration Profiles** link.
4. Click the **Add Profile** button.
5. Select **Create a Configuration Profile**, and then click **Continue**.



6. Enter a display name and description for the profile.

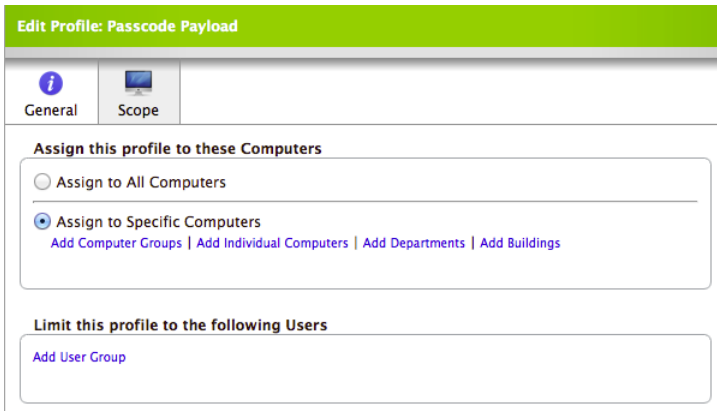


7. Choose “Computer-level” or “User-level” from the **Level** pop-up menu.
8. In the payloads list, select the payload that you want to add, and then click **Configure**. The payloads list displays the payloads that you can configure for the selected level.



9. Use the options and fields in the main pane to configure settings for the payload. There are several variables that you can use to dynamically customize a payload. For more information, see the “Variables for Mac OS X Configuration Profiles” section.
10. To add additional payloads, repeat steps 8 and 9.

- Click the **Scope** tab and assign computers or users to the scope.



- Click **Save**.

Computer-level profiles are installed the next time computers in the scope contact the JSS. User-level profiles are installed the next time users in the scope log in to their computers.

## Variables for Mac OS X Configuration Profiles

There are several variables that you can use to dynamically customize the payloads in a Mac OS X configuration profile.

Enter a variable into any text field in a payload to dynamically populate information about the computers to which you are distributing the profile. When the profile is installed, the variable is translated to the actual value stored in the JSS.

Variable	Computer Information
\$COMPUTERNAME	Computer name
\$UDID	UDID
\$SERIALNUMBER	Serial number
\$USERNAME	For a computer-level configuration profile, the username stored in the computer's location information in the JSS For a user-level configuration profile, the username for the user logging in
\$REALNAME	Real name
\$EMAIL	Email address
\$PHONE	Phone
\$POSITION	Position
\$ROOM	Room

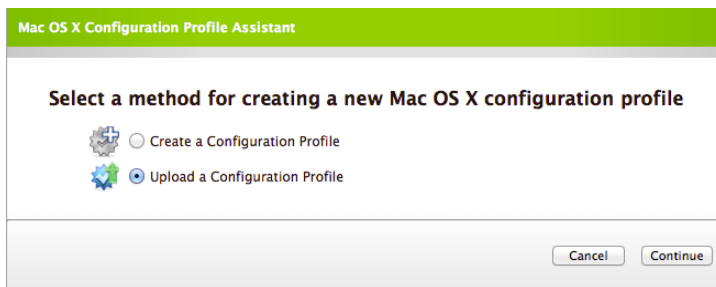
# Installing Mac OS X Configuration Profiles Created with Profile Manager

To install a Mac OS X configuration profile created with Profile Manager, you must upload the profile to the JSS, and then assign computers or users to the scope.

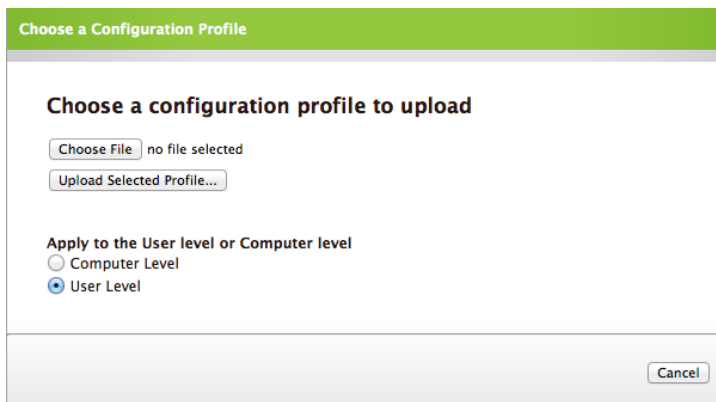
**Note:** Some payloads and settings configured with Profile Manager are not displayed in the JSS. Although you cannot view or edit these payloads, they are applied when the profile is installed.

To install a Mac OS X configuration profile created with Profile Manager:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Configuration Profiles** link.
4. Click the **Add Profile** button.
5. Select **Upload a Configuration Profile**, and then click **Continue**.

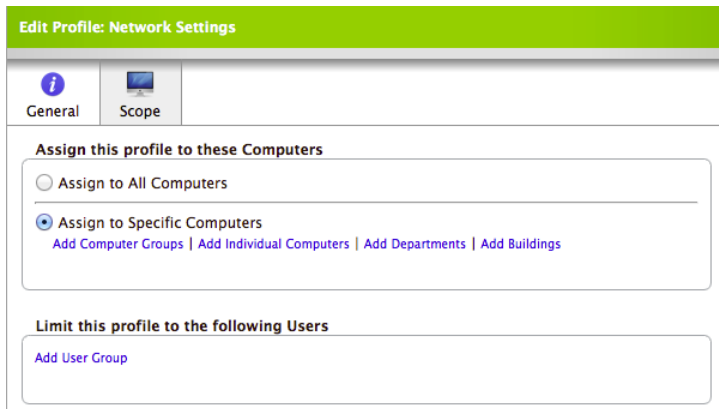


6. Choose whether to apply the profile at computer or user-level by selecting **Computer Level** or **User Level**. Payloads that do not apply to the specified level are permanently removed from the profile.



7. Click **Choose File** and select the profile (.mobileconfig) that you want to upload. Then, click **Upload Selected Profile**.
8. Verify the display name for the profile and enter a description if desired. Then, click **Save**.

9. Click the **Edit** link across from the profile you uploaded.
10. If needed, use the payloads list to add or modify payloads.
11. Click the **Scope** tab and assign computers or users to the scope.



12. Click **Save**.

Computer-level profiles are installed the next time computers in the scope contact the JSS. User-level profiles are installed the next time users in the scope log in to their computers.

## Updating Mac OS X Configuration Profiles

To update a Mac OS X configuration profile, use the JSS to add, modify, or remove payloads as needed.

**Note:** Some payloads and settings configured in Profile Manager are not displayed in the JSS.

### To update a Mac OS X configuration profile:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Configuration Profiles** link.
4. Click the **Edit** link across from the profile.

**Important:** Choosing a new option from the **Level** pop-up menu permanently removes existing level-specific payloads.

5. Use the payloads list to add, modify, or remove payloads as needed.
6. Click **Save**.

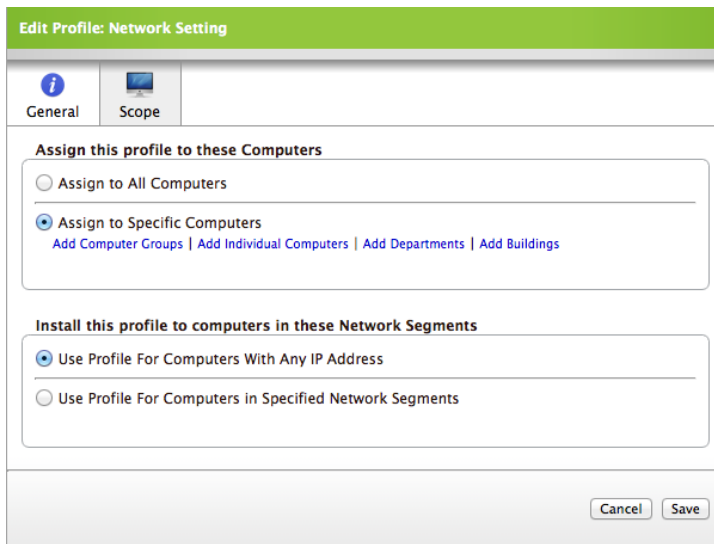
Computer-level profiles are updated the next time computers in the scope contact the JSS. User-level profiles are updated the next time users in the scope log in to their computers.

## Removing Mac OS X Configuration Profiles

To remove a Mac OS X configuration profile from a computer or for a user, remove the computer or user from the scope. When the profile is removed, all settings associated with the profile are also removed.

**To remove a Mac OS X configuration profile:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Configuration Profiles** link.
4. Click the **Edit** link across from the profile.
5. Click the **Scope** tab and remove computers or users from the scope as needed.



6. Click **Save**.

## Deleting Mac OS X Configuration Profiles

Deleting a Mac OS X configuration profile from the JSS removes the profile and its settings from all computers or users in the scope.

**To delete a Mac OS X configuration profile from the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Configuration Profiles** link.
4. Click the **Delete** link across from the profile, and then click the **Delete** button to confirm.



# Running Remote Commands for Mac OS X Computers

The JAMF Software Server (JSS) allows you to manage the security of Mac OS X computers by running the following commands:

- **Remote Lock**—Logs the user out of the computer, reboots the computer, and keeps the computer in a locked state. To unlock the computer, the user must enter a passcode specified by the administrator.
- **Remote Unenroll**—Unenrolls the computer. See "Enrolling Mac OS X Computers with the JSS" for instructions on how to enroll a computer.
- **Remote Wipe**—Permanently erases all data on the computer and deactivates it. To restore the computer to the original factory settings, you must enter a passcode specified by the administrator, reinstall the operating system, and then reboot the computer.

For detailed information on Mac OS X Lion Recovery, see the following Apple Knowledge Base article: <https://support.apple.com/kb/HT4718>

**Note:** Running a remote unenroll or remote wipe command on a computer does not remove the computer from the JSS or modify its inventory information.

You can also use the JSS to view the status of remote commands and cancel a remote command that is pending.

## Requirements

To run remote commands for Mac OS X computers, you need:

- Computers with OS X v10.7 or later and a Recovery Partition
- An Apple Push Notification service (APNs) certificate uploaded to the JSS  
See the "Apple Push Notification Service Certificate" section in "Configuring the Computer Management Framework" for more information.
- The following security options enabled in the JSS:
  - Certificate-based communication
  - Push notifications for OS X v10.7 or later clientsSee the "Security" section in "Configuring the Computer Management Framework" for more information.

- A JSS user account with privileges to run remote commands for Mac OS X computers.  
Remote command privileges are not granted by default. See "Managing JSS User Accounts" for instructions on how to grant privileges to a JSS user account.

## Running Remote Commands


You can run a remote command for a Mac OS X computer by using the icons displayed when viewing a Computer Details report.

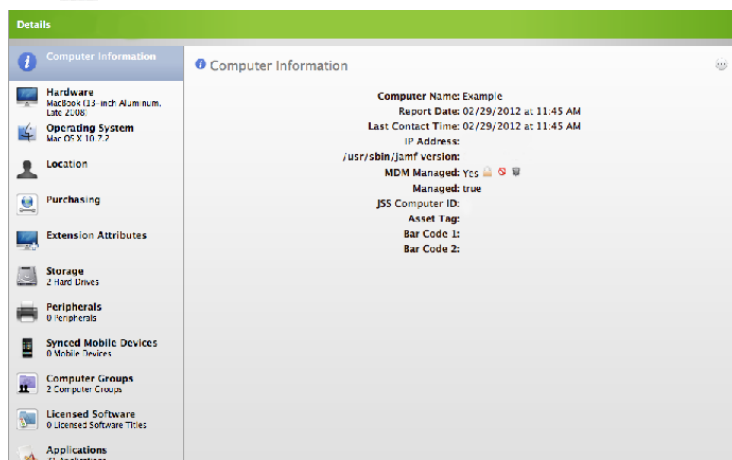
### To run a remote command for a Mac OS X computer:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab and perform a simple or advanced computer search. See the "Performing Simple Computer Searches" or "Performing Advanced Computer Searches" section in "Searching Computers" for complete instructions.
3. Find the computer that you want to run the remote command, and click the **Details** link across from it.
4. Next to the **MDM Capable** field, click the icon for the command you want to run.

The  icon runs the remote lock command.

The  icon runs the remote unenroll command.

The  icon runs the remote wipe command.



5. Follow the onscreen instructions to configure the rest of the command.

The remote command runs on the computer the next time the computer contacts the JSS.

## Viewing the Status of Remote Commands

The JSS allows you to view the status of remote commands for a Mac OS X computer.

### To view the status of remote commands for a Mac OS X computer:

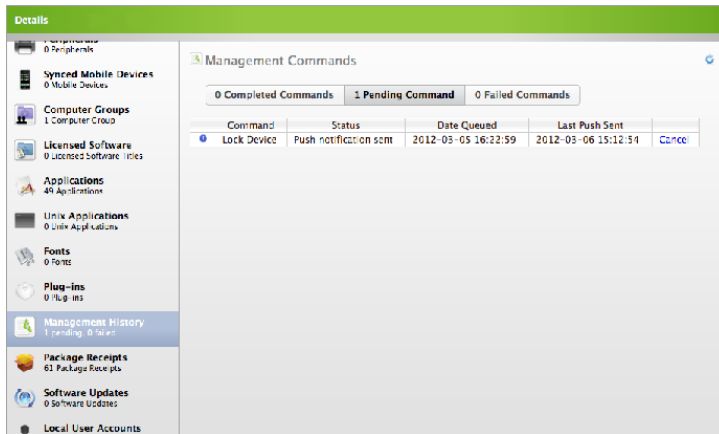
1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab and perform a simple or advanced computer search. See the "Performing Simple Computer Searches" or "Performing Advanced Computer Searches" section in "Searching Computers" for complete instructions.
3. Find the computer that you want to view commands for, and click the **Details** link across from it.
4. Click Management History in the list of categories.
5. Use the **Completed Commands**, **Pending Commands**, and **Failed Commands** tabs to view the status of remote commands.

## Canceling Remote Commands

The JSS allows you to cancel a remote command if the command is in a pending state.

To cancel a remote command for a Mac OS X computer:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab and perform a simple or advanced computer search. See the "Performing Simple Computer Searches" or "Performing Advanced Computer Searches" section in "Searching Computers" for complete instructions.
3. Find the computer that you sent the command to, and click the **Details** link across from it.
4. Click Management History in the list of categories.
5. Click the **Pending Commands** tab.
6. Find the remote command that you want to cancel, and click the **Cancel** link across from it.



7. When prompted, click **OK** to confirm the cancelation.

# Running Scripts

You can run virtually any type of script on client computers. Some of the most commonly used scripts are AppleScript, Perl, and Bash.

Scripts can be run at two priorities:

- **Run before**—Runs the script at the beginning of the policy or Casper Remote session.
- **Run after**—Runs the script just before the end of the policy or Casper Remote session.

By default, each script is passed three parameters:

- Target Drive
- Username (at login or logout)
- Computer Name

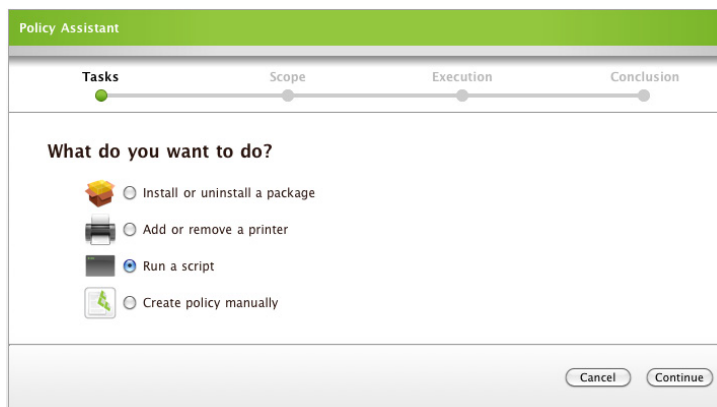
You can pass up to eight additional parameters when running the script.

Before you run a script on a remote computer, you must add the script to the JAMF Software Server (JSS) using Casper Admin.

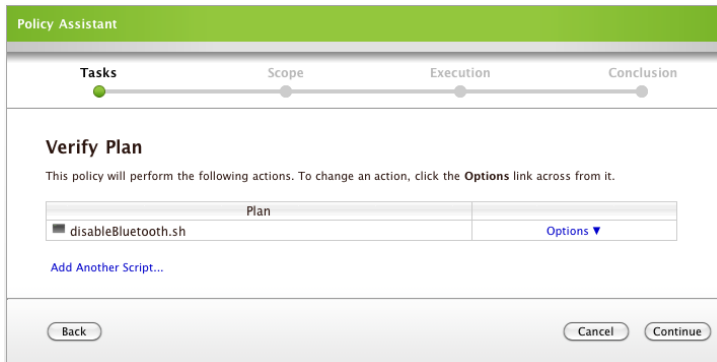
This section explains how to run a script using a policy or Casper Remote.

## To configure a policy to run a script using the Policy Assistant:

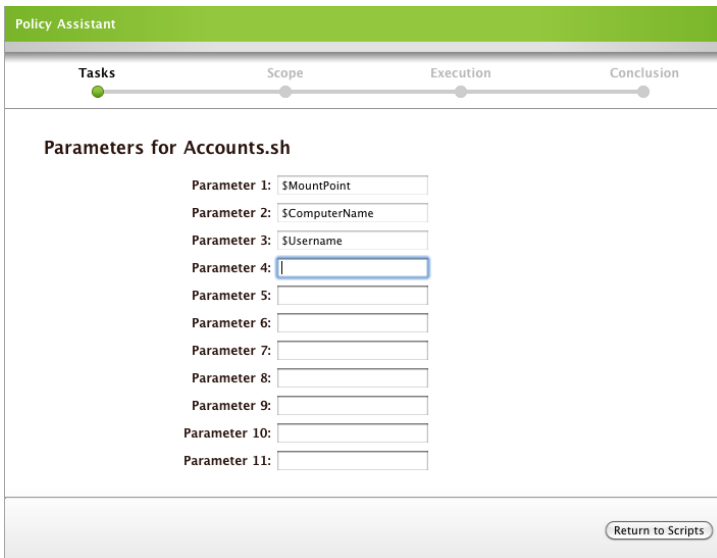
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.
5. Select the **Run a script** option and click the **Continue** button.



6. If you want to specify parameters for the script:
  - a. Follow the onscreen instructions until you get to the Verify Plan pane.
  - b. Click **Options**, and then click **Specify Parameters Values**.



- c. Enter any parameters you want to pass to the script, and then click the **Return to Scripts** button.



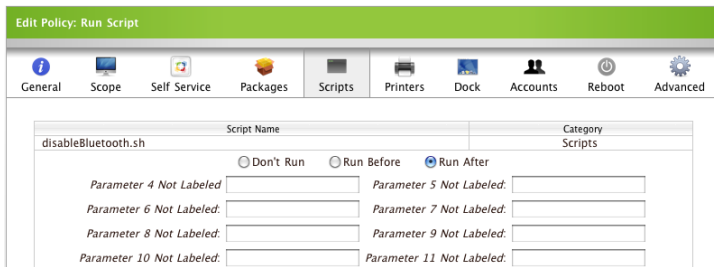
7. Follow the onscreen instructions to configure the rest of the policy.
8. If you want to set a priority for the script:
  - a. Click the **Edit Manually** button on the Conclusion pane.
  - b. Click the **Scripts** tab and select the **Run After** or **Run Before** option for the script.
  - c. Click the **Save** button.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

**To manually configure a policy to run a script:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.

3. Click the **Policies** link.
4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Scripts** tab and click the **Add Script** link.
11. Locate the script you want to run in the list of scripts and select the **Run Before** or **Run After** option.



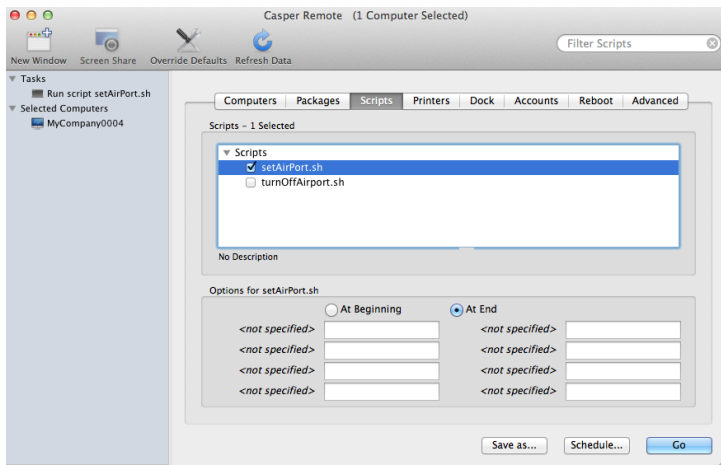
12. In the parameter text fields, enter any parameters you want to pass to the script. Any parameter labels entered in Casper Admin are displayed here.
13. Click the **Add Script(s)** button.
14. Click **Save**.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To run a script using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers you want to run the script on and select the checkbox next to each one.
3. Click the **Scripts** tab.
4. In the **Scripts** list, locate the script you want to run and select the checkbox next to it.

5. Choose when to run the script by selecting the **At Beginning** or **At End** option.



6. Enter any parameters you want to pass to the script.
7. Any parameter labels entered in Casper Admin are displayed here.
8. Click **Go**.

Once you complete these steps, Casper Remote runs the script on client computers by performing the following steps:

1. Casper Remote logs in to each computer using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote runs the script.
4. Casper Remote logs out of each client and ends the SSH connection.

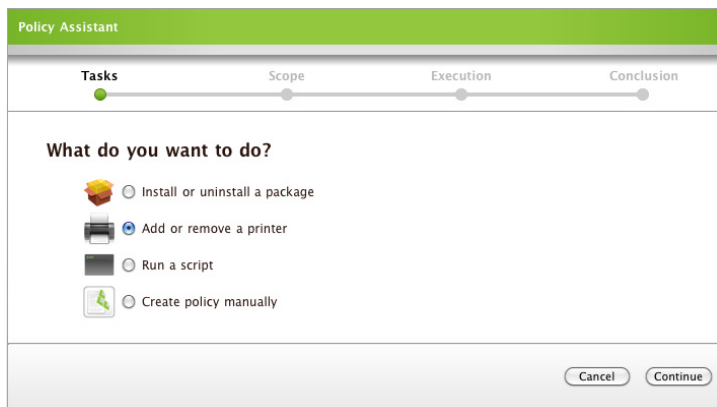
# Managing Printers

Before you add or remove a printer from a remote computer, you must add the printer to the JAMF Software Server (JSS) using Casper Admin.

This section explains how to add and remove a printer using a policy or Casper Remote.

## To configure a policy to add or remove a printer using the Policy Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button in the toolbar.
5. Select the **Add or remove a printer** option and click the **Continue** button.



6. If you want to remove a printer:
  - a. Follow the onscreen instructions until you get to the Verify Plan pane.
  - b. Click **Options**, and then click **Remove Printer from Computer**.
  - c. Click **Continue**.If you want to add a printer, skip this step.
7. Follow the instructions on each pane to configure the rest of the policy.

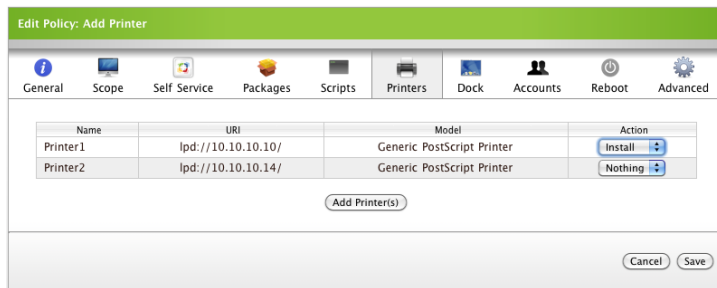
Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

## To manually configure a policy to add or remove a printer:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.



4. Create a policy or edit an existing one.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Printers** tab and click the **Add Printer** link.
11. Locate the printer and choose "Install" or "Delete" from the **Action** pop-up menu across from it.



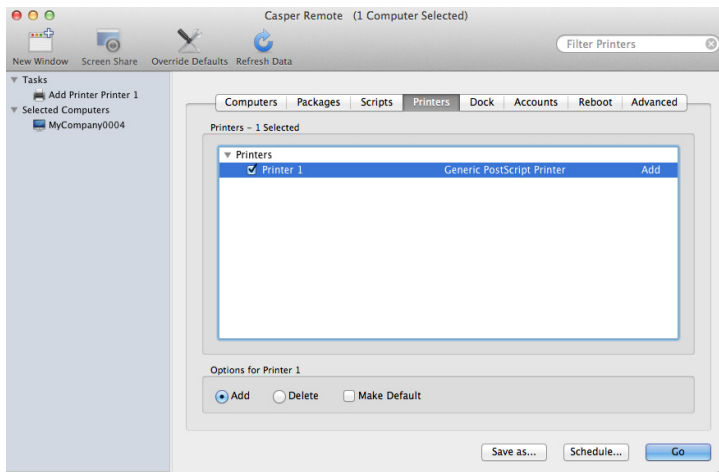
12. Click the **Add Printer(s)** button.
13. If you want to make the printer you are adding the default printer, select the **Make Default** option across from it.
14. Click the **Save** button.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To add or remove a printer using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, select the checkbox next to each computer you want to add the printer to or remove it from.
3. Click the **Printers** tab.
4. Select the checkbox next to the printer you want to add or remove.

5. Select the **Add** or **Delete** option below the list.



6. If you want to make the printer you are adding the default printer, select the **Make Default** option.
7. Click **Go**.

Once you complete these steps, Casper Remote adds or removes the printer from client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote adds or removes the printer.
4. Casper Remote logs out of each client and ends the SSH connection.

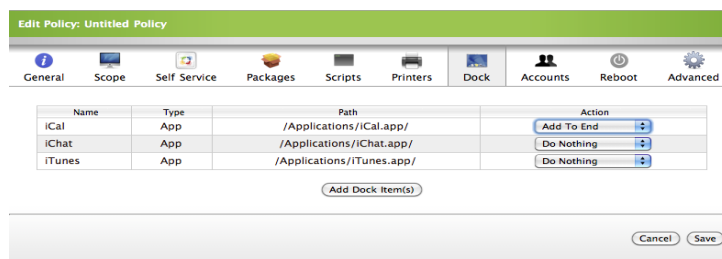
# Managing Dock Items

Before you add an item to the Dock on a remote computer, the item must be added to the JAMF Software Server (JSS) using Casper Admin and displayed as a deployable object.

This section explains how to add and remove a Dock item using a policy or Casper Remote.

## To add or remove a Dock item using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Dock** tab and click the **Add Dock Item** link.
11. Locate the item and choose an action from the **Action** pop-up menu:
  - If you want to add the item, choose "Add to Beginning" or "Add to End" depending on where you want the item to appear in the Dock.
  - If you want to remove the item, choose "Remove".



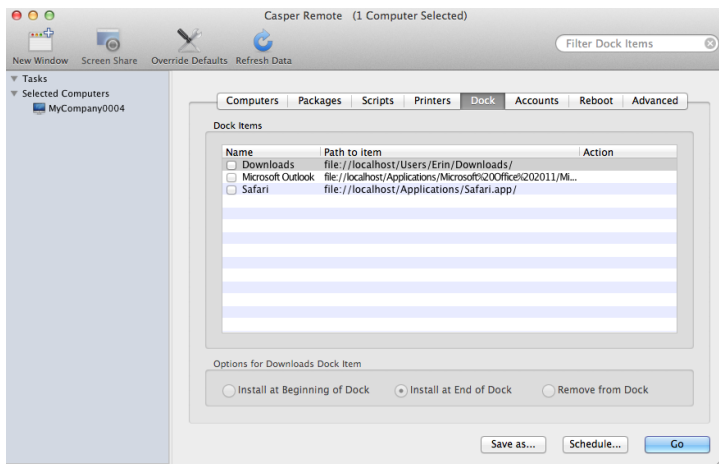
12. Click the **Add Dock Item(s)** button.

13. Click **Save**.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To add or remove a Dock item using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers you want to add or remove the Dock items from and select the checkbox next to each one.
3. Click the **Dock** tab and select the checkbox next to the Dock item.



4. Choose what you want to do with the item by selecting the **Install at Beginning of Dock**, **Install at End of Dock**, or **Remove from Dock** option.
5. Click **Go**.

Once you complete these steps, Casper Remote adds or removes the Dock item on client computers by performing the following steps:

1. Casper Remote logs in to each computer using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote adds or removes the Dock item.
4. Casper Remote logs out of each client and ends the SSH connection.

# Managing Local Accounts

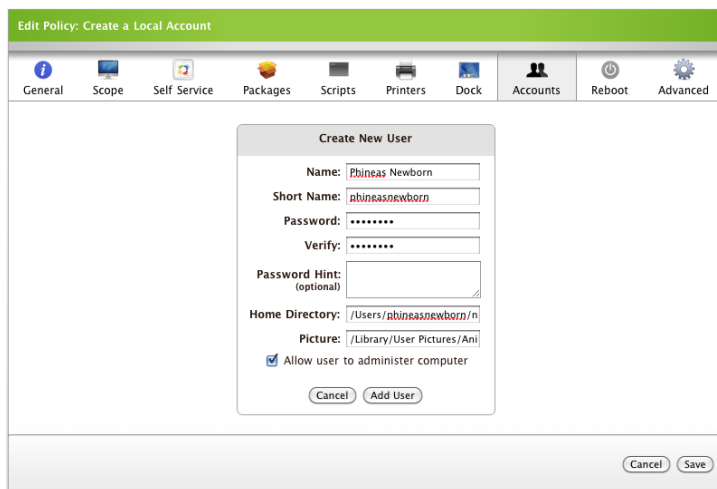
You can manage local user accounts remotely by performing the following management tasks:

- Create a new account.
- Delete an existing account.
- Reset the password for an existing account.
- Reset the password for the management account.

This section explains how to perform these tasks using a policy or Casper Remote.

## To create a local account using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Accounts** tab and click the **New Account** link.
11. Enter information for the new account and click the **Add User** button.



The screenshot shows the 'Create New User' dialog box within the 'Edit Policy: Create a Local Account' window. The dialog box has a title bar 'Create New User' and contains the following fields and options:

- Name:** Phineas Newborn
- Short Name:** phineasnewborn
- Password:** [masked with dots]
- Verify:** [masked with dots]
- Password Hint:** (optional) [empty field]
- Home Directory:** /Users/phineasnewborn/n
- Picture:** /Library/User Pictures/Ani
- Allow user to administer computer
- Buttons: Cancel, Add User

At the bottom of the main window, there are buttons for Cancel and Save.

12. Click **Save**.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To create a local account using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers you want to add the account to and select the checkbox next to each one.
3. Click the **Accounts** tab.
4. Click the **Create** button.
5. Enter information for the new account in the dialog that appears, and then click **OK**.

The screenshot shows a 'User' dialog box with the following fields and values:

- Name: Phineas Newborn
- Short Name: phineasnewborn
- Password: [masked]
- Verify: [empty]
- Password Hint (Optional): [empty]
- Home Directory: /Users/phineasnewborn/
- Allow user to administer this computer

6. Click **Go**.

The screenshot shows the Casper Remote interface with the 'Accounts' tab selected. The 'Create Accounts/Reset Passwords/Delete Accounts' section is active, displaying a table with columns for Username and Action. The table contains one entry: 'phineasnewborn' with the action 'Create'. Below the table are buttons for 'Create', 'Reset Password', and 'Delete'. The 'Change Management Account Password' section has 'Do Not Change' selected. The 'Open Firmware/EFI Password' section has 'Set Open Firmware/EFI Password' unchecked.

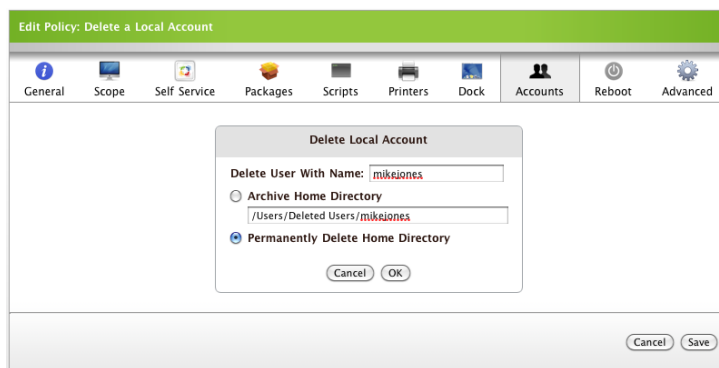
Once you complete these steps, Casper Remote creates the account on client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.

3. Casper Remote creates the account.
4. Casper Remote logs out of each client and ends the SSH connection.

**To delete a local account using a policy:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Accounts** tab.
11. Click the **Delete Existing Account** link.
12. Enter the short username for the account.
13. Choose whether to archive or delete the user's home directory, and then click **OK**.  
If you choose to archive the home directory, enter the location for where you want to store the archive.

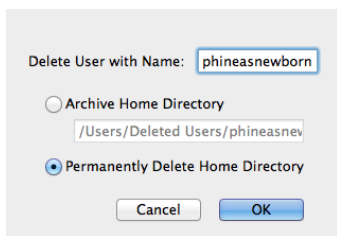


14. Click **Save**.

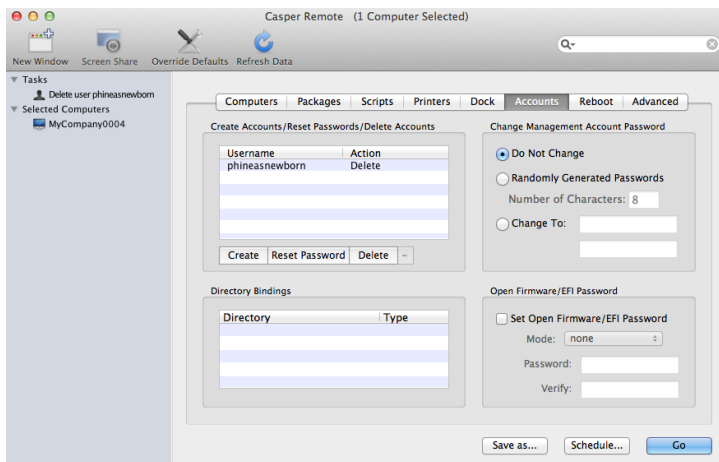
Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

## To delete a local account using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers you want to delete the account from and select the checkbox next to each one.
3. Click the **Accounts** tab.
4. Click the **Delete** button.
5. Enter the short username for the account that you want to delete.
6. Choose whether to archive or delete the user's home directory, and then click **OK**.  
If you choose to archive the home directory, enter the location for where you want to store the archive.



7. Click **Go**.



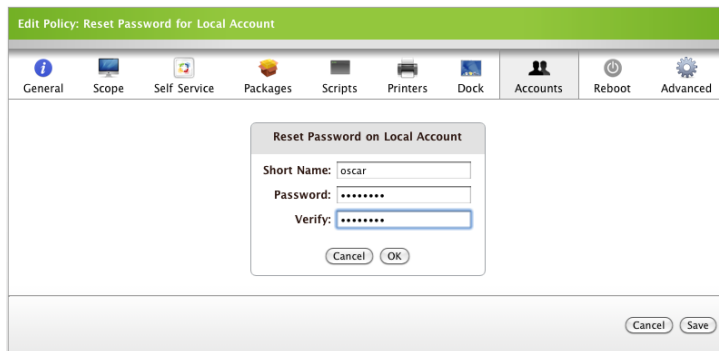
Once you complete these steps, Casper Remote deletes the account from client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote deletes the account.
4. Casper Remote logs out of each client and ends the SSH connection.



### To reset the password for a local account using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Accounts** tab.
11. Click the **Reset Password** link.
12. Enter the short username and password for the account.
13. Enter the password again to verify it, and then click **OK**.



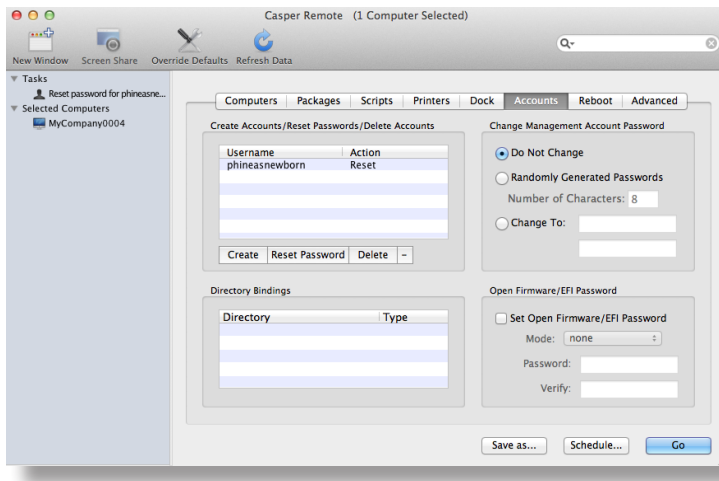
14. Click **Save**.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

### To reset the password for a local account using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers that have the account and select the checkbox next to each one.

3. Click the **Accounts** tab.
4. Click the **Reset Password** button.
5. Enter the short username and password for the account.
6. Type the password again to verify it, and then click **OK**.
7. Click **Go**.



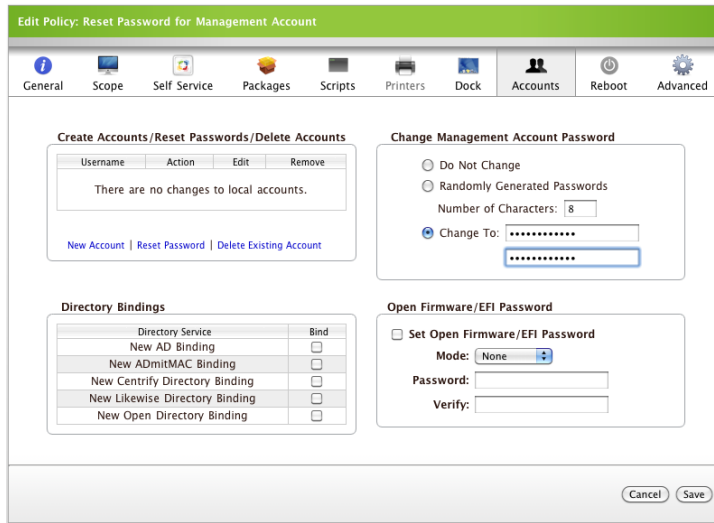
Once you complete these steps, Casper Remote resets the password on client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote resets the password.
4. Casper Remote logs out of each client and ends the SSH connection.

**To reset the password for the management account using a policy:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.

8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Accounts** tab.
11. To randomly generate a new password, select the **Randomly Generated Passwords** option and enter the number of characters you want the password to have.
12. To assign a password, select the **Change To** option and enter and verify the new password.
13. Click **Save**.

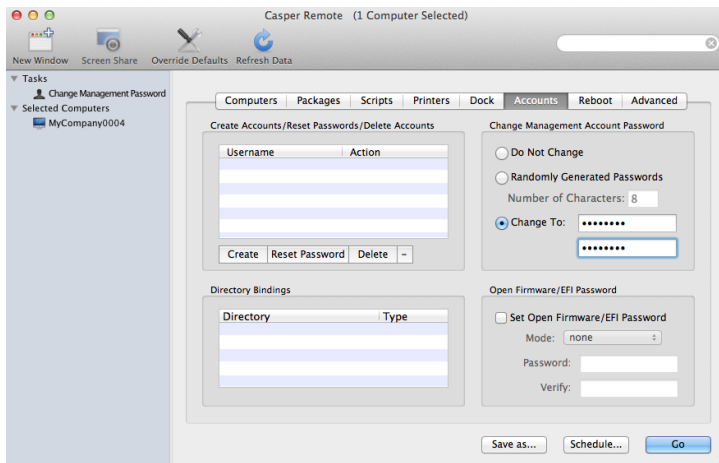


Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To reset the password for the management account using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers that have the account and select the checkbox next to each one.
3. Click the **Accounts** tab.
4. To randomly assign a new password for the management account, select **Randomly Generated Passwords** and enter the number of characters that you want the password to have.
5. To assign a specific password for the management account, select **Change To** and enter the new password.

## 6. Click Go.



Once you complete these steps, Casper Remote resets the password on client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote resets the password.
4. Casper Remote logs out of each client and ends the SSH connection.
5. Casper Remote stores the new password in the JSS.

# Binding to Directory Services

Before you can bind remote computers to a directory service, the JAMF Software Server (JSS) must contain a record of the directory bindings. For more information about creating directory bindings in the JSS, see the “Creating Directory Bindings” section.

This section explains how to bind to a directory service using a policy or Casper Remote.

## To bind to a directory service using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Accounts** tab and select the **Bind** checkbox across from each directory service you want to bind to.
11. Click **Save**.

The screenshot shows the 'Edit Policy: Bind to Directory Service' window. The window has a green header and a toolbar with icons for General, Scope, Self Service, Packages, Scripts, Printers, Dock, Accounts, Reboot, and Advanced. The main content area is divided into several sections:

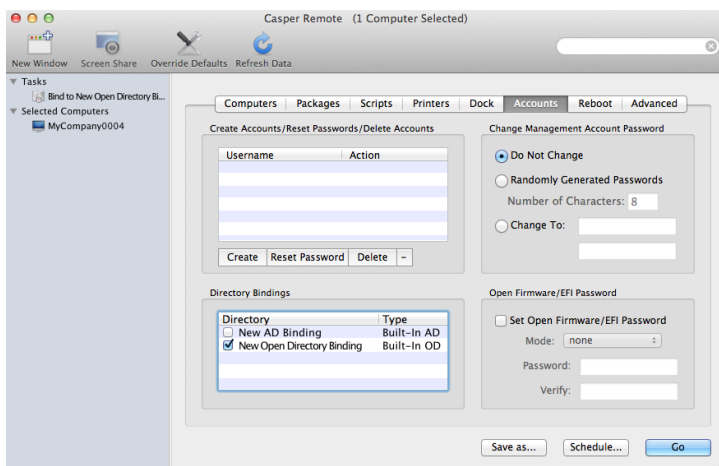
- Create Accounts/Reset Passwords/Delete Accounts:** A table with columns for Username, Action, Edit, and Remove. Below the table, it says "There are no changes to local accounts." and has links for "New Account", "Reset Password", and "Delete Existing Account".
- Change Management Account Password:** Radio buttons for "Do Not Change" (selected), "Randomly Generated Passwords", and "Change To:". The "Randomly Generated Passwords" option has a "Number of Characters" field set to 8.
- Directory Bindings:** A table with columns for Directory Service and Bind. The "New AD Binding" row has the "Bind" checkbox checked.
- Open Firmware/EFI Password:** A checkbox for "Set Open Firmware/EFI Password" (unchecked). Below it is a "Mode" dropdown menu set to "None", and "Password" and "Verify" input fields.

At the bottom right of the window are "Cancel" and "Save" buttons.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

### To bind to a directory service using Casper Remote:

1. Open Casper Remote.
2. In the **Computers** list, locate the computers you want to bind to the directory server and select the checkbox next to each one.
3. Click the **Accounts** tab.
4. In the list of directory bindings, select the checkbox next to each service that you want to bind to.
5. Click **Go**.



Once you complete these steps, Casper Remote binds client computers to the directory service by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote binds the computers to the directory service.
4. Casper Remote logs out of each client and ends the SSH connection.

# Deploying Disk Encryption Configurations

The JSS allows you to deploy disk encryption configurations to activate FileVault 2 on OS X v10.8 computers that have a "Recovery HD" partition present.

Deploying a disk encryption configuration using Casper Remote requires a JSS user account with the "Enable Disk Encryption Configuration Remotely" privilege enabled.

**Note:** A complete workflow for administering FileVault 2 on OS X v10.8 computers is provided in the "Administering FileVault 2 on OS X Mountain Lion with the Casper Suite" technical paper. You can download this technical paper from:

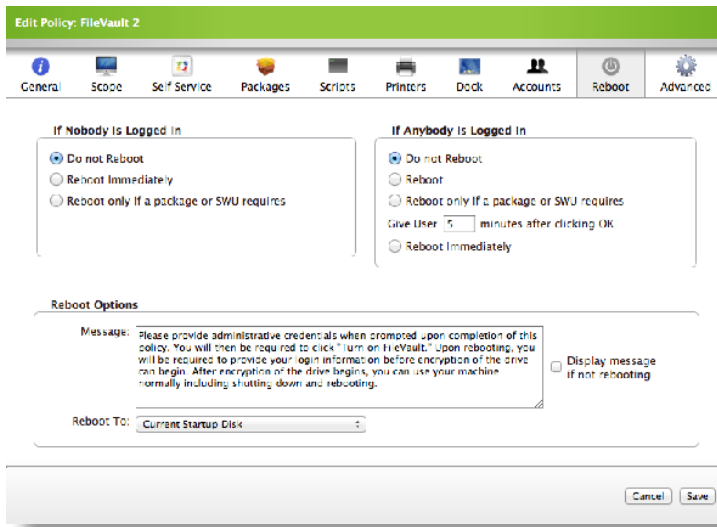
[http://www.jamfsoftware.com/libraries/pdf/white\\_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf](http://www.jamfsoftware.com/libraries/pdf/white_papers/Administering-FileVault-2-on-OS-X-Mountain-Lion-with-the-Casper-Suite.pdf)

This section explains how to deploy a disk encryption configuration using a policy or Casper Remote.

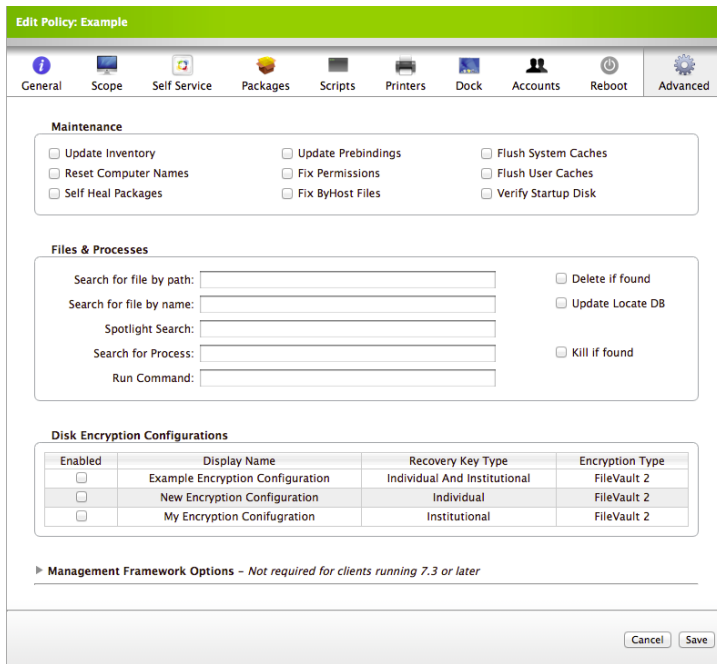
## To deploy a disk encryption configuration using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Select the **Create policy manually** option, and then click **Continue**.
6. Enter a display name for the policy.
7. Assign the policy to a category using the **Category** pop-up menu.
8. Choose a trigger from the **Triggered By** pop-up menu.
9. Choose "Once per computer" from the **Execution Frequency** pop-up menu.
10. Click the **Scope** tab and assign computers or user groups to the scope.

- (Optional) If you enabled the management account when you created the disk encryption configuration, click the **Reboot** tab and configure the desired reboot options. FileVault 2 disk encryption will not be activated until the next time computers in the scope are restarted.



- Click the **Advanced** tab.
- In the Disk Encryption Configurations section, select the checkbox in the **Enabled** column for the disk encryption configuration you want to deploy.



- Click **Save**.

Clients execute the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.



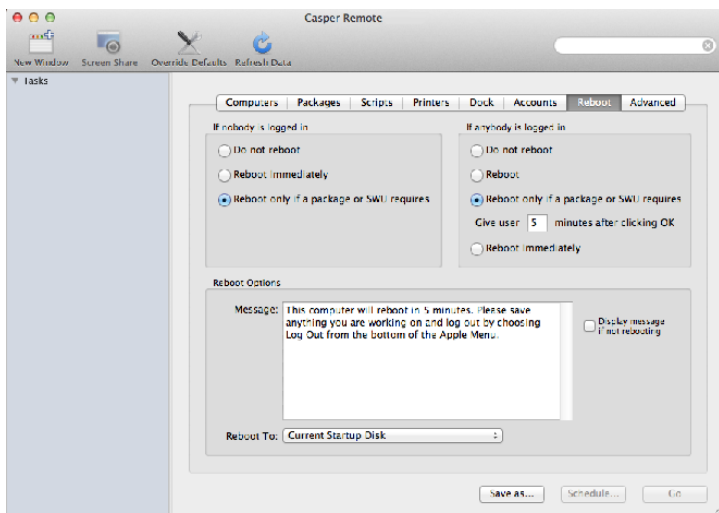
If you deployed a disk encryption configuration that is configured to use the management account as the enabled FileVault 2 user, the disk encryption is activated the next time computers are restarted.

If you deployed a disk encryption configuration that is configured to use the current or next user as the enabled FileVault 2 user, the disk encryption is activated the next time users log out or computers are restarted by users.

### To deploy a disk encryption configuration using Casper Remote:

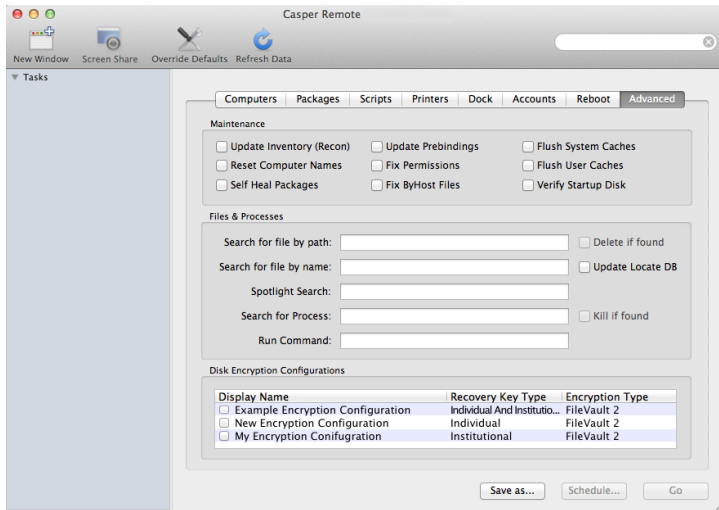
1. Open Casper Remote.
2. In the **Computers** list, locate the computers you want to deploy the disk encryption configuration to and select the checkbox next to each one.
3. (Optional) If you enabled the management account when you created the disk encryption configuration, click the **Reboot** tab and configure the desired reboot options.

FileVault 2 disk encryption will not be activated until the next time computers in the scope are restarted.



4. Click the **Advanced** tab.

5. In the list of Disk Encryption Configurations, select the checkbox next to the disk encryption configuration you want to deploy.



6. Click **Go**.

If you deployed a disk encryption configuration that is configured to use the management account as the enabled FileVault 2 user, the disk encryption is activated the next time computers are restarted.

If you deployed a disk file encryption configuration that is configured to use the current or next user as the enabled FileVault 2 user, the disk encryption is activated next time users log out or computers are restarted by users.

Once these steps are complete, Casper Remote deploys the disk encryption configuration by:

1. Logging in to each computer using an SSH connection.
2. Verifying the computer's identity using the MAC address.
3. Applying the disk encryption configuration to the computer's drive.
4. Logging out of the SSH connection.

# Managing Open Firmware/EFI Passwords

You can manage Open Firmware or EFI passwords remotely to ensure the security of client computers.

This section explains how to set and remove an Open Firmware/EFI password using a policy or Casper Remote.

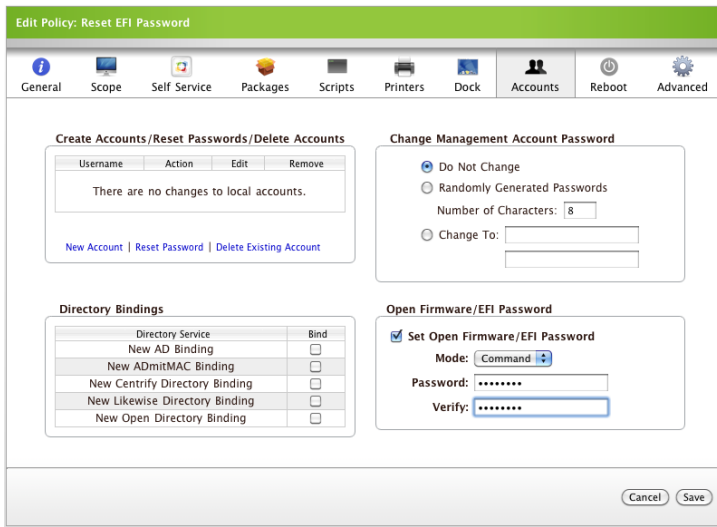
**Important:** If you are setting or removing an Open Firmware/EFI password on models "Late 2010" or later, the "setregproptool" must be present on the volume(s) used to set firmware. For instructions on obtaining and placing the "setregproptool" binary, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=58>

## To set or remove an Open Firmware/EFI password using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create or edit the policy.
  - To create a policy, click the **Create Policy** button in the toolbar, select the **Create policy manually** option, and then click **Continue**.
  - To edit an existing policy, click the **Edit Policy** link across from it.
5. Enter a display name for the policy.
6. Assign the policy to a category using the **Category** pop-up menu.
7. Choose a trigger from the **Triggered By** pop-up menu.
8. Choose how often you want clients to run the policy using the **Execution Frequency** pop-up menu.
9. Click the **Scope** tab and assign computers or user groups to the scope.
10. Click the **Accounts** tab and select the **Set Open Firmware/EFI Password** checkbox.

- If you want to set the password, choose "Command" from the **Mode** pop-up menu, and then enter and verify a password.

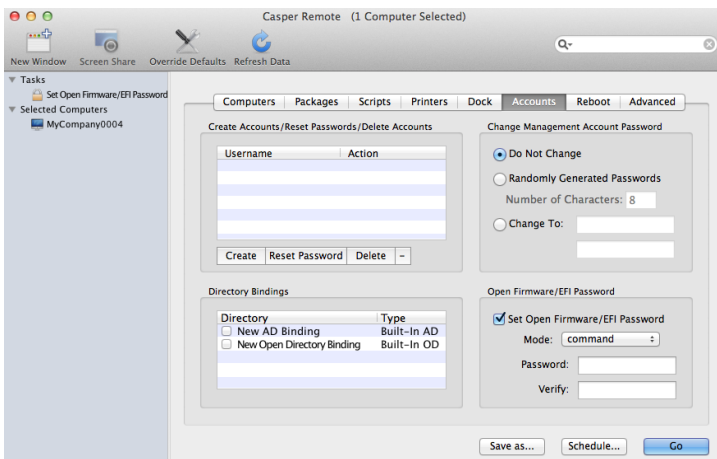


- If you want to remove the password, choose "None" from the **Mode** pop-up menu.
- Click **Save**.

Clients run the policy the next time they check in with the JSS and meet all of the criteria on the General and Scope panes.

#### To set or remove an Open Firmware/EFI password using Casper Remote:

- Open Casper Remote.
- In the **Computers** list, locate the computers on which you want to set an Open Firmware/EFI password and select the checkbox next to each one.
- Click the **Accounts** tab and select the **Set Open Firmware/EFI Password** checkbox.
- If you want to set the password, choose "Command" from the **Mode** pop-up menu, and then enter and verify a password.



5. If you want to remove the password, choose "None" from the **Mode** pop-up menu.
6. Click **Go**.

Once you complete these steps, Casper Remote sets or removes the password on client computers by performing the following steps:

1. Casper Remote logs in to each client using an SSH connection.
2. Casper Remote verifies the identity of the clients using their MAC addresses.
3. Casper Remote sets or removes the password.
4. Casper Remote logs out of each client and ends the SSH connection.

# License Management

## Creating Licensed Software Records

Licensed software records allow you to define and store information about the software licenses owned by your organization. You can use this information to create more accurate inventory reports, monitor compliance, and quickly access license and purchasing information.

There are several ways to create a licensed software record:

- Create the record manually.
- Use a licensed software template that is built into the JSS.
- Upload a licensed software template.

You can download licensed software templates from JAMF Nation at:

<https://jamfnation.jamfsoftware.com/licensedSoftwareTemplates.html>

- Duplicate an existing licensed software record.

### To create a licensed software record manually:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Licensed Software Management** link.
4. Click the **Create Licensed Software** button.
5. Enter a display name for the licensed software record.
6. (Optional) Enter the name of the publisher.
7. Choose the platform that the license was obtained for.
8. To send an email to administrators when a license violation occurs, select the **Send Email Notification on Violation** checkbox.  
An SMTP server must be set up in the JSS to send email notifications. For information on how to set up an SMTP server, see "Enabling Email Notifications".
9. To display only the name of the licensed software record in inventory reports and suppress the name of any individual software titles, select the **Remove Software Titles from Inventory Reports** checkbox.

10. (Optional) Enter additional information in the **Notes** field.

The screenshot shows a dialog box titled "Edit Licensed Software:". It has three tabs: "Info", "Licenses", and "Software Definitions". The "Info" tab is selected. The form contains the following fields and options:

- Display Name:** Adobe CS4 Web Standard
- Publisher:** Adobe Systems Incorporated
- Platform:** Macintosh (dropdown menu)
- Send Email Notification on Violation
- Remove Software Titles from Inventory Reports
- Notes:** (empty text area)

At the bottom right, there are "Cancel" and "Save" buttons.

11. To store license and purchasing information in the record, see "To store license and purchasing information in a licensed software record".
12. To specify the software titles that count toward the license, see "To specify software definitions for a licensed software record".
13. Click **Save**.

**To create a licensed software record from a template that is built into the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Licensed Software Management** link.
4. Click the **Licensed Software from Template** button.
5. Find the software title that you want to create a record for and click the **Create** link across from it.
6. Choose the platform that the license was obtained for.
7. To send an email to administrators when a license violation occurs, select the **Send Email Notification on Violation** checkbox.  
An SMTP server must be set up in the JSS to send email notifications. For information on how to set up an SMTP server, see "Enabling Email Notifications".
8. To display only the name of the licensed software record in inventory reports and suppress the name of any individual software titles, select the **Remove Software Titles from Inventory Reports** checkbox.

- (Optional) Enter additional information in the **Notes** field.

The screenshot shows a dialog box titled "Edit Licensed Software:". It has a green header bar. Below the header are three tabs: "Info", "Licenses", and "Software Definitions". The "Info" tab is selected. The form contains the following fields and options:

- Display Name:** Adobe CS4 Web Standard
- Publisher:** Adobe Systems Incorporated
- Platform:** Macintosh (dropdown menu)
- Send Email Notification on Violation
- Remove Software Titles from Inventory Reports
- Notes:** (empty text area)

At the bottom right, there are "Cancel" and "Save" buttons.

- To store license and purchasing information, see "To store license and purchasing information in a licensed software record".

The software titles that count toward the license are included in the template. To view them, click the **Software Definitions** tab.

- Click **Save**.

#### To upload a licensed software template:

- Log in to the JSS with a web browser.
- Click the **Settings** tab.
- Click the **Licensed Software Management** link.
- Click the **Upload Licensed Software** button.
- Click **Choose File** and select the licensed software template that you want to upload. Then, click **Upload Selected Template**.

The licensed software template must be an XML file.

- Choose the platform that the license was obtained for.
- To send an email to administrators when a license violation occurs, select the **Send Email Notification on Violation** checkbox.

An SMTP server must be set up in the JSS to send email notifications. For information on how to set up an SMTP server, see "Enabling Email Notifications".

- To display only the name of the licensed software record in inventory reports and suppress the name of any individual software titles, select the **Remove Software Titles from Inventory Reports** checkbox.



- (Optional) Enter additional information in the **Notes** field.

The screenshot shows a dialog box titled "Edit Licensed Software:". It has a green header bar. Below the header are three tabs: "Info" (selected), "Licenses", and "Software Definitions". The "Info" tab contains the following fields and options:

- Display Name:** Adobe CS4 Web Standard
- Publisher:** Adobe Systems Incorporated
- Platform:** Macintosh (dropdown menu)
- Send Email Notification on Violation
- Remove Software Titles from Inventory Reports
- Notes:** (empty text area)

At the bottom right of the dialog are "Cancel" and "Save" buttons.

- To store license and purchasing information, see "To store license and purchasing information in a licensed software record".

The software titles that count toward the license are included in the template. To view them, click the **Software Definitions** tab.

- Click **Save**.

#### To duplicate an existing licensed software record:

- Log in to the JSS with a web browser.
- Click the **Settings** tab.
- Click the **Licensed Software Management** link.
- Click the **Duplicate Licensed Software** button.
- Find the licensed software record that you want to duplicate and click the **Duplicate** link across from it.
- Enter a new display name for the licensed software record.
- Add or modify license and purchasing information, and software definitions as needed.
- Click **Save**.

#### To store license and purchasing information in a licensed software record:

- Log in to the JSS with a web browser.
- Click the **Settings** tab.
- Click the **Licensed Software Management** link.

4. Create a licensed software record or edit an existing one.
  - To create a licensed software record, click the **Create New License** button or use one of the other methods explained in this guide.
  - To edit a licensed software record, click the **Edit** link across from it.
5. Click the **Licenses** tab.
6. Click the **Add License** link.
7. Enter the serial number(s) for the license.
8. (Optional) Enter the name of the organization that owns the license.
9. (Optional) Enter the name of the individual that the license is registered to.
10. (Optional) Select the type of license and enter the number of licenses owned.
11. (Optional) Enter additional information in the **Notes** field.
12. (Optional) Specify purchasing information for the license.
13. Click **Store License**.

**Edit Licensed Software: Example**

Info Licenses Software Definitions

**License Info**

Serial Number 1:

Serial Number 2:

Organization Name:

Registered To:

License For:  0 Licenses  
 Concurrent Licenses  
 Site License

Notes:

**Purchasing Info**

Perpetual License  Annual License

PO Number:  PO Date:  /  /

Vendor:  License Expires:  /  /

Purchase Price:  Life Expectancy:

Purchasing Account:  Purchasing Contact:

No Attachments.  
[Attach File...](#)

14. Repeat steps 6 through 13 for each additional license.
15. Click **Save**.

To specify software definitions for a licensed software record:

1. Log in to the JSS with a web browser
2. Click the **Settings** tab.
3. Click the **Licensed Software Management** link.
4. Create a licensed software record or edit an existing one.
  - To create a licensed software record, click the **Create New License** button or use one of the other methods explained in this guide.
  - To edit a licensed software record, click the **Edit** link across from it.
5. Click the **Software Definitions** tab.
6. To add an application, font, or plug-in, click the **Add** link for the item that you want to add.

The screenshot shows the 'Edit Licensed Software: Example' interface. At the top, there is a green header bar with the title 'Edit Licensed Software: Example'. Below the header, there are three tabs: 'Info', 'Licenses', and 'Software Definitions'. The 'Software Definitions' tab is selected. The main content area contains three tables, each with a header row and a body row. The first table is for 'Applications', with columns 'Application Name' and 'Version'. The second table is for 'Fonts', with columns 'Font Name' and 'Version'. The third table is for 'Plug-ins', with columns 'Plug-in Name' and 'Version'. Each table has a message 'There are no [Applications/Fonts/Plug-ins] entered' in the body row. Below each table is a blue link: 'Add Application...', 'Add Font...', and 'Add Plug-in...' respectively. At the bottom right of the interface, there are two buttons: 'Cancel' and 'Save'.

7. Specify the title and version number and click the **Store Definition** button.

The screenshot shows the 'Edit Licensed Software: Example' interface. At the top, there is a green header bar with the title 'Edit Licensed Software: Example'. Below the header, there are three tabs: 'Info', 'Licenses', and 'Software Definitions'. The 'Software Definitions' tab is selected. The main content area contains a form titled 'Application Info'. The form has two rows of input fields. The first row is 'Title: is' followed by a text input field. The second row is 'Version: like' followed by a dropdown menu and a text input field. Below the form, there are two buttons: 'Cancel' and 'Store Definition'. At the bottom right of the interface, there are two buttons: 'Cancel' and 'Save'.

8. Repeat steps 6 and 7 for each additional item.
9. Click **Save**.

**To edit a licensed software record:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Licensed Software Management** link.
4. Find the record that you want to edit and click the **Edit** link across from it.
5. Add or modify information as needed.
6. Click **Save**.

**To delete a licensed software record:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Licensed Software Management** link.
4. Find the record that you want to delete and click the **Delete** link across from it.
5. Click the **Delete** button to confirm.

# Reporting on Licensed Software

Using reports to track licensed software helps you stay organized by storing all of your purchasing information in one, accessible location. Licensed software reports allow you to monitor the number of licenses your organization has and how many are in use, making compliance with software vendors easy to track and maintain.

Licensed software reporting and inventory reporting work in the same way. First, you perform a simple or advanced search of your records. Then, you choose a reporting template in which to view your results.

This section explains how to:

- Perform simple and advanced licensing searches
- View licensing search results

## Performing Simple Licensing Searches

A simple licensing search functions like a search engine, allowing you to locate a general range of results quickly and easily.

Simple searches can be performed based on the following attributes of a licensed software record:

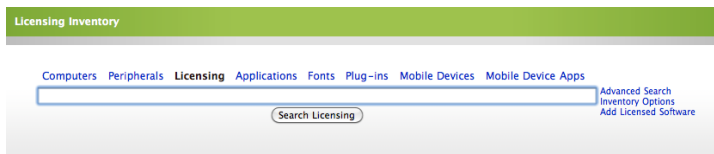
- Display Name
- Publisher
- Notes
- Registration Information for Associated Licenses (organization or individual that a license is registered to)
- Serial Numbers for Associated Licenses
- Purchasing Accounts for Associated Licenses
- Purchasing Contacts for Associated Licenses
- PO Numbers for Associated Licenses
- Notes for Associated Licenses

**Note:** Performing an empty search (with no criteria in the search field) returns all of the licensed software records in your database.

**To perform a simple licensing search:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Licensing** link.
4. Enter one or more terms into the search field.

5. Click the **Search Licensing** button, or press the Enter key.



By default, search results are displayed as a Standard Webpage report and include the following information:

- Licensed software records that match your search criteria
- Total number of licenses your organization owns for the software
- Total number of licenses in use for the software

Any licensed software records in violation of the licensing limit are displayed in red text.

To view a list of computers on which the software is installed, click the **View Computers** link across from the record.

A screenshot of the search results page. At the top, there is a green navigation bar with tabs for 'Inventory', 'Management', 'Logs', and 'Settings'. A search bar contains 'Search JSS Topics'. Below the navigation bar, there is a 'Logout admin' link. The main content area shows '83 Results (1.78 seconds)' and a section titled 'Licensed Software'. Below this title is a table with three columns: 'Display Name', 'Total Licenses', and 'Licenses Used'. Each row also has a 'View Computers...' link. The table contains three rows of data.

Display Name	Total Licenses	Licenses Used	
OmniOutliner Professional	12	8	<a href="#">View Computers...</a>
VMWare Fusion	18	18	<a href="#">View Computers...</a>
OmniGraffle Professional 5	7	6	<a href="#">View Computers...</a>

## Performing Advanced Licensing Searches

When used to search for licensed software and create reports, advanced searches offer a variety of powerful options. The advanced licensing search interface consists of three panes: General, Criteria, and Display Fields.

A detailed description of the information on each pane follows:

## General Pane

The screenshot shows the 'General' tab of the 'Advanced Licensing Search' window. It features three tabs: 'General' (selected), 'Criteria', and 'Display Fields'. Below the tabs, there is a 'Report Name' text input field, a 'Save this Report' checkbox, and a 'View As' dropdown menu currently set to 'Standard Web Page'. At the bottom right, there are 'Cancel' and 'Search' buttons.

This pane allows you to choose a reporting format and save the report so you can access it in the future. If you choose to save a report, you can perform the same search at a later date.

Saved computer searches can be accessed on the Computer Inventory pane. You can edit or delete a saved computer search by clicking the disclosure triangle next to the search and then clicking the **Edit** or **Delete** link.

## Criteria Pane

The screenshot shows the 'Criteria' tab of the 'Advanced Licensing Search' window. It features three tabs: 'General', 'Criteria' (selected), and 'Display Fields'. Below the tabs is a table with columns for 'Field', 'Search Type', 'Criteria', and a '+' sign. The table lists three categories: 'Licensed Software Info', 'Software Licenses Info', and 'License Purchasing Info', each with a '+' sign in the rightmost column. At the bottom right, there are 'Cancel' and 'Search' buttons.

Field	Search Type	Criteria	-	+
		Licensed Software Info		+
		Software Licenses Info		+
		License Purchasing Info		+

This pane allows you to specify the attributes on which to base your search. These options are broken down into three categories:

- Licensed Software Info
- Software License Info
- Software License Purchasing Info

## Display Fields Pane

Advanced Licensing Search

General Criteria Display Fields

Display Name  Publisher  Platform  Total Licenses  
 Licenses Used  Compliant  Matching Computers

License Serial Number  Organization Name  License Registered To

Perpetual License/Annual License  PO Number  PO Date  Vendor  
 Warranty Expires  Lease Expires  AppleCare ID  Purchase Price  
 Life Expectancy  Purchasing Account  Purchasing Contact

Cancel Search

This pane allows you to specify the attributes displayed in your search results.

You can change the default selections by changing your Inventory Display preferences. For more information on changing Inventory Display preferences, see the “Inventory Display Preferences” section.

### To perform an advanced licensing search:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Licensing** link.
4. Click the **Advanced Search** link at the right of the search field.
5. If you want to save your search, enter a name for the report and select the **Save this Report** checkbox.

Advanced Licensing Search

General Criteria Display Fields

Report Name:

Save this Report:

View As:

Cancel Search

6. Choose the format in which you want to view the report from the **View As** pop-up menu.
7. Click the **Criteria** tab, and narrow your search by clicking the **Add (+)** button next to each search type that corresponds to the information that you want to use.  
A list of searchable items is displayed.
8. Click the items that you want to use in your search and further specify the search criteria using the fields provided.



9. Click the **Display Fields** tab select the checkbox next to each attribute that you want displayed in your search results.
10. Click **Search**.

## Viewing Licensing Search Results

By default, licensing search results are displayed in Standard Webpage format. You can view the search results for advanced licensing searches in any of the following alternate formats by choosing from the **View As** pop-up menu on the General pane of the advanced search interface:

- Licensing Compliance Report (PDF)
- Printable Licensed Software Record (PDF)
- CSV
- Tab
- XML

**Note:** The attributes displayed in advanced licensing search results are determined by the settings on the Display Fields pane of the advanced search interface. For more information, see “Performing Advanced Licensing Searches”.

### Standard Webpage

The Standard Webpage report displays the licensed software, the number of licenses your organization owns for the software, and the number of licenses currently in use. As you scroll down the page, a list of computers using the licenses is displayed.


Any licensed software records in violation of the licensing limit are displayed in red.


Display Name	Total Licenses	Licenses Used	
Adobe Acrobat Pro 9	1	2	<a href="#">View Computers...</a>
Adobe Bridge CS4	1	0	
Adobe Device Central CS4	1	0	
Adobe Illustrator	1	1	<a href="#">View Computers...</a>

### Licensing Compliance Report (PDF)

The Licensing Compliance report provides a high-level overview of your licensed software records and any titles that are in violation of the licensing limit.


One record is displayed per line, along with the number of licenses owned and the total number of licenses in use. Records that have more licenses distributed than your organization owns are marked with a yellow alert to the left of the record.

License Compliance Report Generated for My Company 

	Licensed Software Name	Licenses Owned	Licenses Used
	Creative Suite 2 Professional	200	204
	Creative Suite 2 Standard	5	4
	Microsoft Office 2004	160	157

## Printable Licensed Software Record (PDF)

The Printable Licensed Software record report allows you to print licensed software information in a format suitable for hardcopy purchasing records. The records print one per page and include general information about the title, along with each corresponding software license on file.

Licensed Software Records for My Company 

**Microsoft Office 2004**

**Licensed Software Overview**

---

**Publisher** Microsoft Corp  
**Platform** mac  
**Notes** Purchased directly from Microsoft.

---

**License #1**

**Serial Number** XB6JW-2JJCv-DXC8B-88888-7777  
**Organization** My Company  
**Registered To** My Name  
**License Type** 5 Licenses      **License Term** Perpetual License  
**Vendor** Microsoft

---

**License #2**

**Serial Number** XB6JW-2JJCv-DXC8B-66666-55555  
**Organization** My Company  
**Registered To** My Name  
**License Type** 155 Licenses      **License Term** Perpetual License  
**PO Date** January 07, 2007      **Vendor** Apple Store  
**Purchase Price** 399      **Life Expectancy** 1 Year

## CSV

This format exports your search results into a CSV file that you can open in Microsoft Excel and other spreadsheet applications.

## Tab

This format exports your search results into a tab-delimited text file that you can open in Microsoft Excel and other spreadsheet applications.

## XML

This format exports your search results into an XML file. XML files are commonly used to move data between applications.

# Sending Notifications on Licensed Software Violations

Maintaining up-to-date licensed software records allows you to monitor the number of software licenses in use in your environment.

Each time a computer submits an inventory report to the JAMF Software Server (JSS), the licensed software on the computer is analyzed. If the number of computers that report a licensed software title is greater than the actual number of licenses purchased by your organization, the JSS sends an email notification.

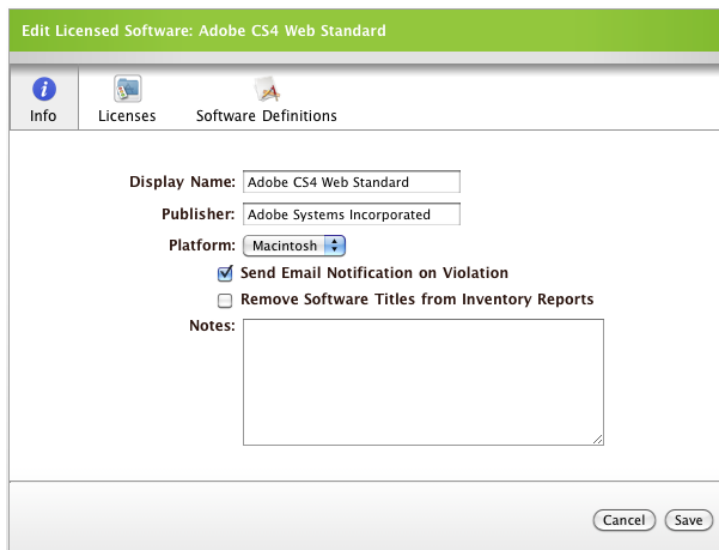
Sending email notifications on licensed software violations requires:

- An SMTP server set up in the JSS (For instructions on how to set up an SMTP server, see “Enabling Email Notifications”).
- The Software License Violation option enabled for each account that you want to receive notifications (For more information, see “Managing JSS User Accounts”).

**Note:** A user must have an account in the JSS to receive email notifications.

**To send an email notification on a licensed software violation:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Licensed Software Management** link.
  - To create a new record, click the **Create Licensed Software** button in the toolbar.
  - To edit an existing record, click the **Edit** link across from it.
4. Select the **Send Email Notification on Violation** checkbox.
5. Click **Save**.



The screenshot shows a web browser window titled "Edit Licensed Software: Adobe CS4 Web Standard". The interface includes a navigation bar with "Info", "Licenses", and "Software Definitions" tabs. The main content area contains the following fields and options:

- Display Name:** Adobe CS4 Web Standard
- Publisher:** Adobe Systems Incorporated
- Platform:** Macintosh (dropdown menu)
- Send Email Notification on Violation**
- Remove Software Titles from Inventory Reports**
- Notes:** (empty text area)

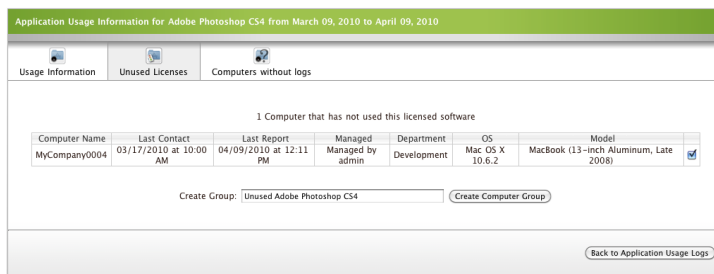
At the bottom right, there are "Cancel" and "Save" buttons.

# Reclaiming Unused Licensed Software

If you have application usage logging enabled (see the “Application Usage” section), you can monitor how often licensed software is being used and remove it from computers if necessary.

## To locate unused licensed software:

1. Log in to the JSS with a web browser.
2. Click the **Logs** tab.
3. Click the **Application Usage Logs** link.
4. On the Licensed Software pane, choose a starting and ending date for your search.
5. Click the **View Usage** link across from the record for which you want to view logs.
6. Click the **Unused Licenses** tab and select the checkbox across from each computer from which you want to remove the software.
7. Create a computer group by entering a name for the group and clicking the **Create Computer Group** button.



After completing these steps, create a policy to uninstall the software and assign the computer group you created in step 7 to the scope.

---

# Usage Management

## Application Usage

Application Usage logs allow you to monitor how frequently applications are used on client computers. You can use this information to reclaim unused software licenses and track usage behaviors across your network.

Before utilizing this feature, you must enable application usage monitoring in the JAMF Software Server (JSS). This prompts clients to submit application usage data each time they generate an inventory report back to the JSS.

To generate Application Usage logs more frequently, create a policy to update inventory more frequently. For example, to generate daily usage logs, create a policy to update inventory once a day.

This section explains how to:

- Enable application usage monitoring
- View Application Usage logs for a single computer
- View Application Usage logs for multiple computers
- View Application Usage logs for licensed software

### To enable application usage monitoring:

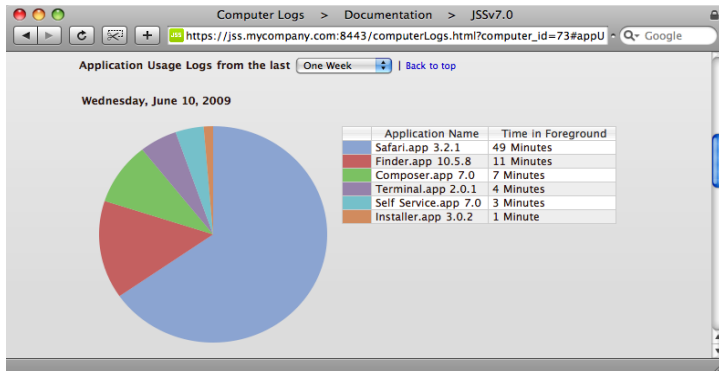
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Application Usage** tab.
5. Select the **Enable application usage monitoring** checkbox.
6. Click **Save**.

### To view Application Usage logs for a single computer:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.

3. Perform a simple search for the computer.
4. Click the **Logs** link across from the computer record.
5. Use the **Application Usage Logs from the last** pop-up menu to see logs from a different timeframe.
6. Click the **Application Usage Logs** link at the top of the page.

Each Application Usage log looks like this:

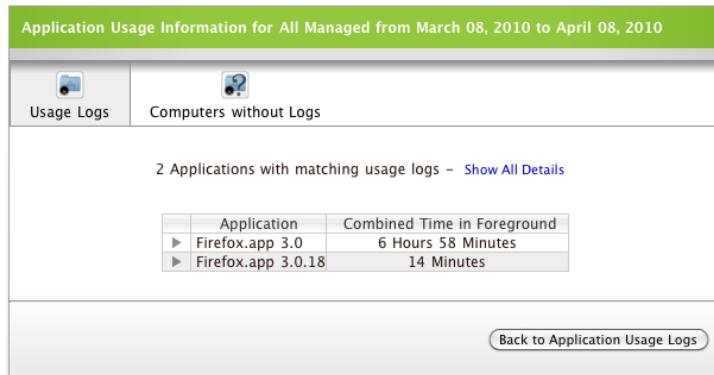


**To view Application Usage logs for multiple computers:**

1. Log in to the JSS with a web browser.
2. Click the **Logs** tab.
3. Click the **Application Usage Logs** link.
4. Click the **Computer Groups**, **Departments**, or **Buildings** tab depending on the logs you want to view.
5. Use the **Reports Starting** and **Reports Ending** pop-up menus to specify the dates you want to view logs for.
6. Enter the application name and version number in the **Application Name** and **Application Version Number** fields to further narrow the reporting criteria.

7. Click the **View Usage** link across from the computer group, department, or building for which you want to view logs.

8. When the list of logs is displayed, you can view additional information about each log:
  - Click the disclosure triangle next to an application record to see a list of computers on which the application was used.
  - Click the disclosure triangle next to the computer record to see a list of users who opened the application.



#### To view Application Usage logs for licensed software:

1. Log in to the JSS with a web browser.
2. Click the **Logs** tab.
3. Click the **Application Usage Logs** link.
4. On the Licensed Software pane, use the **Reports Starting** and **Reports Ending** pop-up menus to specify the dates you want to view logs for.
5. Click the **View Usage** link across from the licensed software record for which you want to view logs.

# Computer Usage

Computer Usage logs allow you to see how frequently each computer is used. These logs can be submitted back to the JAMF Software Server (JSS) at the following triggers:

- Startup
- Login
- Logout

This section explains how to:

- Enable computer usage monitoring
- View Computer Usage logs for all computers
- View Computer Usage logs for a single computer

## To enable computer usage monitoring:

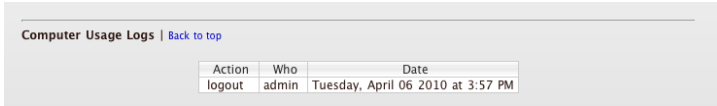
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. To generate logs at startup:
  - a. Click the **Startup Item** tab.
  - b. Select the **Create startup item** checkbox.
  - c. Select the **Log Startup Action** checkbox.
5. To generate logs at login and logout:
  - a. Click the **Create Login/Logout Hooks** tab.
  - b. Select the **Create login and logout hooks** checkbox.
  - c. Select the **Log Username at login and logout** checkbox.
6. Click **Save**.

## To view Computer Usage logs for a single computer:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple search for the computer.
4. Click the **Logs** link across from the computer record.



5. Click the **Computer Usage Logs** link at the top of the page to see a list of logs.

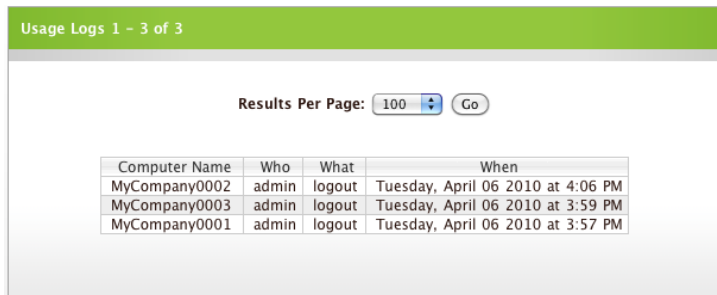


Computer Usage Logs | [Back to top](#)

Action	Who	Date
logout	admin	Tuesday, April 06 2010 at 3:57 PM

**To view Computer Usage logs for all computers:**

1. Log in to the JSS with a web browser.
2. Click the **Logs** tab.
3. Click the **Usage Logs** link.



Usage Logs 1 - 3 of 3

Results Per Page: 100

Computer Name	Who	What	When
MyCompany0002	admin	logout	Tuesday, April 06 2010 at 4:06 PM
MyCompany0003	admin	logout	Tuesday, April 06 2010 at 3:59 PM
MyCompany0001	admin	logout	Tuesday, April 06 2010 at 3:57 PM

# Restricted Software

If there are applications you don't want installed or used on client computers, you can prevent this by creating restricted software records. Restricting software is useful in preventing users from accessing commonly installed administrative utilities or applications that are considered a liability to your company.

There is a Global Exemption list that allows you to specify any computers or users who are exempt from the restrictions. You can also specify exemptions based on individual applications, giving you full control over who has access to the applications on your network.

After you create a restricted software record, the restriction is enforced on client computers the next time they check in to the JAMF Software Server (JSS).

This section explains how to create a restricted software record and edit the Global Exemption list.

## To create a restricted software record:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Restricted Software** link.
4. Click the **Add Restricted Software** button in the toolbar.
5. Enter a display name for the restricted software.
6. Enter the name of the process that you want to restrict.

The process name is case-sensitive and supports filename wildcards.

The screenshot shows a web-based dialog box titled "Edit Restricted Software: Restricted Process". It features a green header bar and three tabs: "General" (active), "Exempt Computers", and "Exempt Users". The "General" tab contains the following fields and controls:

- Display Name:** A text input field containing "Restricted Process".
- Process To Look For:** A text input field containing "LimeWire".
- Send Email Notification:** An unchecked checkbox.
- Kill Process:** An unchecked checkbox.
- Delete:** An unchecked checkbox.
- Display Message to User:** A text area for entering a message.

At the bottom right of the dialog are "Cancel" and "Save" buttons.

7. To receive an email notification each time a violation occurs, select the **Send Email Notification** checkbox.
8. To terminate the software when a violation occurs, select the **Kill Process** checkbox.
9. To delete the software when a violation occurs, select the **Delete** checkbox.

- To display a message to the user who violated the restriction, enter the message that you want to display. If the **Display Message to User** field is left blank, a message is not displayed.

The screenshot shows the 'Edit Restricted Software: Restricted Process' dialog box with the 'General' tab selected. The 'Display Name' field contains 'Restrict LimeWire' and the 'Process To Look For' field contains 'LimeWire'. The 'Send Email Notification', 'Kill Process', and 'Delete' checkboxes are all checked. The 'Display Message to User' field is empty. 'Cancel' and 'Save' buttons are at the bottom right.

- Click the **Exempt Computers** tab.
- Click the **Add <Group>** button to specify exempt computers, computer groups, buildings, or departments.
- Click the **Add** checkbox next to each computer or group you want to make exempt from the restriction.

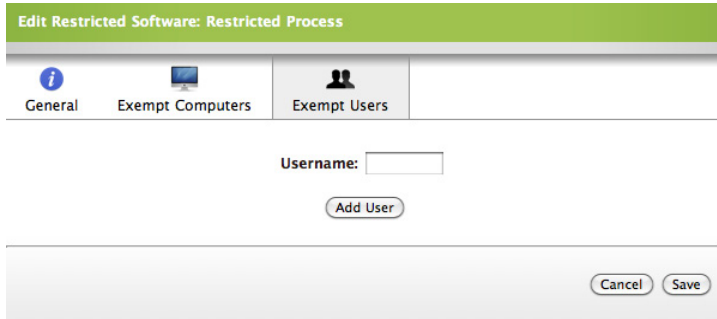
The screenshot shows the 'Edit Restricted Software: Restricted Process' dialog box with the 'Exempt Computers' tab selected. It displays a table of buildings with an 'Add' checkbox for each. Below the table is an 'Add Building(s)' button. 'Cancel' and 'Save' buttons are at the bottom right.

Building	Add
JAMF Eau Claire	<input type="checkbox"/>
JAMF Houston	<input type="checkbox"/>
JAMF Indiana	<input type="checkbox"/>
JAMF Lawrence	<input type="checkbox"/>
JAMF Minneapolis	<input type="checkbox"/>
JAMF Minneapolis & St Paul	<input type="checkbox"/>
JAMF New York	<input type="checkbox"/>
JAMF Portland	<input type="checkbox"/>
JAMF San Francisco	<input type="checkbox"/>
JAMF Washington DC	<input type="checkbox"/>

- Click the **Exempt Users** tab and click the **Add User** button to specify all exempt users.

15. In the **Username** field, enter the username for the account used to open the application. For example, to ensure the administrator account always has access to applications, enter the administrator account username.

You only need to enter the first eight characters of the short username in the **Username** field. For example, if the short username is "administrator", type "administ".



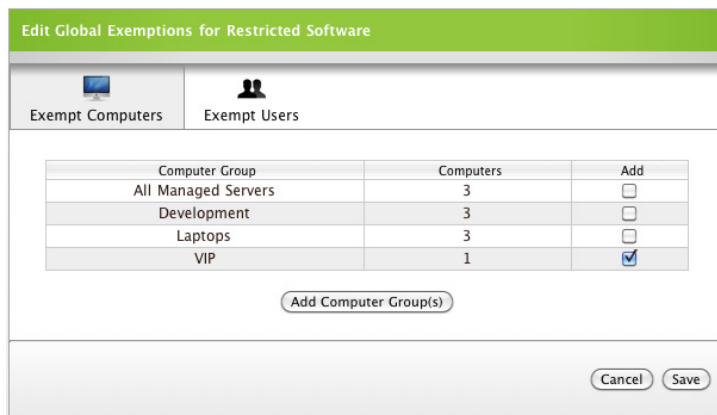
The screenshot shows a dialog box titled "Edit Restricted Software: Restricted Process". It has three tabs: "General", "Exempt Computers", and "Exempt Users". The "Exempt Users" tab is active. Below the tabs, there is a "Username:" label followed by a text input field. Below the input field is an "Add User" button. At the bottom right of the dialog are "Cancel" and "Save" buttons.

16. Click **Save**.

The restriction is enforced on client computers the next time they check in to the JSS.

#### To edit the Global Exemption list:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Restricted Software** link.
4. Click the **Edit Global Exemption List** button in the toolbar.
5. On the Exempt Computers pane, click the **Add <Group>** button to specify exempt computer groups, computers, buildings, or departments.
6. Click the **Add** checkbox next to each computer or group you want to add to the Global Exemption list.



The screenshot shows a dialog box titled "Edit Global Exemptions for Restricted Software". It has two tabs: "Exempt Computers" and "Exempt Users". The "Exempt Computers" tab is active. Below the tabs, there is a table with three columns: "Computer Group", "Computers", and "Add". The "Add" column contains checkboxes. The "VIP" row has its checkbox checked. Below the table is an "Add Computer Group(s)" button. At the bottom right of the dialog are "Cancel" and "Save" buttons.

Computer Group	Computers	Add
All Managed Servers	3	<input type="checkbox"/>
Development	3	<input type="checkbox"/>
Laptops	3	<input type="checkbox"/>
VIP	1	<input checked="" type="checkbox"/>

7. Click the **Exempt Users** tab and click the **Add User** button.

- In the **Username** field, enter the username for the account used to open the application. For example, to ensure the administrator account always has access to applications, enter the administrator account username.

You only need to enter the first eight characters of the short username in the **Username** field. For example, if the short username is "administrator", type "administ".

The screenshot shows a dialog box titled "Edit Global Exemptions for Restricted Software". It features a green header bar. Below the header, there are two tabs: "Exempt Computers" (with a computer icon) and "Exempt Users" (with a person icon). The "Exempt Users" tab is currently selected. The main area of the dialog contains a "Username:" label followed by a text input field. Below the input field is a button labeled "Add User". At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

- Click **Save**.

---

# Self Service

## Overview of Self Service

The Self Service application allows users to run management tasks on their computers without the help of an administrator. Using an intuitive interface similar to the one in iTunes, users can browse and run Self Service policies, access webpages, and utilize plug-ins developed with the Self Service API.

The JAMF Software Server (JSS) allows you to manage every aspect of Self Service, including its installation, preferences, and the items available to users.

The items in Self Service are simply policies configured with a few additional settings. You can make any policy available in Self Service and customize how it is displayed to users. This includes adding an icon and description, displaying the policy in relevant categories, and featuring it on the main page. Assigning users or computer groups to the policy's scope allows you to determine which users have access to it from Self Service.

You can also add plug-ins to extend the functionality of the application. Plug-ins can be URLs, which give users easy access to webpages right from the application, or custom plug-ins developed with the Self Service API.

# Managing User Authentication Preferences

User Authentication preferences allow you to control how users log in to Self Service and authenticate to install Self Service items.

## To manage User Authentication preferences:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Click the **End-User Authentication** tab.
6. In the **Network User Login** section, select how users log in to Self Service.
7. To require login with an LDAP directory account, select the **Users are required to log in** option.
8. To make login with an LDAP directory account optional, select the **Users can log in (Anonymous login is available)** option.

**Note:** Before selecting the required or optional settings, make sure an LDAP server connection is set up in the JSS. For instructions on how to set up an LDAP server connection, see the "Integrating with LDAP Servers" section.

9. If you do not have an LDAP connection set up or you do not want to require login, select the **Users are not required to log in** option.
10. In the **Local Authentication** section, select whether local authentication is required to run Self Service items.
11. Click the **Save** button.

# Installing Self Service

The JSS allows you to install Self Service on client computers using the Computer Management Framework settings or a policy. The Computer Management Framework settings automatically install Self Service on all enrolled computers, while a policy gives you more control over the deployment process.

**Note:** To uninstall Self Service, follow the instructions in the “Uninstalling Packages” section.

## To install Self Service using the Computer Management Framework settings:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Select the **Automatically install Self Service on all enrolled computers** checkbox.
6. To install Self Service in a custom location or give it a custom name, change the path or application name in the **Install Location** field.

Make sure the complete path is entered, including the application name and file extension (.app). For example:

/path/to/application name.app

7. Click the **Save** button.

## To install Self Service using a policy:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Make sure the **Automatically install Self Service on all enrolled computers** checkbox is deselected.
6. Click the **here** link to download the `Self Service.tar.gz` file.
7. Double-click the file to decompress it.
8. Use Composer or another package-building tool to package the Self Service application included in the file.  
For more information about building packages with Composer, see the “Building Packages” section.
9. Use Casper Admin to upload the package.  
For more information, see the “Managing Packages” section.
10. Create a policy to install Self Service.  
For detailed instructions, see the “Installing Packages” section.



# Making Policies Available in Self Service

Self Service items are policies configured with a few additional settings. Any policy can be made available in Self Service, but it is up to you to determine which policies are appropriate and which users should have access to them.

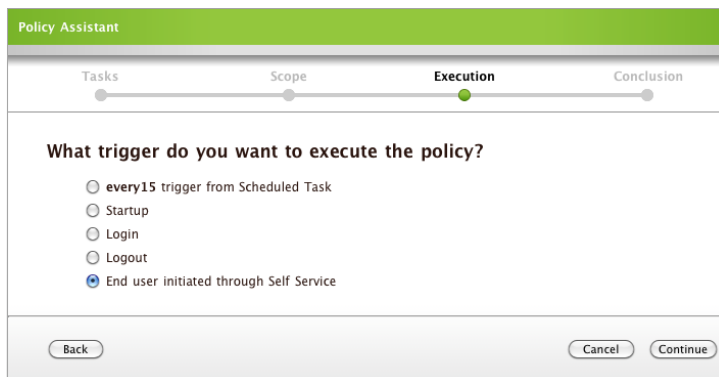
When you configure a policy for Self Service, you can customize the user experience by doing the following:

- Upload an icon
- Enter a description
- Assign the policy to one or more categories
- Feature the policy on the main pane or in a category

This section explains how to configure a policy for Self Service using the Policy Assistant or the manual policy interface.

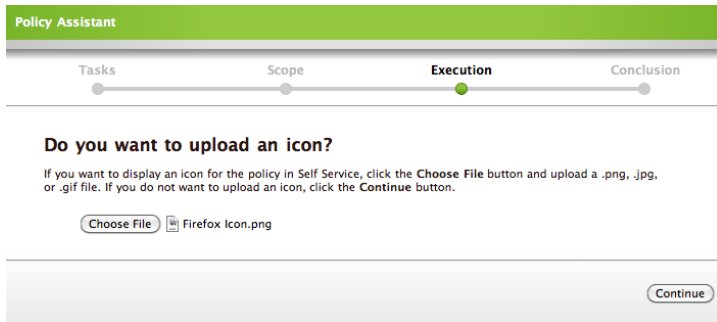
## To configure a policy for Self Service using the Policy Assistant:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Policies** link.
4. Click the **Create Policy** button.
5. Follow the onscreen instructions until you are asked to select a trigger. Then, select the **End user initiated through Self Service** option and click **Continue**.

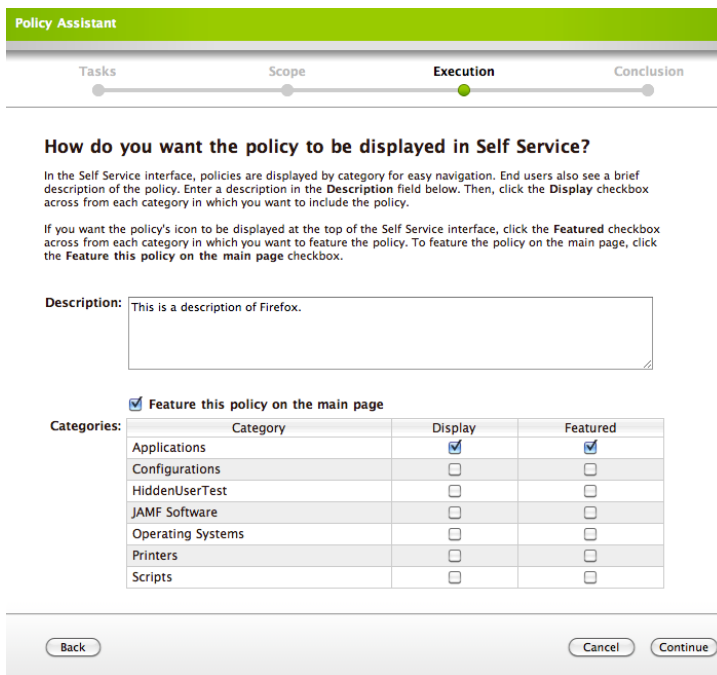


The screenshot shows the 'Policy Assistant' interface. At the top, there is a green header with the text 'Policy Assistant'. Below the header is a progress bar with four steps: 'Tasks', 'Scope', 'Execution', and 'Conclusion'. The 'Execution' step is currently active, indicated by a green dot. Below the progress bar, the question 'What trigger do you want to execute the policy?' is displayed. There are five radio button options: 'every15 trigger from Scheduled Task', 'Startup', 'Login', 'Logout', and 'End user initiated through Self Service'. The 'End user initiated through Self Service' option is selected, indicated by a blue dot. At the bottom of the form, there are three buttons: 'Back', 'Cancel', and 'Continue'.

- To display an icon, click the **Choose File** button and upload an icon. Then, click **Continue**.  
If you do not want to display an icon, simply click **Continue**.



- Enter a description in the **Description** field if desired.
- To display the policy in a category, select the **Display** checkbox across from the category.
- If you uploaded an icon, select the **Feature this policy on the main page** checkbox to feature the policy on the main pane in Self Service.  
To feature the policy in a category, select the **Featured** checkbox across from the category.
- Click **Continue**.

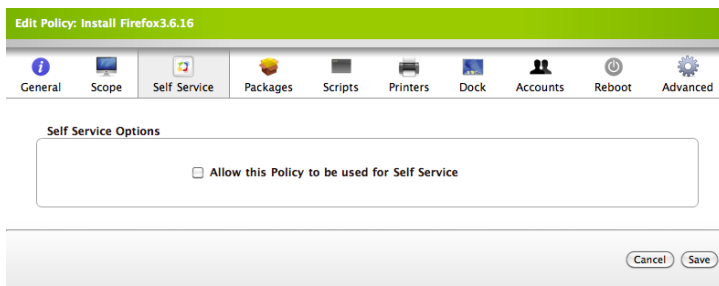


- Follow the rest of the onscreen instructions to complete the Policy Assistant and save the policy.  
Clients in the scope display the policy in Self Service the next time they check in with the JSS.

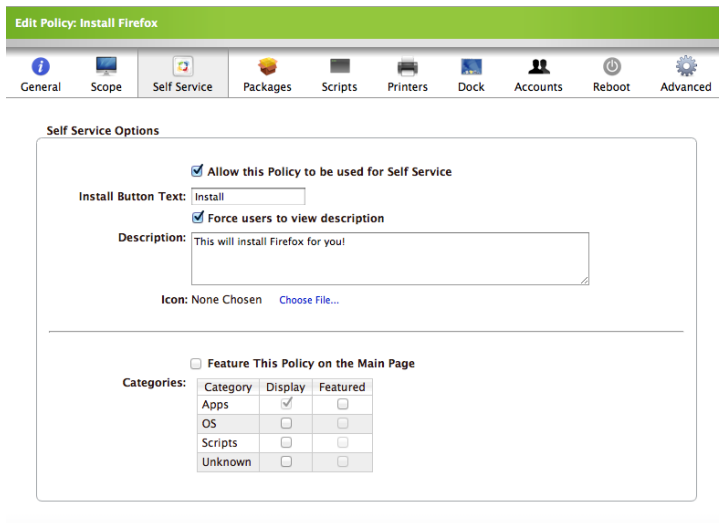
**To configure a policy for Self Service manually:**

- Log in to the JSS with a web browser.

2. Click the **Management** tab.
3. Click the **Policies** link.
4. Create a new policy or edit an existing policy.
  - To create a new policy, click the **Create Policy** button.
  - To edit an existing policy, click the **Edit Policy** link across from the policy.
5. If you created a new policy, configure it as needed.  
For more information, see the “Policies” section.
6. Click the **General** tab and choose “None (or Self Service Only)” from the **Triggered By** pop-up menu.
7. Click the **Self Service** tab and select the **Allow this Policy to be used for Self Service** checkbox.

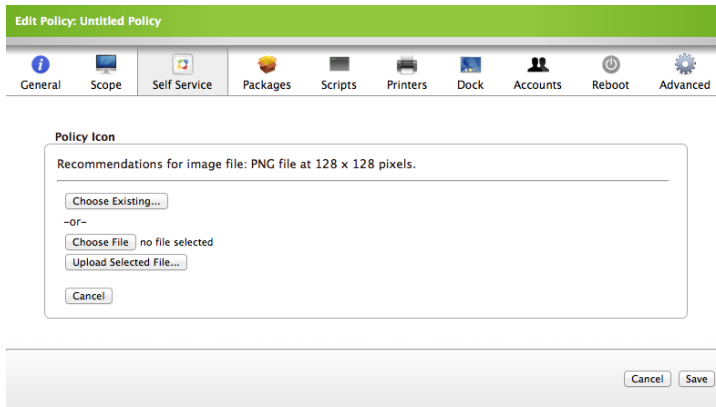


8. To customize the button that users click to run the policy, modify the text in the **Install Button Text** field.  
For example, if the policy allows users to update software, type “Update” in the text field.
9. Enter a description in the **Description** field if desired.

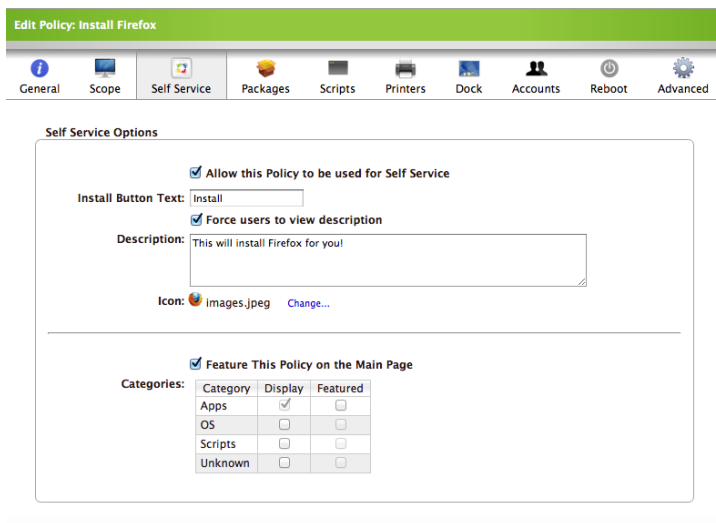


10. To force users to view the description before they run the policy, select the **Force users to view description** checkbox.

11. To display an icon, click the **Choose File** link.
  - To choose an icon that you previously uploaded, click the **Choose Existing** button.
  - To upload a new icon, click the **Choose File** button.



12. If you uploaded an icon, select the **Feature This Policy on the Main Page** checkbox to feature the policy on the main pane in Self Service.
13. To display the policy in a category, select the **Display** checkbox across from the category. The category that you specified on the General pane is selected by default.
14. If you uploaded an icon, select the **Featured** checkbox across from a category to feature the policy in the category.
15. Click **Save**.



Clients in the scope display the policy in Self Service the next time they check in with the JSS and meet the criteria on the General and Scope panes.

# Managing Self Service Plug-ins

The JAMF Software Server (JSS) allows you to add the following plug-ins to Self Service to extend the functionality of the application:

- URL plug-ins that give users quick, easy access to webpages
- Self Service Plug-in bundles that allow users to utilize plug-ins developed with the Self Service API

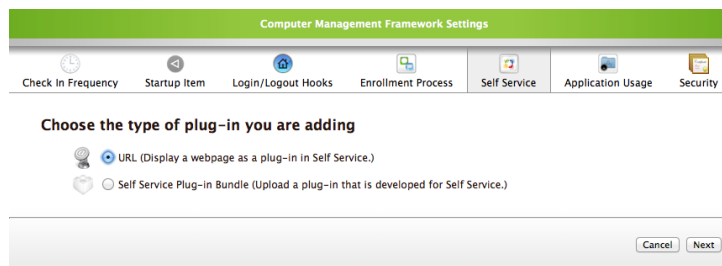
You can also use the JSS to edit URL plug-ins and remove both kinds of plug-ins from Self Service.

## URL Plug-ins

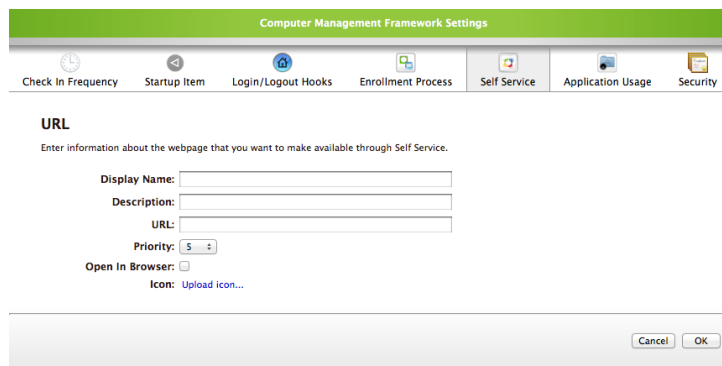
URL plug-ins open a webpage in a browser or display web clips in the Self Service interface.

To add a URL plug-in:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Click the **Plug-ins** tab.
6. Click the **Add new plug-in** link.
7. Make sure the **URL** option is selected and then click **Next**.



8. In the **Display Name** field, enter a name of the webpage, such as "JAMF Software".



9. Enter a description in the **Description** field if desired.
10. Enter the URL of the webpage in the **URL** field. For example:  
http://example.com
11. Use the **Priority** pop-up menu to specify the order in which the plug-in should be displayed in the Plug-ins list. For example, choose "1" to display the plug-in at the top of the list.  
If you do not choose a priority, the plug-in is displayed in alphabetical order by display name.
12. If you want the webpage to automatically open in a browser, select the **Open in Browser** checkbox.  
If you do not select this checkbox, the web clip is displayed in the Self Service interface.
13. To display an icon, click the **Upload icon** link. Click the **Choose File** button to select an icon and then click the **Upload Selected File** button to upload it.
14. Click the **OK** button, and then click **Save**.

#### **To edit a URL plug-in:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Click the **Plug-ins** tab.
6. Click the **Edit** link across from the plug-in you want to edit and make the necessary changes.
7. Click the **OK** button, and then click **Save** for the changes to take effect.

#### **To remove a URL plug-in:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Click the **Plug-ins** tab.
6. Click the **Delete** link across from the plug-in you want to remove from Self Service.
7. Click **Save**.

# Self Service Plug-in Bundles

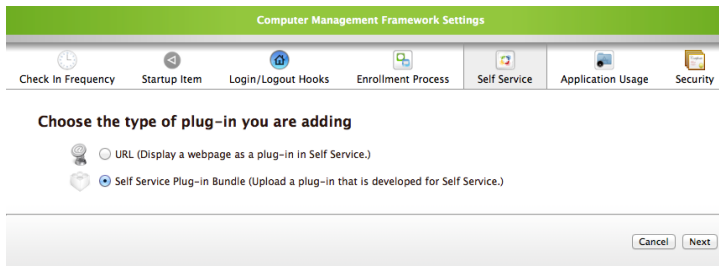
The Self Service API allows developers to write their own plug-ins for Self Service. The Self Service API is located in:

`SelfService.app/Contents/Resources/SSPluginProtocol.h`

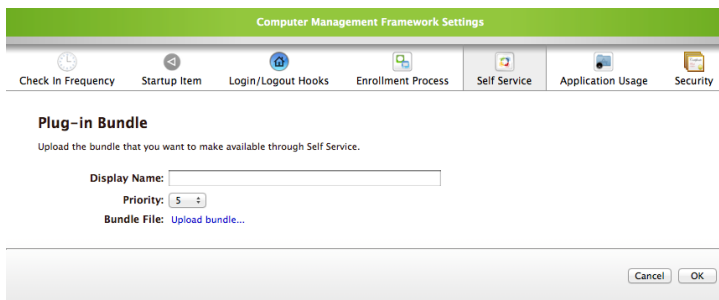
This section explains how to add and remove Self Service Plug-in bundles.

## To add a Self Service Plug-in bundle:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Click the **Plug-ins** tab.
6. Click the **Add new plug-in** link.
7. Select the **Self Service Plug-in Bundle** option and then click **Next**.

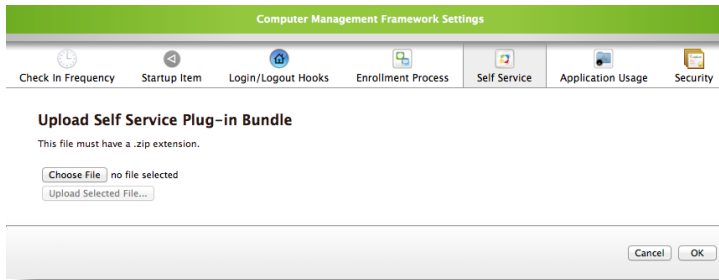


8. Enter a name in the **Display Name** field.



9. Use the **Priority pop-up** menu to specify the order in which the plug-in should be displayed in the Plug-ins list. For example, choose "1" to display the plug-in at the top of the list.  
If you do not choose a priority, the plug-in is displayed in alphabetical order by display name.
10. Click the **Upload Bundle** link.

11. Click the **Choose File** button and select a Self Service Plug-in bundle. This file must be a compressed .bundle file. For example:  
ExamplePluginB.bundle.zip



12. Click the **Upload Selected File** button.
13. Click the **OK** button, and then click **Save**.

#### To remove a Self Service Plug-in bundle:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Computer Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Click the **Plug-ins** tab.
6. Click the **Delete** link across from the plug-in you want to remove.
7. Click **Save**.



# Installing Items from Self Service

Before making policies available through Self Service, make sure that it is installed on client computers. For detailed instructions, see the “Installing Self Service” section.

To run Self Service, clients must meet the following requirements:

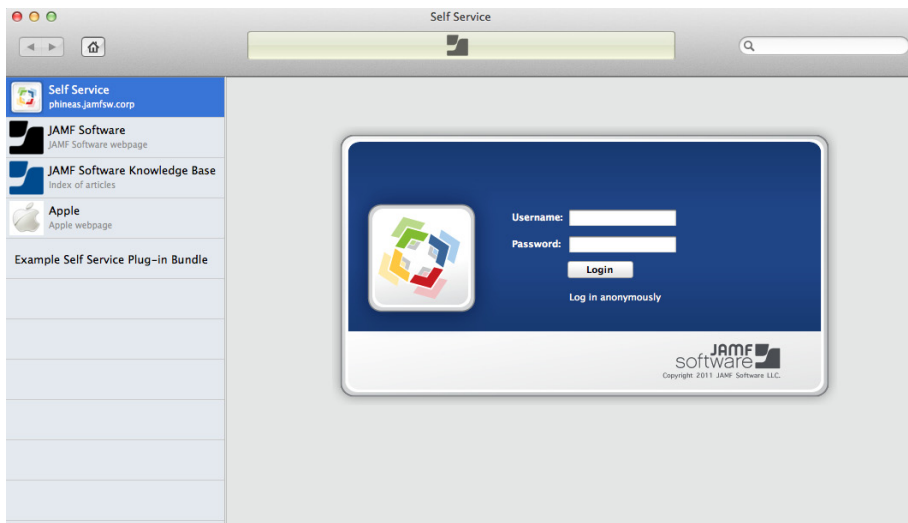
- They are enrolled with the JSS.
- They exist in the JSS and have an SSL (remote login) account associated with them.
- The `com.jamfsoftware.jss.plist` file exists in the following directory:  
/Users/<username>/Library/Preferences/

Self Service allows users to run policies and utilize plug-ins from an interface similar to the one in iTunes.

## Logging In

Users see a Login pane if the User Authentication preferences are configured to require login or make it optional. (See the “Managing User Authentication Preferences” section for more information.)

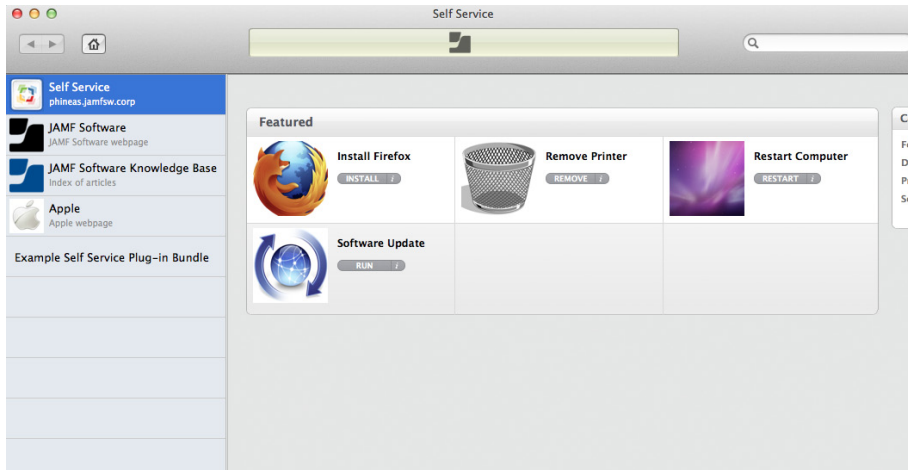
To log in, users must enter credentials for an LDAP directory account. If optional login is permitted, they can also click the **Log in anonymously** link.



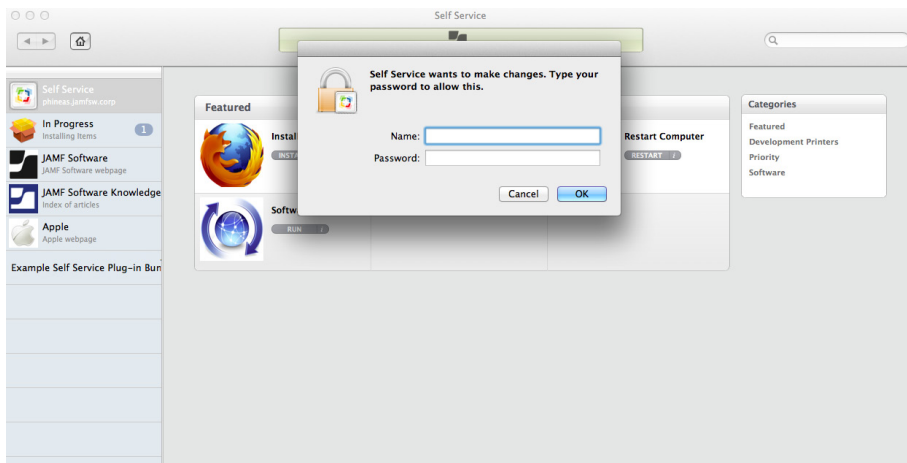
## Running Policies

Users can browse policies from the Featured section or the Categories list.

**Note:** Only policies configured with the **Feature This Policy on the Main Page** option are displayed in the Featured section. See the “Making Policies Available in Self Service” section for more information.

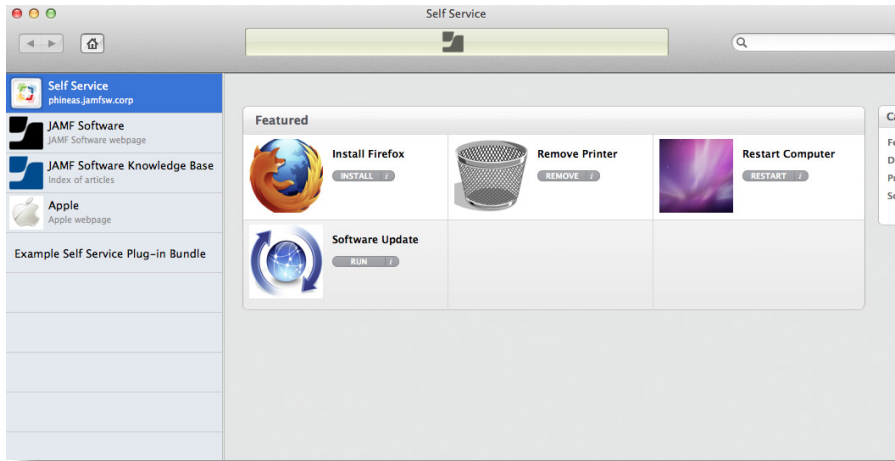


Users run a policy by clicking the button next to it. If the User Authentication preferences are configured to require local authentication, users are prompted to enter their local credentials before running the policy.

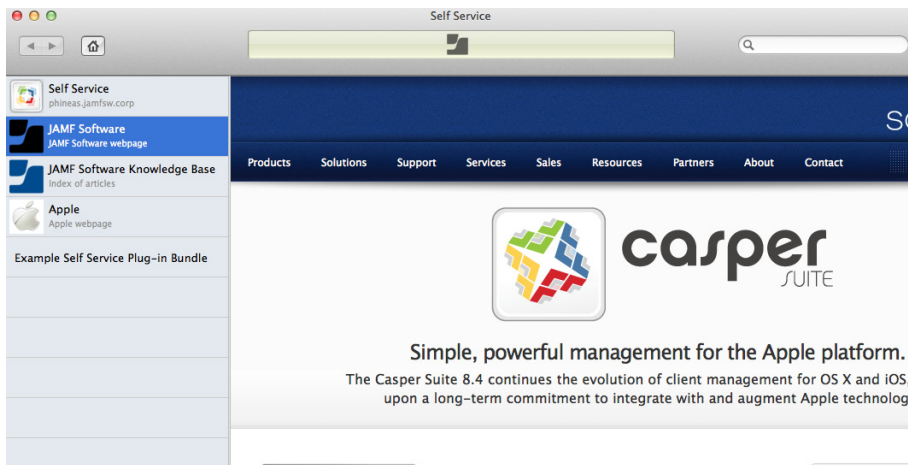


## Accessing Plug-ins

Plug-ins are displayed in the Plug-in Library to the left of the window.



Users click a plug-in to display a webpage or utilize a plug-in developed with the Self Service API.





## Chapter 3: Mobile Device Management

# Building Your MDM Framework

## Configuring the Mobile Device Management Framework

Use the Global and Computer Management Framework settings to control how the JAMF Software Server (JSS) and enrolled mobile devices interact.

### Global Management Framework Settings

The Global Management Framework settings allow you to configure and manage the following security components for the JSS:

- JSS URL
- Public key infrastructure (PKI)
- Apple Push Notification service (APNs) certificate

#### JSS URL

The JSS URL is the URL that enrolled mobile devices connect to when communicating with the JSS. The full URL of the JSS must be entered on this pane, including the correct protocol, domain, and port. For example:

`https://jss.mycompany.com:8443/`

If this field is blank or the URL is incorrect, enrolled devices are unable to connect to the server.

#### To view the JSS URL:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.

4. Click the **JSS URL** tab.

The URL of the JSS is entered in the **JSS URL** field.

The screenshot shows a dialog box titled "Global Management Framework Settings" with three tabs: "JSS URL", "Public Key Infrastructure", and "Push Notification Certificate". The "JSS URL" tab is active. Below the tab header, there is a description: "This is the URL that computers and mobile devices will connect to when communicating with the JSS." There are two input fields: "JSS URL:" with the value "https://norman.local:8443/" and an example "Example: https://jss.mycompany.com:8443/"; and "JSS URL (HTTP):" with the value "http://norman.local:9006/" and an example "Example: http://jss.mycompany.com:9006/". A note below the fields states: "Note: The JSS URL HTTP is only used for accessing the built-in SCEP server if you are installing Enrollment Profiles with iPhone Configuration Utility. If your JSS has a pre-trusted root certificate, you can leave this field blank." At the bottom right, there are "Cancel" and "Save" buttons.

5. Click **Save**.

## Public Key Infrastructure

To ensure the security of over-the-air tasks, the JSS requires a PKI that supports certificate-based authentication. This includes:

- A certificate authority (CA) with Simple Certificate Enrollment Protocol (SCEP) capabilities
- A signing certificate
- A CA certificate

If you do not have access to an external CA with SCEP capabilities, you can use the built-in CA that is enabled by default in the JSS. The built-in CA has the signing and CA certificates uploaded for you.

If your organization uses an external CA with SCEP capabilities, you can integrate it with the JSS using one of the following methods:

- **Create a signing certificate and upload a CA certificate**

This method allows you to use the JSS to generate a certificate signing request (CSR) that you will use to obtain the signing certificate. After you obtain the signing certificate from the CA, upload it and the CA certificate to the JSS to complete the integration.
- **Upload a signing certificate keystore and a CA certificate**

This method allows you to include a certificate chain for the signing certificate. To do this, you must upload a signing certificate keystore (.jks or .p12 file) that includes a private key and its associated certificate or certificate chain. Once you've selected the certificate to use as your signing certificate, you can upload a CA certificate or CA certificate bundle to complete the integration.

### To integrate an external CA with the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.

3. Click the **Global Management Framework Settings** link.
4. Click the **Public Key Infrastructure** tab.
5. Select **Use External Certificate Authority** and specify information about the CA and the SCEP server. Be sure to choose the type of challenge password that will be used as the pre-shared secret for enrollment.
  - If you want computers and devices to use the same challenge password, select the **Static** option.
  - If you have a non-Microsoft CA and want computers and devices to use unique challenge passwords, select the **Dynamic** option.

The **Dynamic** option requires use of the JSS API and membership in the JAMF Software Developer Program. Before selecting this option, contact your Account Manager to learn more about the JAMF Software Developer Program and the additional steps you need to take to use this option.

  - If you have a Microsoft CA and want computers and devices to use unique challenge passwords, select the **Dynamic-Microsoft CA** option.

**Note:** If you want mobile devices to use unique challenge passwords, you must enroll them over-the-air (OTA). For more information on OTA enrollment, see "Enrolling Mobile Devices OTA".

The screenshot shows the 'Public Key Infrastructure' configuration page within the 'Global Management Framework Settings' application. The page has a green header and three tabs: 'JSS URL', 'Public Key Infrastructure' (selected), and 'Push Notification Certificate'. Below the tabs, the 'Public Key Infrastructure' section contains a descriptive paragraph and several configuration options:

- Two radio buttons for 'Use Built-in Certificate Authority' (unselected) and 'Use External Certificate Authority' (selected).
- Input fields for 'Base URL for the SCEP Server' (required), 'The name of the instance: CA-IDENT' (optional), and 'Subject (Representation of a X.500 name)' (optional).
- A dropdown menu for 'Subject Alternative Name Type' set to 'None'.
- 'Challenge Type' radio buttons: 'Static' (selected), 'Dynamic', and 'Dynamic-Microsoft CA'.
- Input fields for 'Challenge' and 'Verify Challenge', both masked with asterisks.
- A dropdown menu for 'Key Size in bits' set to '1024'.
- Two checked checkboxes: 'Use as digital signature' and 'Use for key encipherment'.
- An empty input field for 'Fingerprint hex string'.
- A link at the bottom: 'Signing Certificate: [Signing and CA Certificate Assistant...](#)

6. Click the **Signing and CA Certificate Assistant** link.
7. Choose a method for providing the signing and CA certificates, and then click **Continue**.
8. Follow the onscreen instructions.
9. When you complete the assistant, click **Save**.

## Apple Push Notification Service Certificate

For the JSS to perform over-the-air management tasks, it must be able to communicate with Apple Push Notification service (APNs). To enable this communication, you must obtain an APNs certificate (.pem) from Apple and upload it to the JSS.

The JSS guides you through the process of generating or renewing an APNs certificate from the Apple Push Certificates Portal. This process requires:

- A valid JAMF Nation account  
To create a JAMF Nation account, go to:  
<https://jamfnation.jamfsoftware.com/createAccount.html>
- A valid Apple ID

### To generate or renew an APNs certificate:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Global Management Framework Settings** link.
4. Click the **Push Notification Certificate** tab.
5. To generate an APNs certificate for the first time, click the **Create a certificate using the Push Notification Certificate Assistant** link.  
To renew your APNs certificate, click the **Renew your Push Notification Certificate** link.
6. Choose how you want to obtain the CSR.
  - If the server hosting the JSS has an outbound connection, select **Request Signed CSR Automatically through JAMF Nation**. Enter the username and password for your JAMF Nation account, and then click **Continue**.

Push Notification Certificate Assistant

Get Signed CSR   Request Cert   Upload Cert   Complete

### Get Signed CSR

Before Apple issues a Push Notification Certificate for you to use, JAMF Software must provide you with a signed CSR. The CSR is generated by your JSS and sent to JAMF Software. Once JAMF Software has verified the authenticity of the request, a signed CSR will be returned in a plist file. JAMF Software never has access to the private key used to generate the CSR.

Request Signed CSR Automatically through JAMF Nation

JAMF Nation Username:

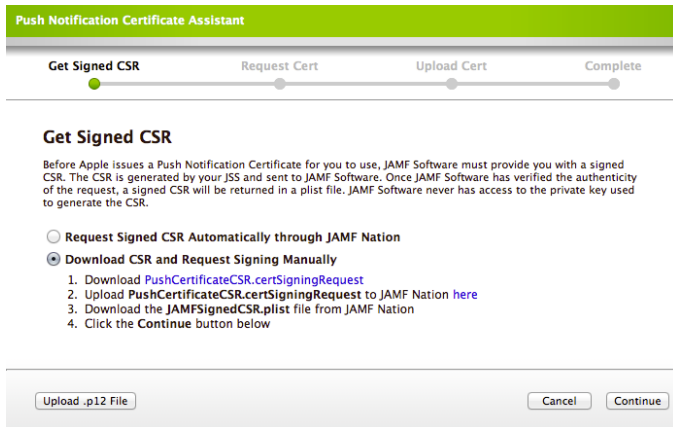
Password:

Download CSR and Request Signing Manually

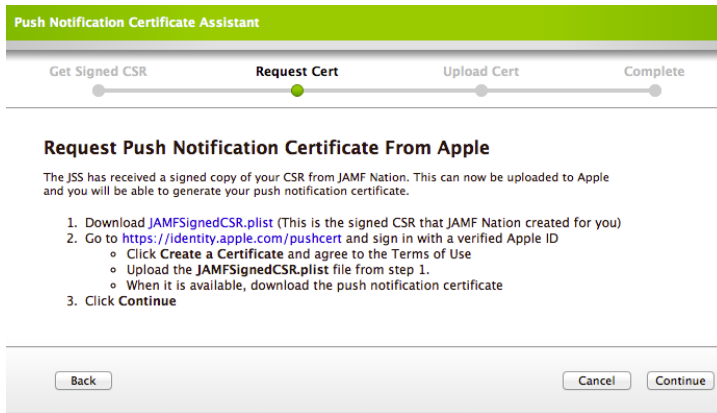
The JSS connects to JAMF Nation over port 443 and obtains the signed CSR. (You will download the CSR in the next step.)



- If the server hosting the JSS does not have an outbound connection, select **Download CSR and Request Signing Manually**. Then, follow the onscreen instructions to get the CSR signed.



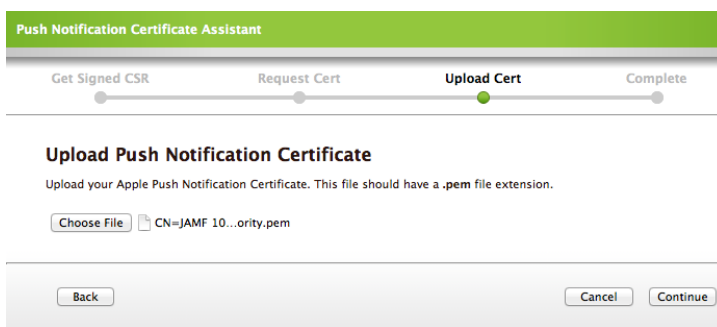
7. On the Request Cert pane, follow the onscreen instructions to request an APNs certificate from Apple.



**Note:** It is recommended that you sign in to the Apple Push Certificates Portal with a corporate Apple ID, since the account will be associated with your corporate APNs certificate.

If you are renewing an APNs certificate originally obtained from Apple's iOS Developer Enterprise Program (iDEP), you must sign in using the Apple ID for the iDEP Agent account.

8. On the Upload Cert pane, click **Choose File**. Select the APNs certificate (.pem) that you want to upload and click **Choose**. Then, click **Continue** in the JSS.



9. Click **Done** to save the certificate.

# Mobile Device Management Framework Settings

The Mobile Device Management Framework settings allow you to set up and manage preferences for the following aspects of MDM:

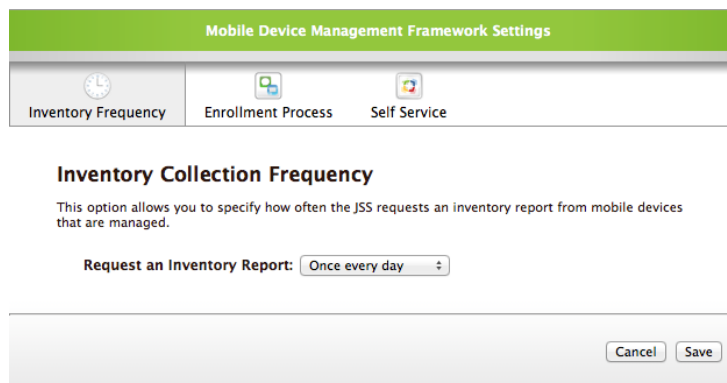
- Inventory collection frequency
- Over-the-Air (OTA) enrollment process
- Self Service web clip

## Inventory Collection Frequency

The inventory collection frequency allows you to control how often enrolled devices submit inventory to the JSS. Devices can submit inventory once every day, once every week, or once every month.

**To modify the inventory collection frequency:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Mobile Device Management Framework Settings** link.
4. Choose an inventory collection frequency from the **Request an Inventory Report** pop-up menu.



5. Click **Save**.

## OTA Enrollment

Use the Enrollment Process pane to set up or modify the following preferences for OTA enrollment:

### **Allow enrollment without invitation**

Allows you to provide an enrollment URL where users can initiate the enrollment process. (This option is selected by default.)

### **Users should install the CA Certificate**

Requires users to install the CA certificate during the OTA enrollment process. (This option is selected by default.)

### **Login and Profile page fields**

Allows you to customize the text that is displayed to users on the Login and Profile pages of the OTA enrollment process.

### To set up or modify OTA Enrollment preferences:

1. Log in to the JSS in a web browser.
2. Click the **Settings** tab.
3. Click the **Mobile Device Management Framework Settings** link.
4. Click the **Enrollment Process** tab.
5. Select or deselect options as needed.

The screenshot shows the 'Mobile Device Management Framework Settings' interface. At the top, there is a green header with the title. Below it, a navigation bar contains three tabs: 'Inventory Frequency', 'Enrollment Process' (which is selected), and 'Self Service'. The main content area is titled 'Enrollment Process' and includes a sub-header 'Enrollment Process' and a descriptive paragraph: 'This section allows you to customize the end user experience for over-the-air enrollment.' There are two checked checkboxes: 'Allow enrollment without invitation' and 'Users should install the CA Certificate'. Below these are four input fields: 'Login page title' (containing 'OTA Enrollment'), 'Login page description' (containing 'Complete this process for secure access to our network.'), 'Profile Display Name' (containing 'MDM Profile'), and 'Profile description' (containing 'This profile ensures the security of your mobile device.'). At the bottom right, there are 'Cancel' and 'Save' buttons.

6. Customize text for the Login and Profile pages as needed. These pages are displayed to users during the enrollment process.
7. Click **Save**.

## Self Service Web Clip

The Self Service web clip is added to enrolled devices by default. It allows you to distribute configuration profiles, apps, eBooks, and updated MDM profiles to devices for users to install. Users tap the web clip to browse and install items using an interface similar to the App Store.

Use the Self Service Web Clip pane to set up and modify the following preferences for the Self Service web clip:

### Install Self Service Web Clip

Adds the Self Service web clip to all enrolled devices. When this option is selected, the Self Service web clip is displayed on devices' Home screens after the devices are enrolled with the JSS. (This option is selected by default.)

### **Require users to log in**

Requires users to log in to the Self Service web clip with credentials for an LDAP directory account or a JSS user account that has OTA enrollment privileges. (See “Integrating with LDAP Servers” or “Managing JSS User Accounts” for more information.)

### **Allow users to install all in-house applications with one tap**

Displays an **Install All** button in the Self Service web clip that allows users to install all in-house apps with a single tap. (This option is selected by default.)

### **Prompt user to update MDM Profile**

Displays an updated MDM profile in the Self Service web clip when an enrolled device is upgraded to iOS 5. When the user installs the update, the device receives app management capabilities without losing communication with the JSS.

**Note:** Only devices enrolled by OTA invitation or enrollment URL can obtain an updated MDM profile via the Self Service web clip.

### **Show App Store App Updates**

Displays App Store app updates in the Self Service web clip.

**Note:** The **Update** tab in the Self Service web clip only displays App Store app updates that are distributed using the JSS.

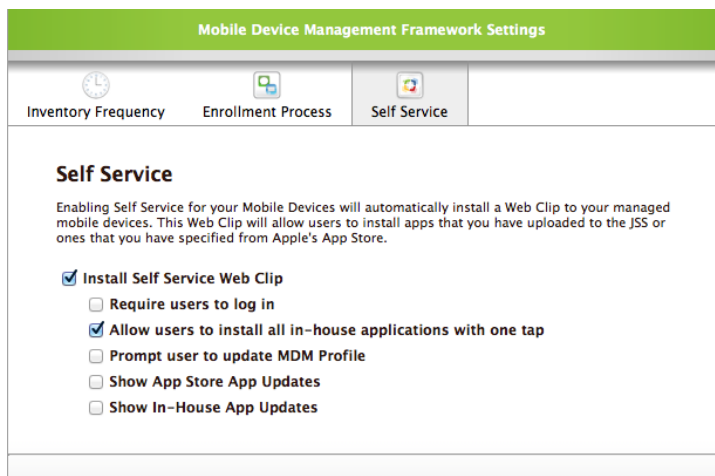
### **Show In-House App Updates**

Displays in-house app updates in the Self Service web clip.

### **To set up or modify Self Service web clip preferences:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Mobile Device Management Framework Settings** link.
4. Click the **Self Service** tab.
5. Select the **Install the Self Service Web Clip** checkbox to add the Self Service web clip to enrolled mobile devices.

6. Select or deselect additional options as needed.



7. Click **Save**.

# Enrollment

## About Mobile Device Enrollment

Enrolling mobile devices with the JAMF Software Server (JSS) is the first step to managing mobile devices. Enrollment establishes a connection between the devices and the JSS, allowing you to perform over-the-air management tasks without requiring user interaction.

The following components are installed during enrollment:

- **Profile that contains the CA certificate.** The CA certificate establishes trust between the certificate authority (CA) and enrolled mobile devices.
- **MDM profile.** This profile includes a SCEP enrollment request and an MDM enrollment request.
- **Device certificate.** This certificate validates the identity of enrolled mobile devices each time they communicate with the JSS.
- **Self Service Web Clip.** The Self Service web clip is added to enrolled devices by default. It allows you to distribute configuration profiles, apps, eBooks, and updated MDM profiles to devices for users to install. Users tap the web clip to browse and install items using an interface similar to the App Store. For information on how to configure Self Service Web Clip preferences, see the "Self Service Web Clip" section in "Configuring the Mobile Device Management Framework".

The JSS allows you to initiate over-the-air enrollment by providing users with an enrollment URL or sending an OTA invitation to devices or users.. You can also enroll devices that are connected to a computer by USB by creating an enrollment profile in the JSS and installing it on the devices.

For complete instructions on enrolling mobile devices, see "Enrolling Mobile Devices OTA" or "Enrolling Connected Mobile Devices".

# Enrolling Mobile Devices OTA

The JSS allows you to initiate over-the-air enrollment by providing users with an enrollment URL or sending an OTA invitation to devices or users.

## Providing an Enrollment URL

You can allow users to enroll their own devices by providing them with an enrollment URL. The enrollment URL is the full URL for the JSS followed by /enroll/. For example:

`https://jss.mycompany.com/8443/enroll/`

Users go to the URL, log in with an LDAP directory account or JSS user account, and then follow a series of onscreen instructions to enroll their devices.

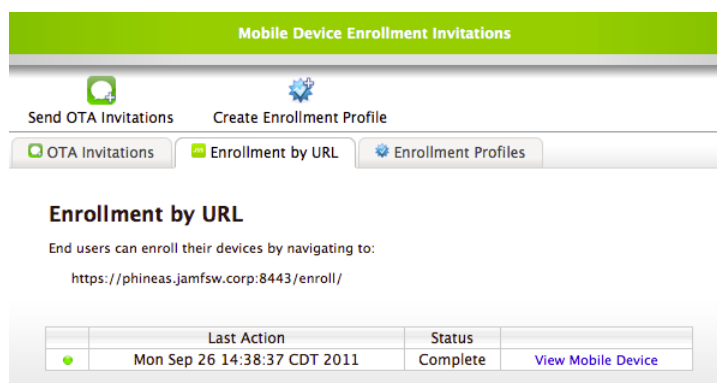
If location information collection is enabled in the JSS and users log in with an LDAP directory account, location information for the device is collected during enrollment.

Providing an enrollment URL requires:

- An LDAP server connection set up in the JSS or a JSS user account with OTA enrollment privileges (See "Integrating with LDAP Servers" or "Managing JSS User Accounts" for instructions on how to set up one of these requirements.)
- The **Allow enrollment without invitation** option enabled in the JSS (See the "OTA Enrollment" section in "Configuring the Mobile Device Management Framework" for more information.)
- Mobile devices with access to a wireless network connection

**To view the status of URL enrollments:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link, and then click the **Enrollment by URL** tab.



**Mobile Device Enrollment Invitations**

Send OTA Invitations    Create Enrollment Profile

OTA Invitations    **Enrollment by URL**    Enrollment Profiles

**Enrollment by URL**

End users can enroll their devices by navigating to:  
`https://phineas.jamfsw.corp:8443/enroll/`

	Last Action	Status	
●	Mon Sep 26 14:38:37 CDT 2011	Complete	<a href="#">View Mobile Device</a>

## Sending OTA Invitations

You can allow users to enroll their own devices by sending them an OTA invitation via email or text message (SMS). Users tap the URL in the invitation and follow a series of onscreen instructions to enroll their devices.

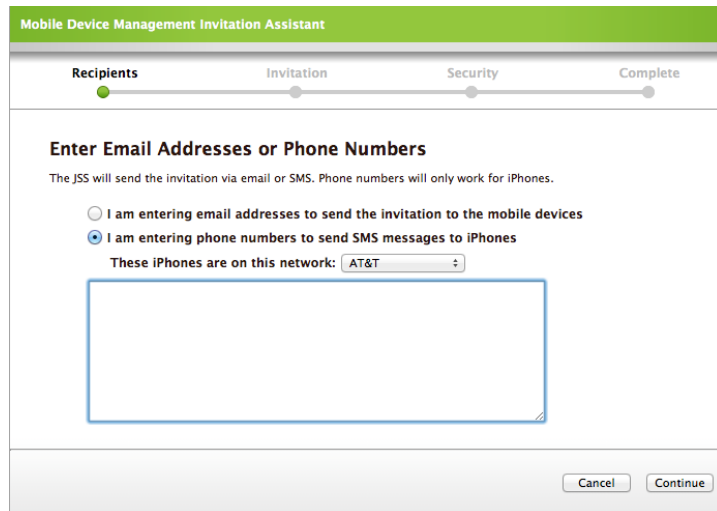
Enrolling mobile devices by sending an OTA invitation requires:

- An SMTP server set up in the JSS (See “Enabling Email Notifications” for detailed instructions.)
- Mobile devices with access to a wireless network connection
- (SMS invitations only) A valid phone number with SMS capabilities

**To enroll mobile devices by sending an OTA invitation:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link.
4. Click the **Send OTA Invitations** button.
5. Choose whether to send the invitation by email or SMS.

If you choose to send an SMS invitation, use the pop-up menu that is displayed to specify the network carrier.



The screenshot shows the 'Mobile Device Management Invitation Assistant' interface. At the top, there is a green header bar with the title. Below it is a progress bar with four steps: 'Recipients', 'Invitation', 'Security', and 'Complete'. The 'Recipients' step is currently active, indicated by a green dot. The main content area is titled 'Enter Email Addresses or Phone Numbers' and includes the instruction: 'The JSS will send the invitation via email or SMS. Phone numbers will only work for iPhones.' There are two radio buttons: 'I am entering email addresses to send the invitation to the mobile devices' (unselected) and 'I am entering phone numbers to send SMS messages to iPhones' (selected). Below the radio buttons is a dropdown menu labeled 'These iPhones are on this network:' with 'AT&T' selected. A large empty text input field is provided for entering the addresses. At the bottom right, there are 'Cancel' and 'Continue' buttons.

6. Enter the email addresses or phone numbers that you want to send the invitation to, and then click **Continue**.  
Each entry must be separated with a line break or comma.



7. Customize the invitation message as needed, and then click **Continue**.

The screenshot shows the 'Enter Invitation Message' step in the Mobile Device Management Invitation Assistant. The progress bar at the top indicates the current step is 'Invitation', with 'Recipients', 'Security', and 'Complete' following. The main content area contains the following fields and text:

- Sender's name:** JSS (optional)
- Reply-To:** (optional)
- Subject:** Your Mobile Device Enrollment Invitation
- Message:** A text area containing the message content: "Please follow the link below on your iPhone, iPad or iPod touch. Enrolling your mobile device gives you better access to our network and ensures the security of your data." followed by "%@" and "Thank you, Your IT Department".

At the bottom, there are three buttons: 'Back', 'Cancel', and 'Continue'.

8. Specify an expiration date for the invitation.

The screenshot shows the 'Invitation Security Options' step in the Mobile Device Management Invitation Assistant. The progress bar at the top indicates the current step is 'Security', with 'Recipients', 'Invitation', and 'Complete' following. The main content area contains the following options:

- Expires On:** 12 / 23 / 2010 at 11 : 00 : AM
- Require login**
- Allow multiple uses of invitations**

At the bottom, there are three buttons: 'Back', 'Cancel', and 'Continue'.

9. If you want to require users to authenticate with an LDAP directory account or a JSS user account with OTA enrollment privileges, leave the **Require login** checkbox selected. See "Integrating with LDAP Servers" or "Managing JSS User Accounts" for more information.
10. If you want to allow multiple uses of the invitation, leave the **Allow multiple uses of invitations** checkbox selected, and then click **Continue**.

11. Verify that the information on the Complete pane is correct, and then click **Send**.

The screenshot shows the 'Complete' pane of the Mobile Device Management Invitation Assistant. At the top, a progress bar indicates four steps: Recipients, Invitation, Security, and Complete, with 'Complete' being the active step. The main content area is titled 'Complete!' and contains the following details:

- To:** useremail@mycompany.com
- From:** JSS
- Subject:** Your Mobile Device Enrollment Invitation
- Message:** Please follow the link below on your iPhone, iPad or iPod touch. Enrolling your mobile device gives you better access to our network and ensures the security of your data. %@ Thank you, Your IT Department

At the bottom of the pane, there are three buttons: 'Back', 'Cancel', and 'Send'.

#### To view the status of OTA enrollments:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link, and then click the **OTA Invitations** tab.

The screenshot shows the 'Over-the-Air Invitations' section of the Mobile Device Enrollment Invitations interface. The toolbar includes 'Send OTA Invitations' and 'Create Enrollment Profile'. The 'OTA Invitations' tab is selected, showing a table of sent invitations.

	Sent to	Last Action	Status	
•	useremail@mycompany.com	Mon Sep 26 12:20:56 PDT 2011	Invitation sent	<a href="#">Revoke...</a>

# The OTA Enrollment User Experience

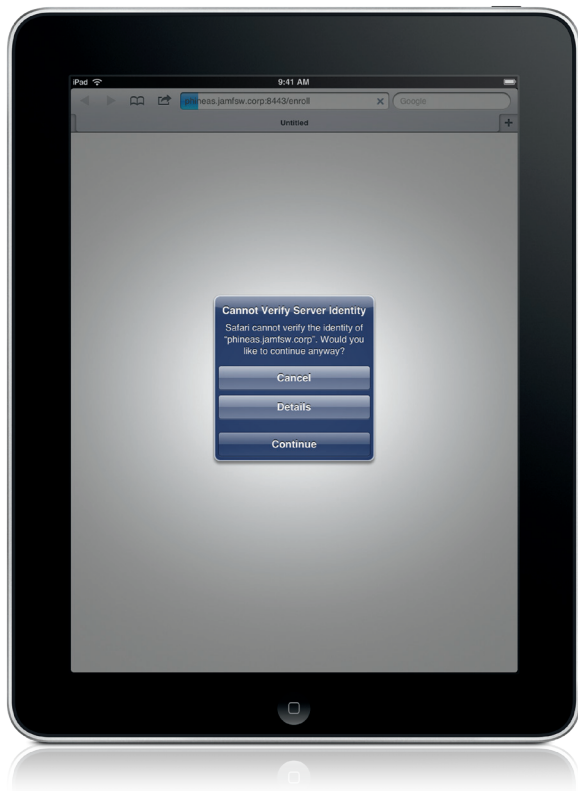
When users tap the URL in an OTA invitation or navigate to the enrollment URL from their devices, they are guided through the following steps to enroll:

1. If prompted, users must enter credentials for an LDAP directory account or a JSS user account with OTA enrollment privileges, and then tap **Login**.

This login prompt only appears if you initiated the enrollment process by providing users with an enrollment URL, or by sending an OTA invitation and requiring login. (See “Enrolling Mobile Devices OTA” for more information.)

2. If notified that the device cannot verify the identity of the JSS, users must tap **Continue**.

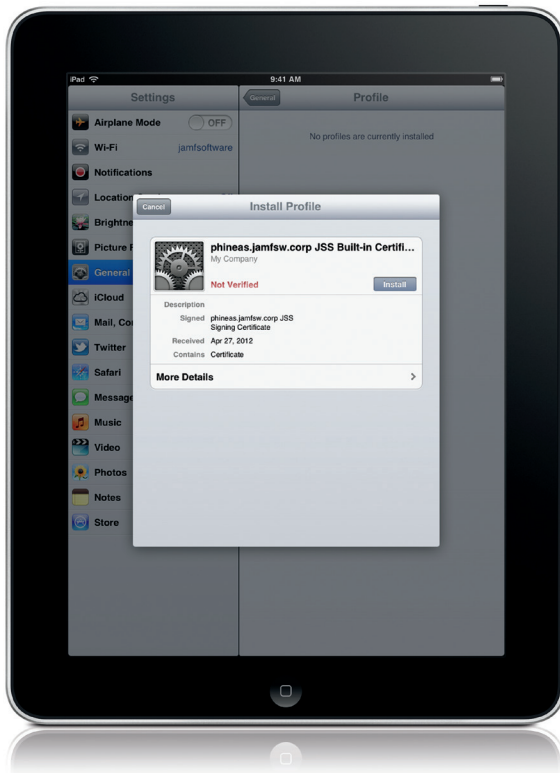
This notification only appears if your web server certificate is not natively trusted by devices.



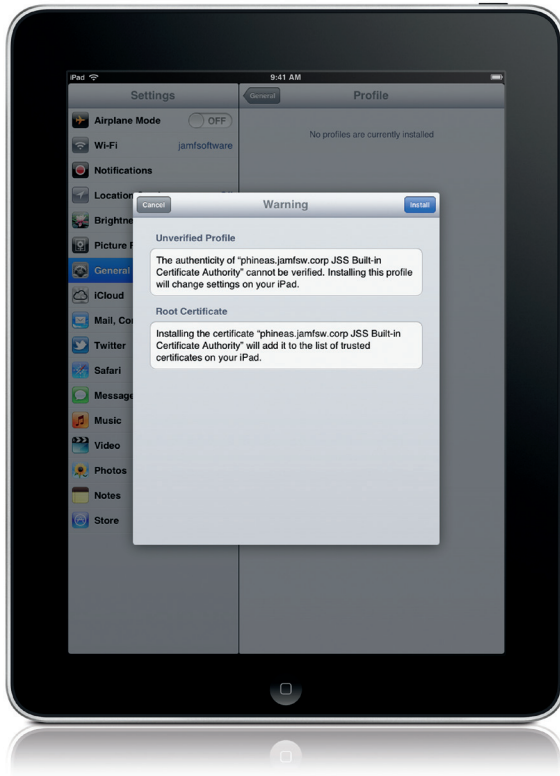
- Users must tap **Install Certificate** to initiate installation of the profile that contains the CA certificate.



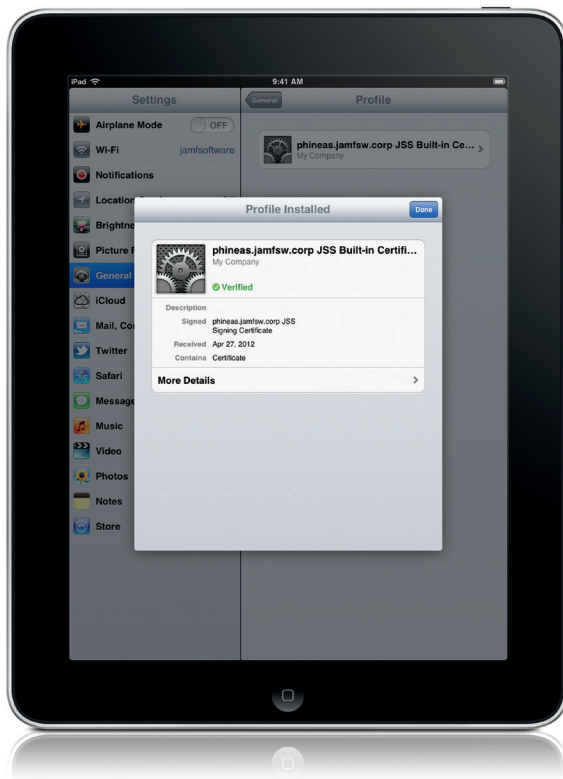
- Users must tap **Install** to continue.



- When notified that the profile will change settings on the device, users must tap **Install** again.



- If the device has a passcode set, users must enter their passcode.
- Users must tap **Done** to move on to the next step.



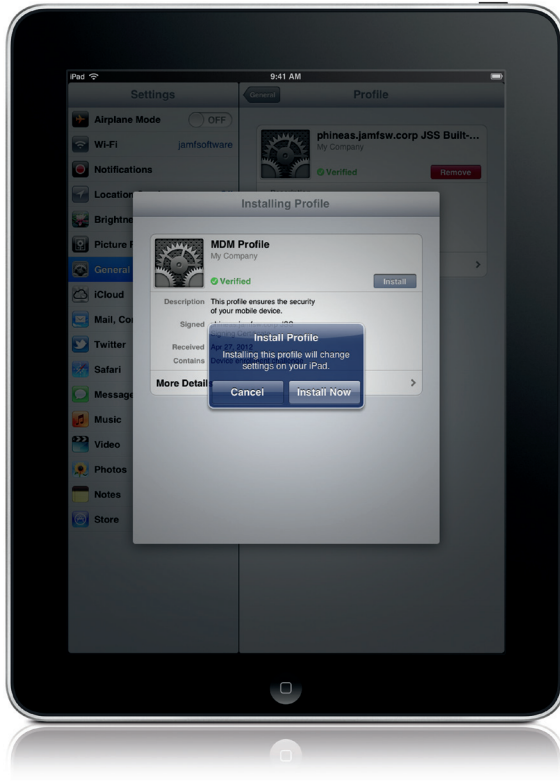
8. Users must tap **Install Profile** to initiate the installation of the MDM profile.



9. Users must tap **Install** to continue.



10. If the device has a passcode set, users must enter their passcode.
11. When notified that installing the profile will change settings on the device, users must tap **Install Now**.



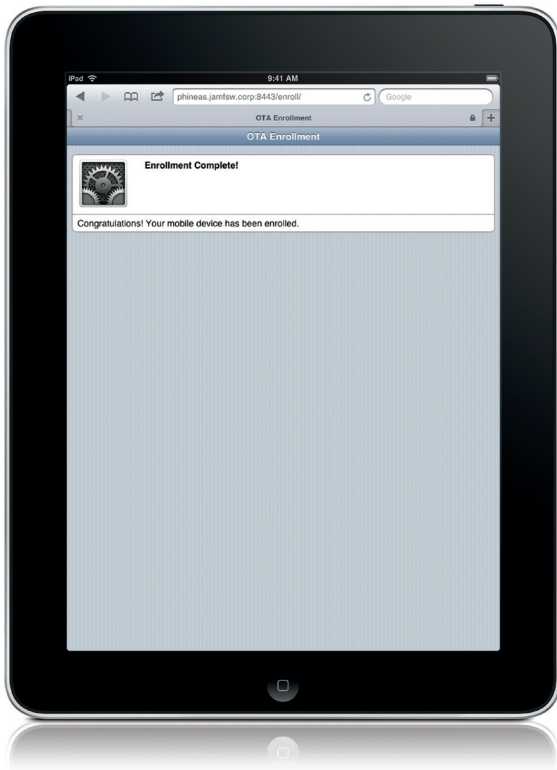
12. When notified that installing the profile will allow an administrator to remotely manage the device, users must tap **Install**.



13. Users must tap **Done** to complete the enrollment process.



When a user completes the enrollment process, the device is enrolled with the JSS.





# Enrolling Connected Mobile Devices

The alternative to OTA enrollment is to enroll devices that are connected to a computer by USB. The JSS allows you to create enrollment profiles (.mobileconfig) that you can download and install on connected devices using Apple's iPhone Configuration Utility (iPCU) or Apple Configurator.

**Important:** Updated MDM profiles cannot be distributed to devices that are enrolled using this method.

Enrolling connected mobile devices requires mobile devices with access to a wireless network connection.

This section explains how to create, download, edit, and delete enrollment profiles in the JSS.

For instructions on installing enrollment profiles on devices using iPCU or Apple Configurator, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=211>

## Creating Enrollment Profiles

Use the JSS to create an enrollment profile that you can install on connected devices using iPCU or Apple Configurator.

To create an enrollment profile:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link.
4. Click the **Create Enrollment Profile** button.
5. Enter a display name for the profile.

This is displayed in iPCU and Apple Configurator and is also the filename of the profile.

**Edit Mobile Device Enrollment Profile**

General Location Information Purchasing Information

### Mobile Device Enrollment Profile

Enter a display name and a description for the Profile. These will be displayed on the device when it is installed.

Display Name:

Target iOS:

Notify JSS when profile is removed ⓘ

Description:

Cancel Save

- Choose a target iOS from the **Target iOS** pop-up menu.  
The target iOS must match the iOS on the device(s) that you plan to enroll.
- If you want the JSS to display a removal notification on the Mobile Device Details pane for the device(s) when the profile is removed, leave the **Notify JSS when profile is removed** checkbox selected.

**Important:** If you plan to use Apple Configurator to install the enrollment profile, you must deselect the **Notify JSS when profile is removed** checkbox.

- Enter a description for the profile.  
This is displayed in iPCU and Apple Configurator.
- To populate location information for the device(s) that you plan to enroll, click the **Location Information** tab and enter information as needed.

The screenshot shows the 'Edit Mobile Device Enrollment Profile' dialog box with the 'Location Information' tab selected. The title is 'Mobile Device Enrollment Profile - Default Location Information'. Below the title is a note: 'Information filled out here will be assigned as default location information for any device enrolled with this profile.' The form contains the following fields:

- Username: [text input]
- Real Name: [text input]
- Email Address: [text input]
- Position: [text input]
- Phone: [text input]
- Department: [dropdown menu, currently 'No Department']
- Building: [dropdown menu, currently 'No Building']
- Room: [text input]

At the bottom right are 'Cancel' and 'Save' buttons.

- To populate purchasing information for the device(s) that you plan to enroll, click the **Purchasing Information** tab and enter information as needed.  
You can also upload attachments that will be assigned to the device(s).

The screenshot shows the 'Edit Mobile Device Enrollment Profile' dialog box with the 'Purchasing Information' tab selected. The title is 'Mobile Device Enrollment Profile - Default Purchasing Information'. Below the title is a note: 'Information filled out here will be assigned as default purchasing information for any device enrolled with this profile.' The form contains the following fields:

- Purchased  Leased
- PO Number: [text input]
- Vendor: [text input]
- AppleCare ID: [text input]
- Purchase Price: [text input]
- Purchasing Account: [text input]
- PO Date: [dropdown] / [dropdown] / [dropdown]
- Warranty Expires: [dropdown] / [dropdown] / [dropdown]
- Lease Expires: [dropdown] / [dropdown] / [dropdown]
- Life Expectancy: [dropdown, currently 'N/A']
- Purchasing Contact: [text input]

Below the fields is an 'Attachment' section with a table containing 'No Attachments' and an 'Attach File...' link. At the bottom right are 'Cancel' and 'Save' buttons.

- Click **Save**.

## Downloading Enrollment Profiles

Before you can install an enrollment profile with iPCU or Apple Configurator, you must download the profile from the JSS.

**To download an enrollment profile:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link.
4. Click the **Download** link across from the profile.

If you are working on OS X v10.7 or later, you may be prompted to install the profile on your computer. Click **Cancel** to decline.

The profile is saved as a .mobileconfig file.

## Editing Enrollment Profiles

**To edit an existing enrollment profile:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link.
4. Click the **Enrollment Profiles** tab.
5. Click the **Edit** link across from the profile, and make changes as needed.
6. Click **Save**.

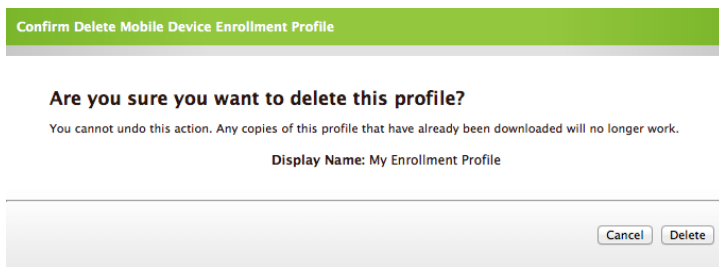
## Deleting Enrollment Profiles

Once you delete an enrollment profile, the profile becomes invalid. If you have already downloaded the profile, you can no longer use it to enroll devices. Devices that have already installed the profile are affected.

**To delete an enrollment profile:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Enrollment** link.
4. Click the **Enrollment Profiles** tab.

5. Click the **Delete** link across from the profile, and then click the **Delete** button to confirm.




# Unenrolling Mobile Devices

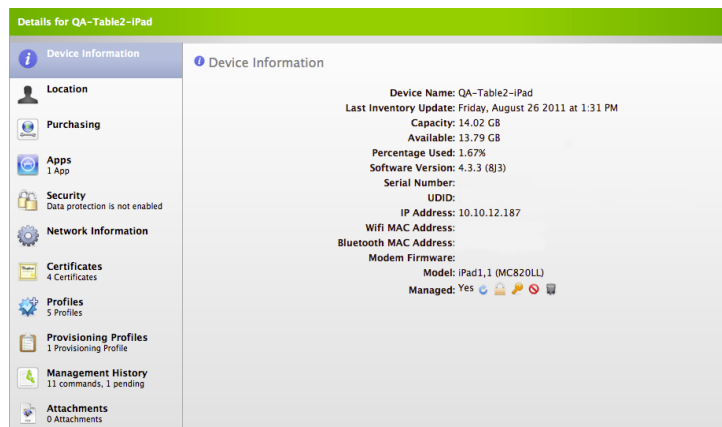
Unenrolling a mobile device stops communication between the device and the JSS, and you can no longer perform over-the-air management tasks on a device after it is unenrolled. Although an unenrolled device can no longer submit inventory, its inventory record remains in the JSS.

When you use the JSS to unenroll a device, the following components are removed from the device:

- The MDM profile
- The device certificate
- The Self Service web clip
- Configuration profiles that were distributed with the Casper Suite
- Managed apps that were distributed with the **Remove apps when MDM profile is removed** checkbox selected

## To unenroll a mobile device:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab, and perform a simple mobile device search for the device that you want to unenroll.
3. Click the **Details** link across from the device.
4. Click the  icon on the Device Information pane.



5. Click **OK** to confirm.

# Inventory

## Searching Mobile Devices

Once mobile devices are acquired or enrolled with the JAMF Software Server (JSS), they can be viewed for inventory and reporting purposes.

This section explains how to:

- Perform simple and advanced mobile device searches
- View mobile device details

### Performing Simple Mobile Device Searches

A simple mobile device search functions like a search engine, allowing you to locate a general range of results quickly and easily.

Simple searches can be performed based on the following mobile device attributes:

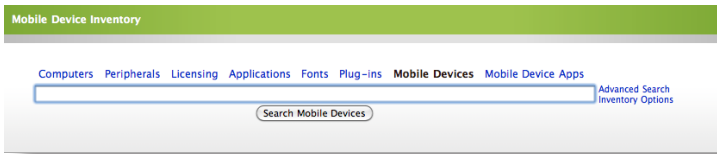
- UDID
- Display name
- Device name
- GUID
- ICCID
- IMEI
- Phone number
- Serial number
- Username
- Real name
- Email address
- Position
- Department
- Building
- Room

**Note:** Performing an empty search (with no criteria in the search field) returns all mobile devices in your database.

**To perform a simple mobile device search:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.

3. Click the **Mobile Devices** link above the search field.



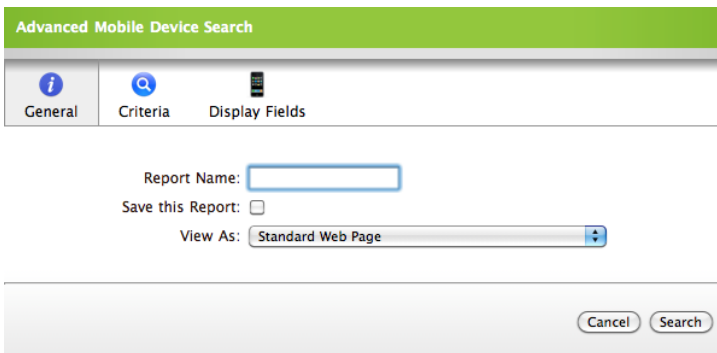
4. Enter one or more terms into the search field.
5. Click **Search Mobile Devices**, or press the Enter key.

## Performing Advanced Mobile Device Searches

When used to search for devices and create reports, advanced mobile device searches offer you a variety of powerful options. The advanced search interface consists of three navigation panes: General, Criteria, and Display Fields.

A description of the information on each pane follows:

### General Pane



This pane allows you to choose a reporting format and save the report so that you can access it in the future.

Saved mobile device searches can be accessed on the Mobile Devices Inventory pane. You can edit or delete a saved search by clicking the disclosure triangle next to the search, and then clicking the **Edit** or **Delete** link.

## Criteria Pane

Field	Search Type	Criteria	-	+
		<b>General Information</b>		+
		<b>Mobile Device Details</b>		+
		<b>Location</b>		+
		<b>Purchasing</b>		+
		<b>Apps</b>		+
		<b>Security</b>		+
		<b>Network</b>		+
		<b>Certificates</b>		+
		<b>Configuration Profiles</b>		+
		<b>Provisioning Profiles</b>		+

This pane allows you to specify the attributes on which to base your search. These options are broken down into the following categories:

- General Information
- Mobile Device Details
- Location
- Purchasing
- Apps
- Security
- Network
- Certificates
- Configuration Profiles
- Provisioning Profiles



## Display Fields Pane

Advanced Mobile Device Search

General Criteria Display Fields

<input type="checkbox"/> Info Link	<input type="checkbox"/> Mobile Device Display Name	<input type="checkbox"/> Mobile Device Serial Number	<input type="checkbox"/> UDID
<input type="checkbox"/> Wifi MAC Address	<input type="checkbox"/> Bluetooth MAC Address	<input type="checkbox"/> Managed	<input type="checkbox"/> IP Address
<input type="checkbox"/> Device Name	<input type="checkbox"/> Capacity	<input type="checkbox"/> Available	<input type="checkbox"/> Percentage
<input type="checkbox"/> Phone Number	<input type="checkbox"/> Mobile Device Model	<input type="checkbox"/> OS Version	<input type="checkbox"/> OS Build
<input type="checkbox"/> Battery Level	<input type="checkbox"/> Modem Firmware	<input type="checkbox"/> Last Backup Time	<input type="checkbox"/> Last Inventory Update
<input type="checkbox"/> Username	<input type="checkbox"/> Real Name	<input type="checkbox"/> Email Address	<input type="checkbox"/> Department
<input type="checkbox"/> Building	<input type="checkbox"/> Room	<input type="checkbox"/> Phone	<input type="checkbox"/> Position
<input type="checkbox"/> Purchased/Leased	<input type="checkbox"/> PO Number	<input type="checkbox"/> PO Date	<input type="checkbox"/> Vendor
<input type="checkbox"/> Warranty Expires	<input type="checkbox"/> Lease Expires	<input type="checkbox"/> AppleCare ID	<input type="checkbox"/> Purchase Price
<input type="checkbox"/> Life Expectancy	<input type="checkbox"/> Purchasing Account	<input type="checkbox"/> Purchasing Contact	
<input type="checkbox"/> Data Protection	<input type="checkbox"/> Hardware Encryption	<input type="checkbox"/> Passcode Present	<input type="checkbox"/> Block-Level Encryption
<input type="checkbox"/> File-Level Encryption	<input checked="" type="checkbox"/> Passcode Compliant	<input type="checkbox"/> Passcode Compliant with Profile	

Cancel Search

This pane allows you to specify the attributes that are displayed in your search results when viewing them in one of the following formats:

- Standard Webpage
- CSV
- Tab
- XML

You can change the default selections on this pane by changing the Inventory Display preferences. For more information, see the “Inventory Display Preferences” section.

### To perform an advanced mobile device search:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Mobile Devices** link.
4. Click the **Advanced Search** link.
5. If you want to save the search, enter a name for the report and select **Save this Report**.

Advanced Mobile Device Search

General Criteria Display Fields

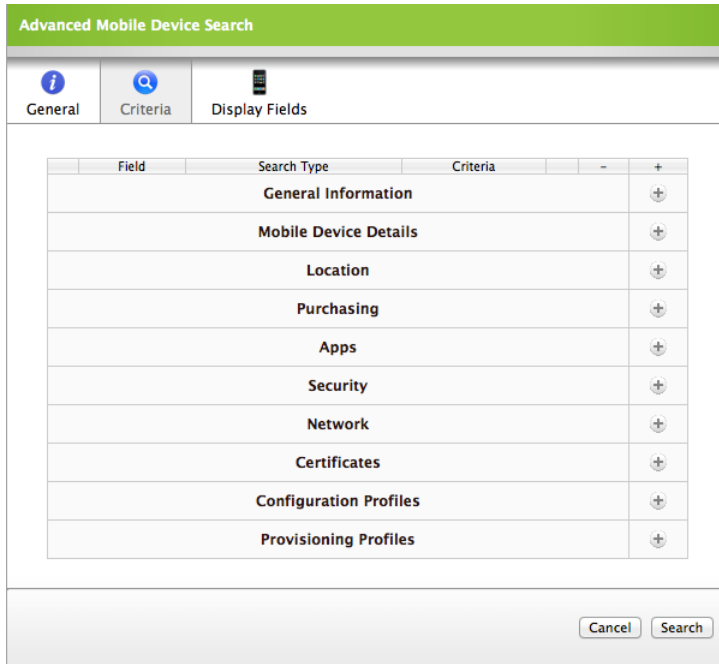
Report Name:

Save this Report:

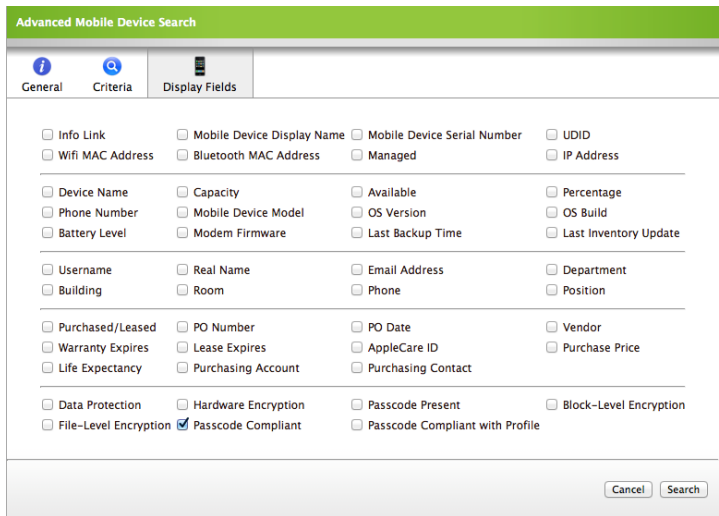
View As: Standard Web Page

Cancel Search

6. Choose a format for the report from the **View As** pop-up menu.
7. Click the **Criteria** tab.
8. Click **Add (+)** next to the category you want to use to define your search.  
A list of searchable items is displayed.



9. Click the item that you want to use in your search.
10. Specify search criteria for the item.
11. Click the **Display Fields** tab and select the attributes you want to display in the search results.



12. Click the **Search** button.

## Viewing Mobile Device Search Results

By default, mobile device search results are displayed in Standard Webpage format. You can view the search results in any of the following alternate formats:

- CSV
- Tab
- XML

For simple mobile device searches, choose one of these options from the **View Results As** pop-up menu at the bottom of the results list. For advanced mobile device searches, choose one of these options from the **View As** pop-up menu on the General pane of the advanced search interface.

**Note:** The attributes displayed in simple mobile device search results are determined by your Inventory Display preferences. See the “Managing Inventory Attributes” section for more information. The attributes displayed in advanced mobile device search results are determined by the settings on the Display Fields pane of the advanced search interface. For more information, see “Performing Advanced Mobile Device Searches”.

### CSV

This format exports your search results into a CSV file that you can open in Microsoft Excel and other spreadsheet applications.

### Tab

This format exports your search results into a tab-delimited text file that you can open in Microsoft Excel and other spreadsheet applications.

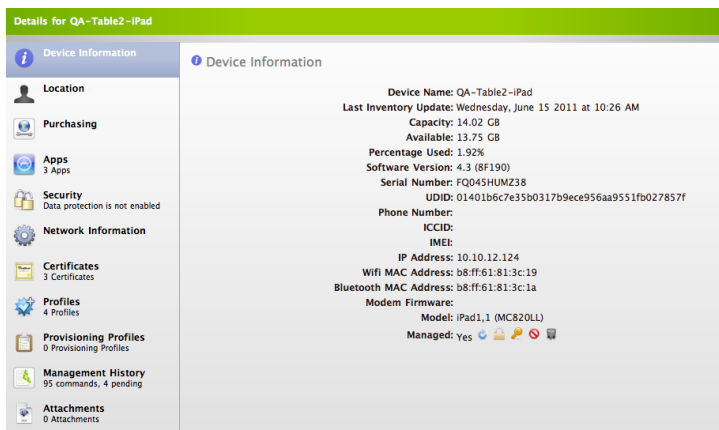
### XML

This format exports your search results into an XML file. XML files are commonly used to move data between applications.

## Viewing Mobile Device Details

After performing a mobile device search, you can view a Details report for any search result by clicking the **Details** link across from it.

Details reports are broken down by category. Clicking a category in the sidebar displays related information in the category pane. Some panes allow you to edit information, view history, and add components.



The following table describes each category pane and the actions that you can perform from it:

Category	Description	Actions that you can perform
<b>Device Information</b>	General information about the device, including device name, date/time of last inventory report, UDID, IP address, and enrollment status	Update inventory Run a remote command (remote lock, remote clear passcode, and remote wipe) Unenroll the device
<b>Location</b>	Information about the device's physical location on the network	Edit location information Perform LDAP lookup (See "Integrating with LDAP Servers" for information on setting up an LDAP server connection.)
<b>Purchasing</b>	Purchasing information for the device, including PO details, warranty information, and purchasing contact	Edit purchasing information Perform GSX lookup (See "Integrating with GSX" for information on setting up a GSX connection.)
<b>Apps</b>	A list of installed apps, and their version number and management status	--
<b>Security</b>	Security components enabled on the device, including data protection, hardware encryption, and passcode information	--
<b>Network Information</b>	Information about the network, including carrier, network and country codes, cellular technologies, carrier-specific information, and roaming status	--
<b>Certificates</b>	A list of certificates installed on the device	--

Category	Description	Actions that you can perform
<b>Profiles</b>	A list of profiles installed on the device, including version number and bundle identifier	--
<b>Provisioning Profiles</b>	A list of provisioning profiles installed on the device, including expiration date	--
<b>Management History</b>	A list of management commands run on the device	Update management history Cancel a remote command that is pending
<b>Attachments</b>	A list of files attached to the device's inventory record	Upload attachments

# Searching Mobile Device Apps

You can search and report on the apps installed on devices, regardless of their enrollment status.

The instructions in this section explain how to:

- Perform simple app searches
- Perform advanced app searches
- View app search results
- View app distribution

## Performing Simple App Searches

A simple app search functions like a search engine, allowing you to locate a general range of results quickly and easily.

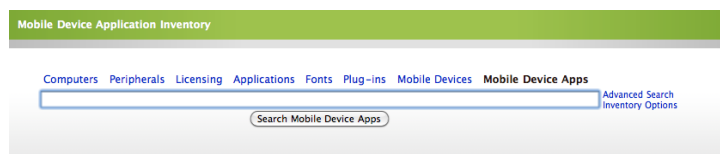
Simple searches can be based on the following attributes:

- App Name
- Version Number

**Note:** Blank searches cannot be performed for apps. You must enter criteria in the search field.

**To perform a simple app search:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Mobile Device Apps** link.



4. Type one or more terms into the search field.
5. Click **Search Mobile Device Apps**, or press the Enter key.

## Performing Advanced App Searches

When used to search for apps and create reports, advanced app searches offer you a variety of powerful options. The advanced search interface consists of three navigation panes: General, Criteria, and Display Fields.

A description of the information on each pane follows:

## General Pane

The screenshot shows the 'General' pane of the 'Advanced Mobile Device Application Search' interface. It features a green header bar with the title. Below the header is a navigation bar with three tabs: 'General' (selected), 'Criteria', and 'Display Fields'. The main content area contains a 'Report Name' text input field, a 'Save this Report' checkbox, and a 'View As' dropdown menu currently set to 'Standard Web Page'. At the bottom right, there are 'Cancel' and 'Search' buttons.

This pane allows you to choose a reporting format and save the report so that you can perform it at a later date.

Saved app searches can be accessed on the Mobile Device Apps Inventory pane. You can edit or delete a saved search by clicking the disclosure triangle next to the search and clicking the **Edit** or **Delete** link.

## Criteria Pane

The screenshot shows the 'Criteria' pane of the 'Advanced Mobile Device Application Search' interface. It features a green header bar with the title. Below the header is a navigation bar with three tabs: 'General', 'Criteria' (selected), and 'Display Fields'. The main content area contains two search criteria: 'Application Name' and 'Application Version'. Each criterion has a dropdown menu set to 'like' and an adjacent text input field. At the bottom right, there are 'Cancel' and 'Search' buttons.

This pane allows you to define the following criteria on which to base your search:

- Application Name
- Application Version

## Display Fields Pane

The screenshot shows the 'Display Fields' pane of the 'Advanced Mobile Device Application Search JSS Mobile' application. The pane has a green header with the title. Below the header are three tabs: 'General' (with an information icon), 'Criteria' (with a magnifying glass icon), and 'Display Fields' (with a document icon). The 'Display Fields' tab is active. Below the tabs, there are two checkboxes: 'Application Name' and 'Application Version', both of which are currently unchecked. At the bottom right of the pane are two buttons: 'Cancel' and 'Search'.

This pane allows you to specify the attributes displayed in your search results when you view your search in one of the following reporting formats:

- Standard Webpage
- CSV
- Tab
- XML

### To perform an advanced app search:

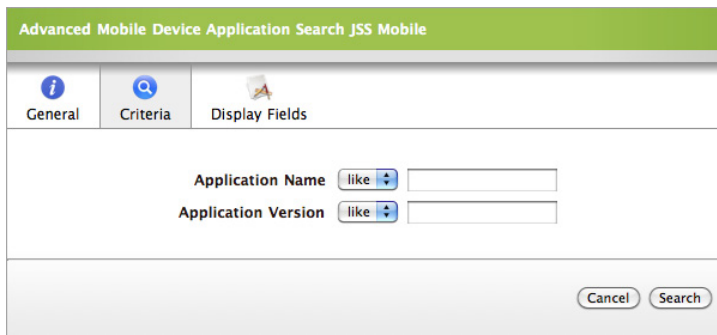
1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Click the **Mobile Device Apps** link.
4. Click the **Advanced Search** link.
5. If you want to save your search, enter a name for the report and select **Save this Report**.

The screenshot shows the 'Advanced Mobile Device Application Search JSS Mobile' application with the 'Display Fields' pane. The 'Report Name' field is now populated with a text input box. Below it, the 'Save this Report' checkbox is checked. The 'View As' dropdown menu is set to 'Standard Web Page'. At the bottom right of the pane are two buttons: 'Cancel' and 'Search'.

6. Choose the format you want to view the report in.



7. Click the **Criteria** tab and define criteria for the search.



Advanced Mobile Device Application Search JSS Mobile

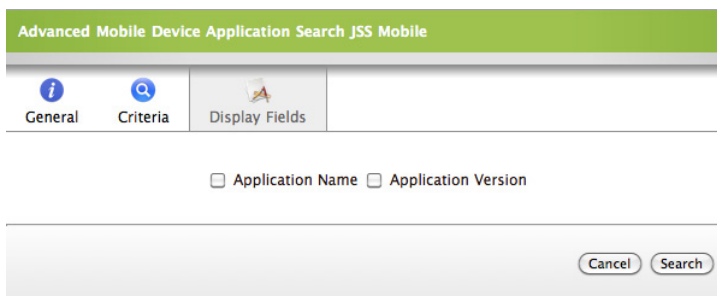
General Criteria Display Fields

Application Name like

Application Version like

Cancel Search

8. Click the **Display Fields** tab and select the attributes you want to display in your results.



Advanced Mobile Device Application Search JSS Mobile

General Criteria Display Fields

Application Name  Application Version

Cancel Search

9. Click **Search**.

## Viewing App Search Results

By default, app search results are displayed in Standard Webpage format. You can view the search results for advanced app searches in any of the following alternate formats by choosing from the **View As** pop-up menu on the General pane of the advanced search interface:

- CSV
- Tab
- XML

**Note:** The attributes displayed in advanced app search results are determined by the settings on the Display Fields pane of the advanced search interface. For more information, see “Performing Advanced App Searches”.

### CSV

This format exports your search results into a CSV file that you can open in Microsoft Excel and other spreadsheet applications.

## Tab

This format exports your search results into a tab-delimited text file that you can open in Microsoft Excel and other spreadsheet applications.

## XML

This format exports your search results into an XML file. XML files are commonly used to move data between applications.

## Viewing App Distribution

After performing an app search, you can view a list of devices that have the app installed by clicking the **View Distribution** link across from it.

# Performing Mass Actions on Mobile Device Search Results

Mass actions are a quick way to perform the following tasks on the results of a mobile device search:

- Look up purchasing information from Apple’s Global Service Exchange (GSX).
- Email users.
- Delete from the JAMF Software Server (JSS).

## Mass Look up Purchasing Information from GSX

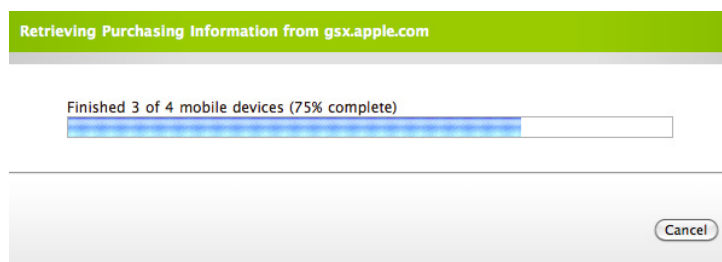
This allows you to look up and populate purchasing information from Apple’s Global Service Exchange (GSX).

To utilize this feature, a GSX connection must be set up in the JSS. For more information on setting up this connection, see “Integrating with GSX.”

**Note:** GSX lookups may not always return complete purchasing information. The lookup only returns information available in GSX.

### To perform a mass GSX lookup:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced mobile device search.
4. Choose “Look up Purchasing Info in GSX” from the **Take Action on Results** pop-up menu. Then, click **Go**. The progress of the lookup is displayed.



5. When the results are displayed, click the **Update Records** button to populate the information in the JSS. Then, click **Continue** to confirm.  
If the information is already up-to-date, click the **Cancel** button.

## Mass Emailing Users

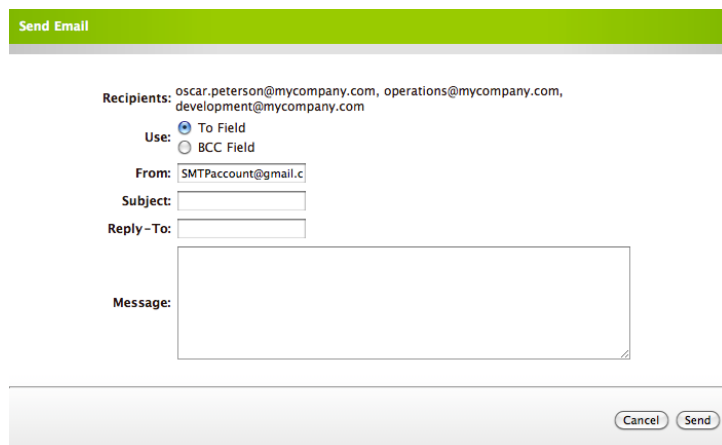
Mass emails are a convenient way to notify users of an upcoming update or another issue.

Mass emails are sent from the SMTP server that is specified in the JSS. If you have not specified an SMTP server, see "Enabling Email Notifications" for instructions on how to do so.

### To mass email users:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced mobile device search.
4. Choose "Send Email" from the **Take Action on Results** pop-up menu. Then, click **Go**.
5. Use the options and fields provided to compose the email message.

The email address you send the message from must be associated with the SMTP server in the JSS. Replies are also sent to this address unless you specify otherwise.



6. Click the **Send** button.
7. Click **Continue** to confirm.

## Mass Deleting Mobile Devices

You can remove mobile devices from your inventory by deleting them from the JSS.

**Important:** Deleting mobile devices from the JSS does not unenroll them. For instructions on unenrolling a device, see the "Unenrolling Mobile Devices" section in "Enrolling Mobile Devices with the JSS".

### To mass delete mobile devices from the JSS:

1. Log in to the JSS with a web browser.

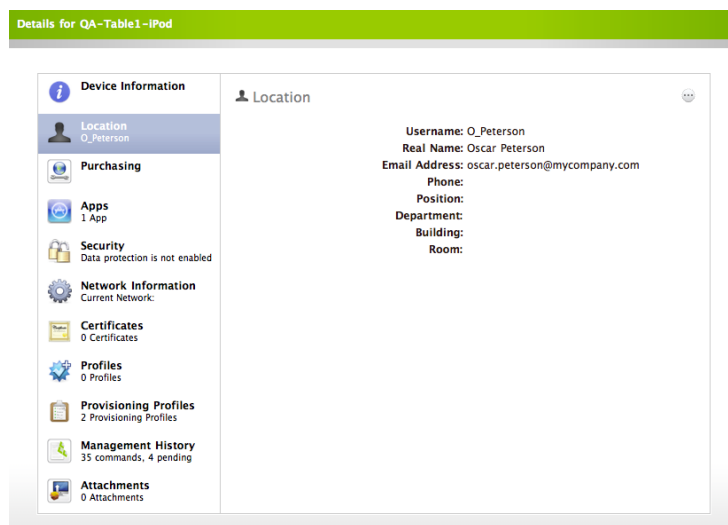
2. Click the **Inventory** tab.
3. Perform a simple or advanced mobile device search.
4. Choose "Delete Mobile Devices" from the **Take Action on Results** pop-up menu. Then, click **Go**.
5. Click the **Delete Mobile Devices** button.
6. Click **Continue** to confirm the deletion.


# Editing Mobile Device Records

You use the JAMF Software Server (JSS) to edit location and purchasing information for a mobile device and attach files to the mobile device record.

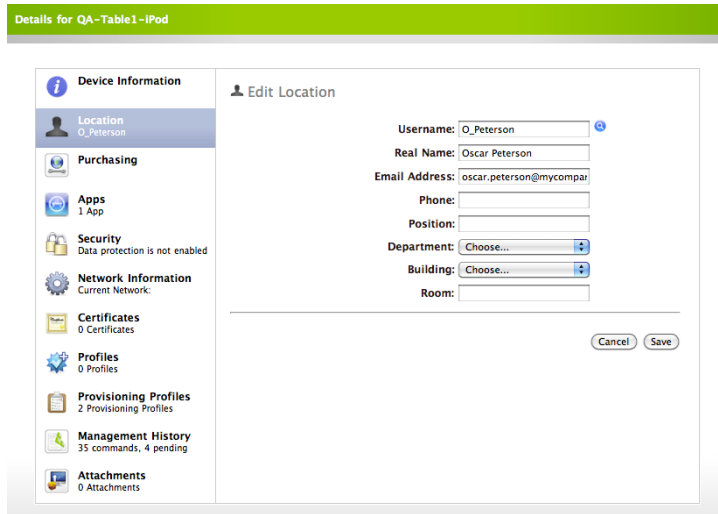
## To edit location or purchasing information for a mobile device record:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced mobile device search.
4. Click **Details** across from the device record you want to edit.
5. Click **Location** or **Purchasing** in the categories list.
6. Click the **Ellipsis** button to display the editable fields.



7. Add or modify information as needed, or click the **Search**  icon to perform an LDAP or GSX lookup. Performing a lookup populates the fields with information from an LDAP server or Apple's Global Service Exchange (GSX).

**Note:** The lookup feature is only available if an LDAP server and/or GSX connection is set up in the JSS. For more information on setting up these connections, see the "Integrating with LDAP Servers" and "Integrating with GSX" sections.



Details for QA-Table1-iPod

**Device Information**

- Location: O\_Peterson
- Purchasing
- Apps: 1 App
- Security: Data protection is not enabled
- Network Information: Current Network
- Certificates: 0 Certificates
- Profiles: 0 Profiles
- Provisioning Profiles: 2 Provisioning Profiles
- Management History: 35 commands, 4 pending
- Attachments: 0 Attachments

**Edit Location**

Username:

Real Name:

Email Address:

Phone:

Position:

Department:

Building:

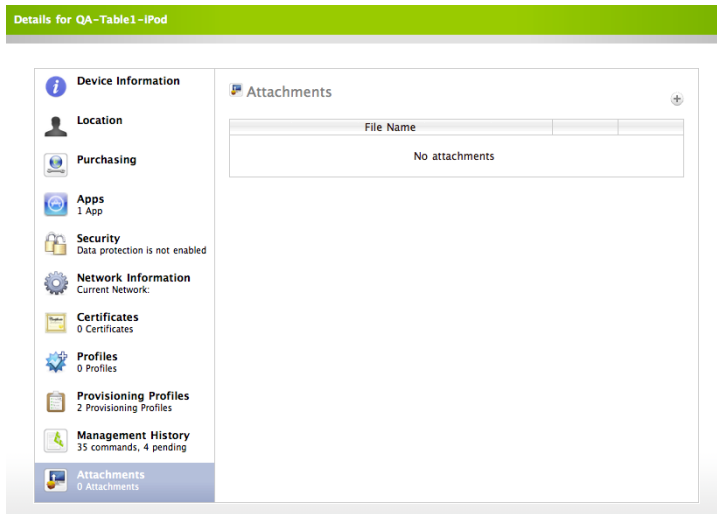
Room:

8. Click **Save**.

**To attach a file to a mobile device record:**

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced mobile device search.
4. Click **Details** across from the device record.
5. Click **Attachments** in the categories list.

6. Click the **Add**  icon.



7. Click the **Choose File** button and upload a file.
8. Click the **Save Attachment** button.



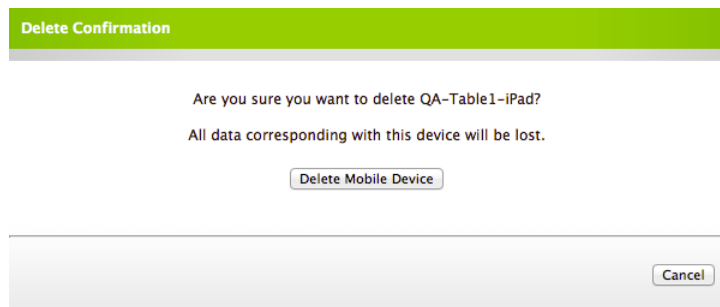
# Deleting Mobile Devices from the JSS

You can remove a mobile device from your inventory by deleting it from the JAMF Software Server (JSS).

**Important:** Deleting a mobile device from the JSS does not unenroll it. For instructions on unenrolling a device, see the "Unenrolling Mobile Devices" section in "Enrolling Mobile Devices with the JSS".

## To delete a mobile device from the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple or advanced mobile device search.
4. Click **Delete** across from the device record, and then click the **Delete Mobile Device** button to confirm.



# Creating Mobile Device Groups

Mobile device groups provide an easy way to identify and manage devices that share common attributes or meet custom criteria. You can use these groups to assign devices to a profile or app's scope, and track mobile devices for reporting purposes.

The JAMF Software Server (JSS) allows you to create two kinds of mobile device groups: smart mobile device groups and static mobile device groups. Smart mobile device groups are based on inventory attributes and have dynamic group membership. This means that group membership changes automatically anytime a change in criteria or device inventory occurs. Conversely, static mobile device groups are hardcoded and have fixed memberships that can only be changed by an administrator.

Only enrolled devices can be members of a mobile device group.

This section explains how to create two kinds of mobile device groups:

- A smart mobile device group
- A static mobile device group

## To create a smart mobile device group:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Smart Mobile Device Groups** link.
4. Click the **Create Smart Group** button in the toolbar.
5. Enter a name for the smart group.

**Edit Smart Mobile Device Group:**

Mobile Device Group Name:

Send Email Notification on Change:

Field	Search Type	Criteria	-	+
General Information			-	+
Mobile Device Details			-	+
Location			-	+
Purchasing			-	+
Apps			-	+
Security			-	+
Network			-	+
Certificates			-	+
Configuration Profiles			-	+
Provisioning Profiles			-	+

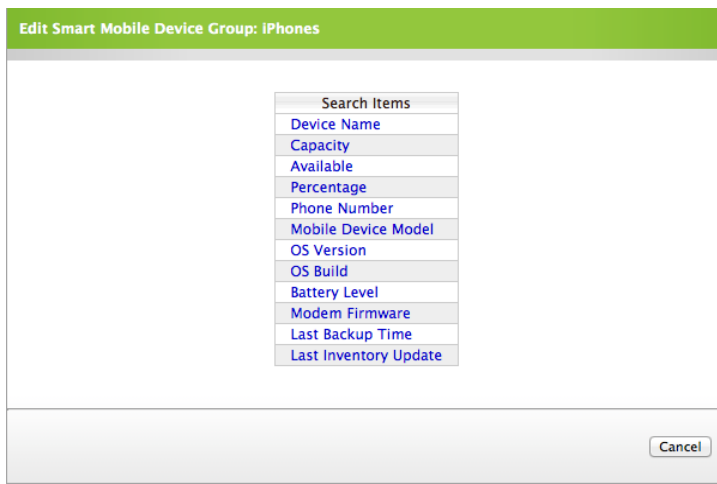
Cancel Save

- To send an email notification when membership changes occur, select the **Send Email Notification on Change** option.

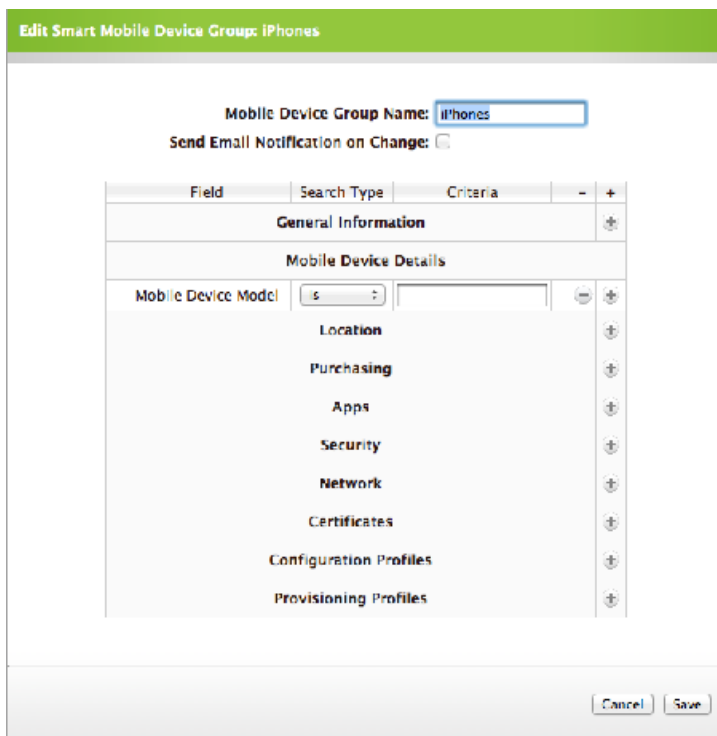
The JSS sends email notifications to the email addresses for accounts that have smart mobile device group email privileges enabled.

**Note:** An SMTP server must be set up in the JSS to send email notifications. For information on how to set up an SMTP server, see the “Enabling Email Notifications” section.

- Click **Add (+)** next to the category that you want to base the group on.
- Click the item that you want to base the group on.



- Specify criteria for the group.



10. Repeat steps 7 through 9 as needed.
11. Click **Save**.

**To create a static mobile device group:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Static Mobile Device Groups** link.
4. Click the **Create Static Group** button in the toolbar.
5. Enter a name for the static mobile device group.

**Edit Static MobileDevice Group:**

Mobile Device Group Name

Mobile Device Name	User	Department	Building	
QA-Table3-iPod				<input type="checkbox"/>
QA-Table2-iPhone				<input type="checkbox"/>

Cancel Save

6. Select the devices you want to include in the group.
7. Click **Save**.

# Configuration

## Creating and Distributing iOS Configuration Profiles

iOS configuration profiles are XML files (.mobileconfig) that define groups of settings for enrolled mobile devices. The JAMF Software Server (JSS) allows you to create configuration profiles using an interface similar to Apple's iPhone Configuration Utility (iPCU) and Profile Manager.

When you are done creating the profile, you can distribute it wirelessly by choosing a distribution method and assigning devices to the scope.

**Note:** Some payloads and settings available in iPCU and Profile Manager cannot be configured with the JSS.

Before creating a configuration profile, you should have basic knowledge of configuration profile payloads and settings and how they affect devices. Most payloads and settings are explained in Apple's iPCU documentation, available at:

<https://help.apple.com/iosdeployment-ipcu/#>

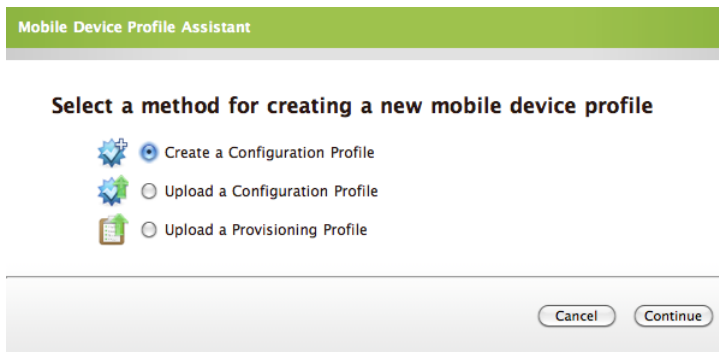
Some configuration profile settings can only be configured using the JSS. For more information on these settings, see the following Knowledge Base article:

<https://jamfnation.jamfsoftware.com/article.html?id=217>

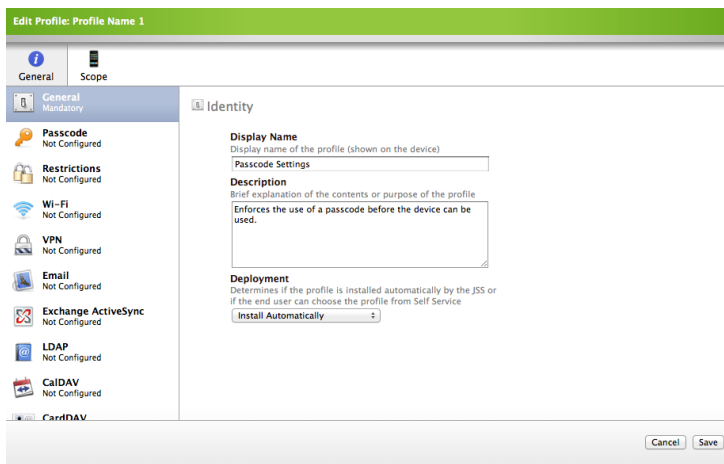
**To create and distribute an iOS configuration profile using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Add Profile** button.

5. Select **Create a Configuration Profile**, and then click **Continue**.

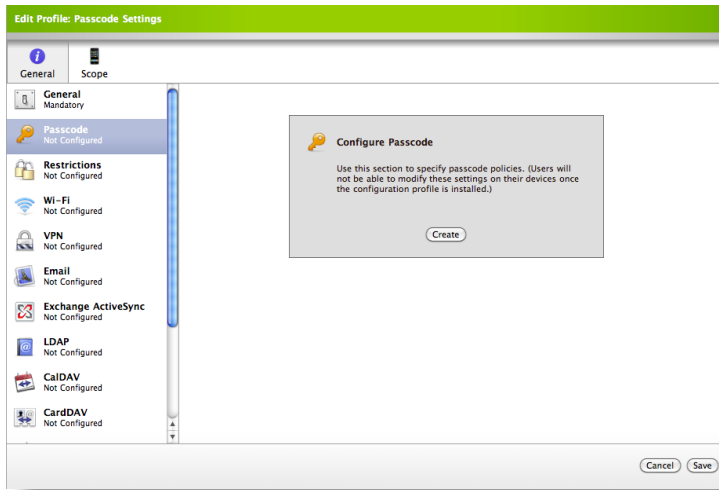


6. Enter a display name and description for the profile.
7. Choose a distribution method from the **Deployment** pop-up menu:
  - To install the profile automatically, choose "Install Automatically".
  - To distribute the profile in the Self Service web clip, choose "Make Available in Self Service Web Clip".

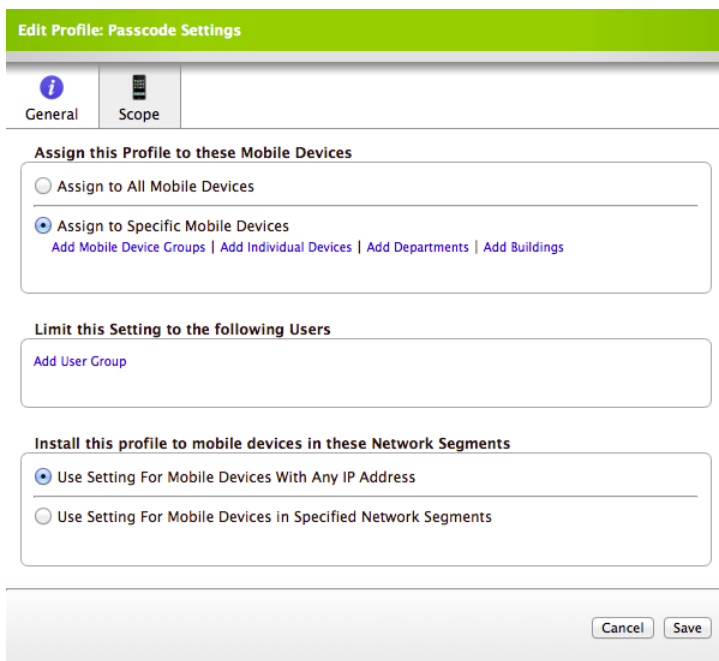


8. If you chose to distribute the profile in the Self Service web clip, upload an icon to display and choose a security setting from the **Security** pop-up menu.

9. In the payloads list, select the payload that you want to add, and then click **Create**.



10. Use the options and fields in the main pane to configure settings for the payload. There are several variables that you can use to dynamically customize a payload. For more information, see the "Variables for iOS Configuration Profiles" section.
11. To add additional payloads, repeat steps 9 and 10.
12. Click the **Scope** tab and assign devices to the scope.



13. Click **Save**.

The next time devices in the scope contact the JSS, they receive the profile based on the distribution method you chose.

## Variables for iOS Configuration Profiles

There are several variables that you can use to dynamically customize the payloads in an iOS configuration profile.

Enter a variable into any text field in a payload to dynamically populate information about the devices to which you are distributing the profile. When the profile is installed, the variable is translated to the actual value stored in the JSS.

Variable	Mobile Device Information
\$UDID	UDID
\$SERIALNUMBER	Serial number
\$USERNAME	Username
\$REALNAME	Real name
\$EMAIL	Email address
\$PHONE	Phone
\$ROOM	Room
\$POSITION	Position



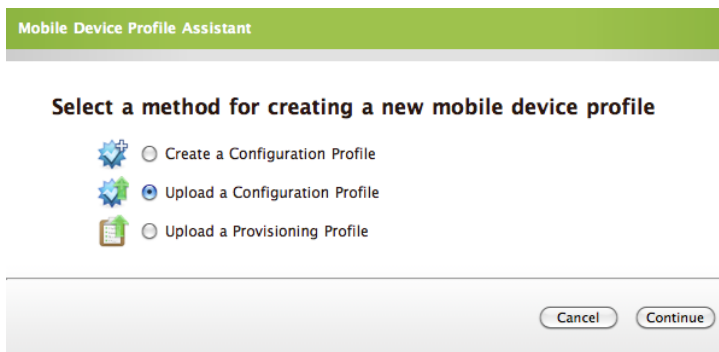
# Distributing iOS Configuration Profiles Created with Apple's Tools

To distribute an iOS configuration profile created with Apple's iPhone Configuration Utility (iPCU) or Profile Manager, you must first upload the profile to the JAMF Software Server (JSS). Then, you can choose a distribution method and assign devices to the scope.

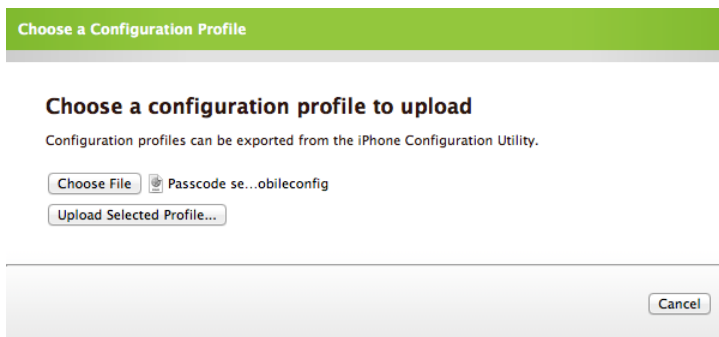
**Note:** Some payloads and settings configured with iPCU and Profile Manager are not displayed in the JSS. Although you cannot view or edit these payloads, they are applied to devices when the profile is installed.

To distribute an iOS configuration profile created with Apple's tools:

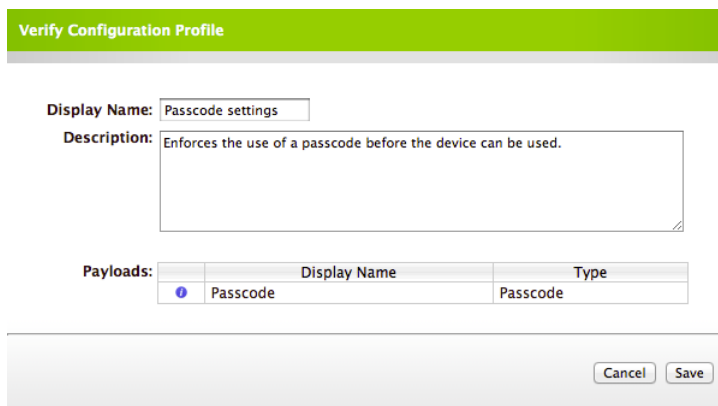
1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Add Profile** button.
5. Select **Upload a Configuration Profile**, and then click **Continue**.



6. Click **Choose File** and select the profile (.mobileconfig) that you want to upload. Then, click **Upload Selected File**.



7. Verify the display name for the profile and enter a description if desired. Then, click **Save**.

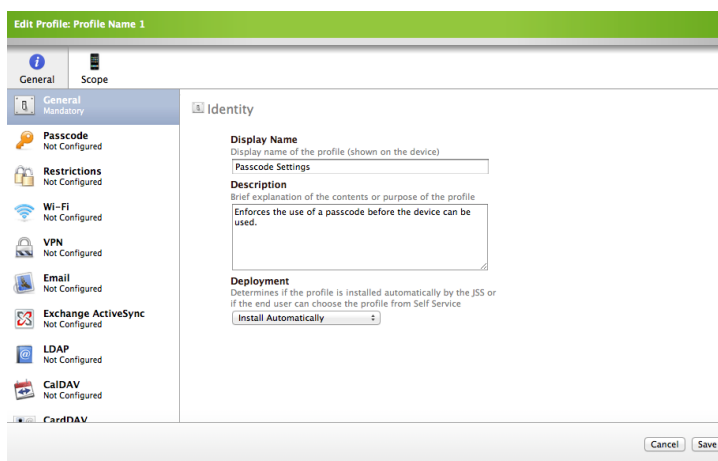


The dialog box titled "Verify Configuration Profile" has a green header. It contains a "Display Name" field with the text "Passcode settings". Below it is a "Description" text area containing the text "Enforces the use of a passcode before the device can be used.". At the bottom, there is a "Payloads:" section with a table:

	Display Name	Type
	Passcode	Passcode

At the bottom right of the dialog are "Cancel" and "Save" buttons.

8. Click the **Edit** link across from the profile that you uploaded.
9. Choose a distribution method from the **Deployment** pop-up menu:
  - To install the profile automatically, choose "Install Automatically".
  - To distribute the profile in the Self Service web clip, choose "Make Available in Self Service Web Clip".



The dialog box titled "Edit Profile: Profile Name 1" has a green header. It features a left sidebar with a "General" tab selected, showing a list of settings: Passcode (Not Configured), Restrictions (Not Configured), Wi-Fi (Not Configured), VPN (Not Configured), Email (Not Configured), Exchange ActiveSync (Not Configured), LDAP (Not Configured), CalDAV (Not Configured), and CardDAV. The main area is titled "Identity" and contains:

- Display Name:** "Passcode Settings" (shown on the device)
- Description:** "Enforces the use of a passcode before the device can be used."
- Deployment:** A dropdown menu set to "Install Automatically".

"Cancel" and "Save" buttons are at the bottom right.

10. If you chose to distribute the profile in the Self Service web clip, upload an icon to display and choose a security setting from the **Security** pop-up menu.
11. If needed, use the payloads list to add or modify payloads.

12. Click the **Scope** tab and assign devices to the scope.

The screenshot shows a web-based configuration interface for a mobile device profile. The title bar reads "Edit Profile: Passcode Settings". Below the title bar are two tabs: "General" (with an information icon) and "Scope" (with a mobile phone icon). The "Scope" tab is active. The main content area is divided into three sections:

- Assign this Profile to these Mobile Devices:** This section contains two radio buttons. The first is "Assign to All Mobile Devices". The second is "Assign to Specific Mobile Devices", which is selected. Below this selected option are four links: "Add Mobile Device Groups", "Add Individual Devices", "Add Departments", and "Add Buildings".
- Limit this Setting to the following Users:** This section contains a single link: "Add User Group".
- Install this profile to mobile devices in these Network Segments:** This section contains two radio buttons. The first is "Use Setting For Mobile Devices With Any IP Address", which is selected. The second is "Use Setting For Mobile Devices in Specified Network Segments".

At the bottom right of the dialog box are two buttons: "Cancel" and "Save".

13. Click **Save**.

The next time devices in the scope contact the JSS, they receive the profile based on the distribution method you chose.

# Updating iOS Configuration Profiles

To update an iOS configuration profile, use the JAMF Software Server (JSS) to add, modify, or remove payloads as needed.

**Note:** Some payloads and settings configured in iPCU or Profile Manager are not displayed in the JSS.

## To update an iOS configuration profile:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Edit** link across from the profile.
5. Use the payloads list to add, modify, or remove payloads as needed.
6. Click **Save**.

The configuration profile is updated the next time devices in the scope contact the JSS.

# Removing iOS Configuration Profiles

To remove an iOS configuration profile from a device, remove the device from the scope. When the profile is removed, all settings associated with the profile are also removed.

## To remove an iOS configuration profile:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Edit** link across from the profile.
5. Click the **Scope** tab and remove devices from the scope as needed.

**Edit Profile: Passcode Settings**

General | **Scope**

**Assign this Profile to these Mobile Devices**

Assign to All Mobile Devices

Assign to Specific Mobile Devices  
[Add Mobile Device Groups](#) | [Add Individual Devices](#) | [Add Departments](#) | [Add Buildings](#)

**Individual Devices** | [Back to top](#)

Device Name	User	Department	Room	Remove
QA-Table3-iPod				<a href="#">Remove</a>
QA-Table1-iPad				<a href="#">Remove</a>
QA-Table2-iPad				<a href="#">Remove</a>

**Limit this Setting to the following Users**

[Add User Group](#)

**Install this profile to mobile devices in these Network Segments**

Use Setting For Mobile Devices With Any IP Address

Use Setting For Mobile Devices in Specified Network Segments

[Cancel](#) [Save](#)

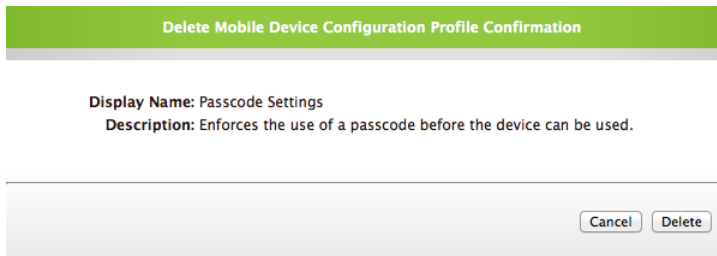
6. Click **Save**.

# Deleting iOS Configuration Profiles

Deleting an iOS configuration profile from the JAMF Software Server (JSS) removes the profile and its settings from all devices in the scope.

## To delete an iOS configuration profile from the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Delete** link across from the profile, and then click the **Delete** button to confirm.



# Security Management

## Running Remote Commands for Mobile Devices

The JAMF Software Server (JSS) allows you to manage to security of mobile devices by running the following commands:

- **Remote Lock**—Locks the device. If the device has a passcode, the user must enter it to unlock the device.
- **Remote Clear Passcode**—Removes the passcode from the device.
- **Remote Wipe**—Permanently erases all data on the device and deactivates it. To restore the device to the original factory settings, you must manually reactivate the device.

**Note:** Running a remote wipe command on a device does not remove the device from the JSS or modify its inventory information.

There are two ways to run a remote command from the JSS:

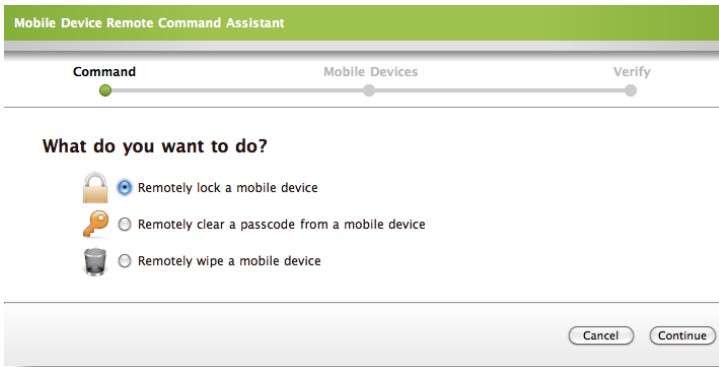
- Use the Remote Command Assistant.
- Use the icons displayed when viewing a Mobile Device Details report.

**Note:** Using the icons displayed when viewing a Mobile Device Details report runs a remote command for an individual device only.

**To run a remote command using the Remote Command Assistant:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Remote Commands** link.
4. Click the **New Remote Command** button.

- Select the command that you want to run, and then click **Continue**.






- Follow the onscreen instructions to configure the rest of the command.

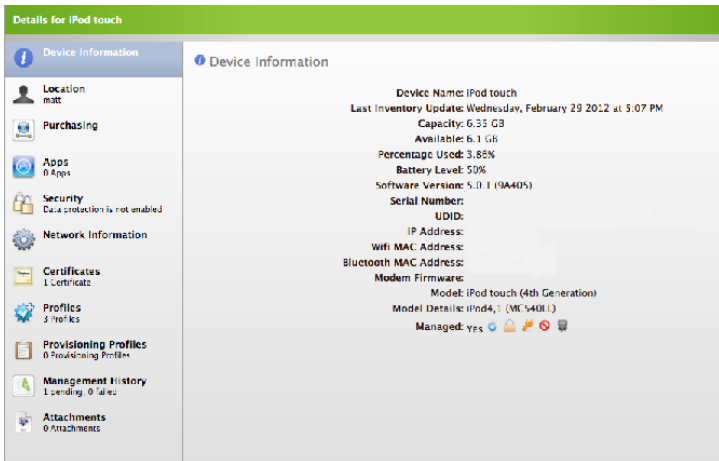
The remote command runs on the devices that you specified the next time the devices contact the JSS.

**To run a remote command from a Mobile Device Details report:**

- Log in to the JSS with a web browser.
- Click the **Inventory** tab and perform a simple or advanced mobile device search. See the "Performing Simple Mobile Device Searches" or "Performing Advanced Mobile Device Searches" section in "Searching Mobile Devices" for complete instructions.
- Find the device that you want to run the remote command, and click the **Details** link across from it.
- Next to the **Enrolled** field, click the icon for the command you want to run.

**Note:** If you have upgraded the JSS from v8.5 or earlier, the command icons are next to the **Managed** field.

- The  icon runs the remote lock command.
- The  icon runs the remote clear passcode command.
- The  icon runs the remote wipe command.



The remote command runs on the device the next time the device contacts the JSS.

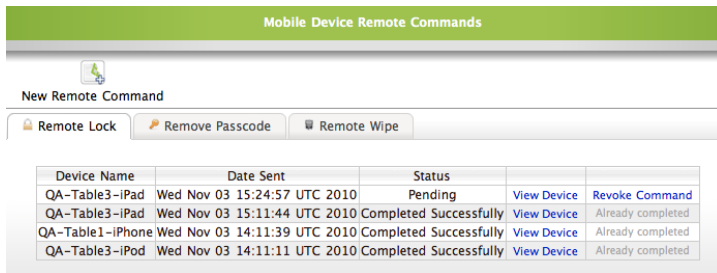


# Viewing the Status of Remote Commands for Mobile Devices

The JSS allows you to view the status of all remote commands for mobile devices or view the status of remote commands for an individual device.

## To view the status of all remote commands for mobile devices:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Remote Commands** link.
4. Use the **Remote Lock**, **Remove Passcode**, and **Remote Wipe** tabs to view the status of remote commands.

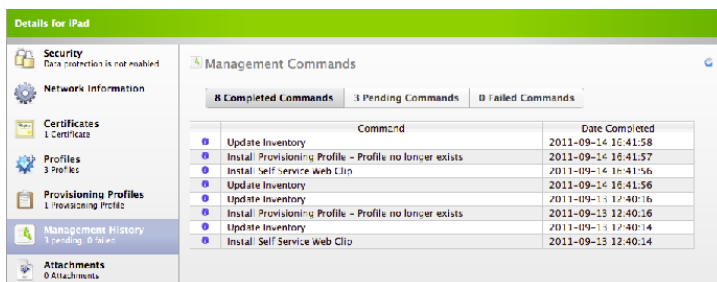


Device Name	Date Sent	Status	View Device	Revoke Command
QA-Table3-iPad	Wed Nov 03 15:24:57 UTC 2010	Pending	<a href="#">View Device</a>	<a href="#">Revoke Command</a>
QA-Table3-iPad	Wed Nov 03 15:11:44 UTC 2010	Completed Successfully	<a href="#">View Device</a>	Already completed
QA-Table1-iPhone	Wed Nov 03 14:11:39 UTC 2010	Completed Successfully	<a href="#">View Device</a>	Already completed
QA-Table3-iPod	Wed Nov 03 14:11:11 UTC 2010	Completed Successfully	<a href="#">View Device</a>	Already completed

The status of each remote command is displayed as "Pending" or "Completed Successfully," along with the date and time that the command was sent.

## To view the status of remote commands for an individual device:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab and perform a simple or advanced mobile device search. See the "Performing Simple Mobile Device Searches" or "Performing Advanced Mobile Device Searches" section in "Searching Mobile Devices" for complete instructions.
3. Find the device that you want to view commands for, and click the **Details** link across from it.
4. Click Management History in the list of categories.
5. Use the **Completed Commands**, **Pending Commands**, and **Failed Commands** tabs to view the status of remote commands.



Command	Date Completed
Update Inventory	2011-09-14 16:41:58
Install Provisioning Profile - Profile no longer exists	2011-09-14 16:41:57
Install Self Service Web Clip	2011-09-14 16:41:56
Update Inventory	2011-09-14 16:41:56
Update Inventory	2011-09-13 12:40:16
Install Provisioning Profile - Profile no longer exists	2011-09-13 12:40:16
Update Inventory	2011-09-13 12:40:14
Install Self Service Web Clip	2011-09-13 12:40:14

# Canceling Remote Commands for Mobile Devices

The JSS allows you to cancel a remote command if the command is in a pending state. You can cancel a command for all mobile devices or cancel a command for an individual device.

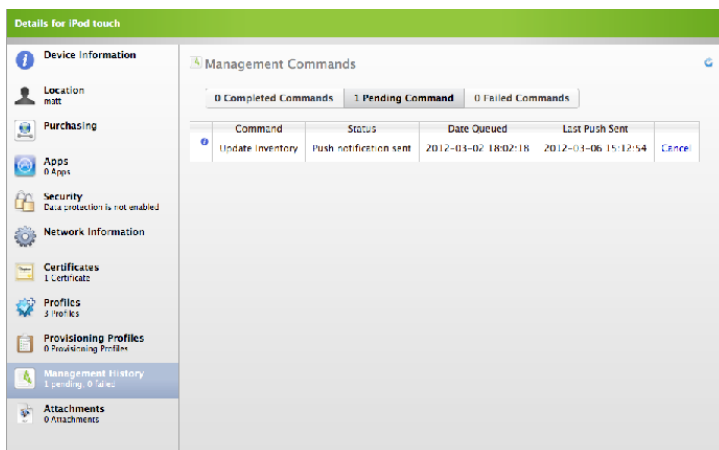
## To cancel a remote command for all mobile devices:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Remote Commands** link.
4. Use the **Remote Lock**, **Remove Passcode**, and **Remote Wipe** tabs to find the command you want to cancel, and then click the **Cancel** link across from the command.

The **Cancel** link is only displayed for remote commands in a pending state.

## To cancel a remote command for an individual device:

1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab and perform a simple or advanced mobile device search. See the "Performing Simple Mobile Device Searches" or "Performing Advanced Mobile Device Searches" section in "Searching Mobile Devices" for complete instructions.
3. Find the device that you sent the command to, and click the **Details** link across from it.
4. Click Management History in the list of categories.
5. Click the **Pending Commands** tab.
6. Find the remote command you want to cancel, and click the **Cancel** link across from it.



7. When prompted, click **OK** to confirm the cancelation.

# Distribution

## Apps

### Understanding Unmanaged and Managed Apps

The Casper Suite allows you to manage the apps that you distribute to mobile devices. Managing an app gives you more control over installation and removal of the app, and allows you to set some additional management options.

The primary advantages to managing an app are that you can prompt users to install the app, and you can remove the app from devices that have it installed.

The following table shows the differences between an unmanaged app and a managed app:

	Unmanaged app	Managed app
<b>Distribution Methods</b>		
Display in Self Service web clip	✓	✓
Prompt user to install		✓
<b>Removal Options</b>		
Remove from Self Service web clip	✓	✓
Remove from device		✓
<b>Additional Management Options</b>		
Remove app when MDM profile is removed		✓
Prevent backup of app data		✓

### Requirements for Managing Apps

There are three factors that determine whether you can manage an app:

- The type of app
  - The app must be an in-house app, a free App Store app, or a paid App Store app with VPP codes.

- The devices to which you distribute the app

Managing an app requires a mobile device with iOS 5 or later and an MDM profile that supports managed apps. Devices that have iOS 5 or later at the time they are enrolled with the Casper Suite v8.3 or later automatically receive an MDM profile that supports managed apps.

For information on distributing an updated MDM profile that supports managed apps, see the “Self Service Web Clip” section in “Configuring the Mobile Device Management Framework”.

- The method you use to distribute the app

When configuring the app for distribution in the JAMF Software Server (JSS), you must choose one of the following distribution methods:

- Prompt user to install
- Make available in the Self Service web clip and manage when possible

See the "Understanding App Distribution Methods" section for more information.

## Understanding App Distribution Methods

The Casper Suite allows you to distribute apps to devices in three ways:

- Prompt users to install the app.
- Make the app available in the Self Service web clip and manage it when possible.
- Make the app available in the Self Service web clip and do not manage it.

You choose how you want to distribute an app when configuring it for distribution in the JSS. For detailed instructions on distributing an app, see the “Distributing In-House Apps” or “Distributing App Store Apps” section.

The distribution method that you choose affects:

- Management status of the app
- Installation of the app
- Installation of updates to the app
- Removal of the app

### Prompt Users to Install

This distribution method has a different effect on devices that support managed apps and devices that do not.

On devices that support managed apps, the app is managed. Users are prompted to install the app and any future updates to the app. Removing the app removes it from the devices.

On devices that do not support managed apps, the app is unmanaged. The app and any future updates to the app are displayed in the Self Service web clip. Removing the app removes it from the Self Service web clip only.

## Make Available in the Self Service Web Clip and Manage When Possible

This distribution method has a different effect on devices that support managed apps and devices that do not.

On devices that support managed apps, the app is managed. The app and any future updates to the app are displayed in the Self Service web clip. Removing the app removes it from devices that have it installed and from the Self Service web clip.

On devices that do not support managed apps, the app is unmanaged. The app and any future updates to the app are displayed in the Self Service web clip. Removing the app removes it from the Self Service web clip only.

## Make Available in the Self Service Web Clip and Do Not Manage

This distribution method makes the app unmanaged on all devices, regardless of whether they support managed apps or not. The app and any future updates to the app are displayed in the Self Service web clip. Removing the app removes it from the Self Service web clip only.

## Provisioning Profiles

Provisioning profiles (.mobileprovision) authorize the use of in-house apps. For an in-house app to work, the provisioning profile that authorizes its use must be installed on devices.

If the provisioning profile that authorizes an in-house app is not bundled in the app archive (.ipa) file, you can use the JSS to upload the provisioning profile and associate it with the app.

This section explains how to upload and delete provisioning profiles in the JSS.

For more information on in-house apps and how to distribute an in-house app and its provisioning profile, see the "Distributing In-House Apps" section.

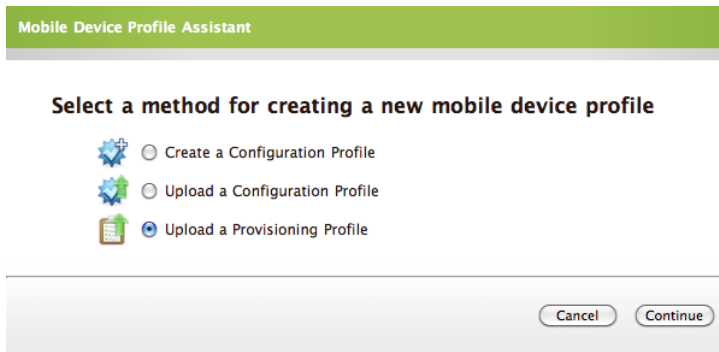
## Uploading Provisioning Profiles

If the provisioning profile for an in-house app is not bundled in the archived app file (.ipa), upload the provisioning profile to the JSS before you distribute the app.

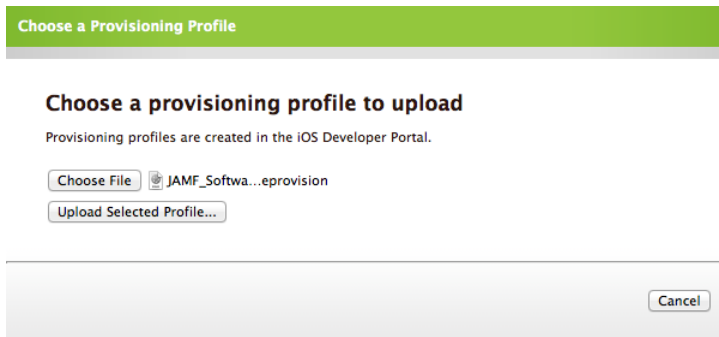
### To upload a provisioning profile to the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Add Profile** button.

5. Select **Upload a Provisioning Profile**, and then click **Continue**.



6. Click **Choose File** and select the profile that you want to upload. Then, click **Upload Selected File**. The profile must have a .mobileprovision file extension.



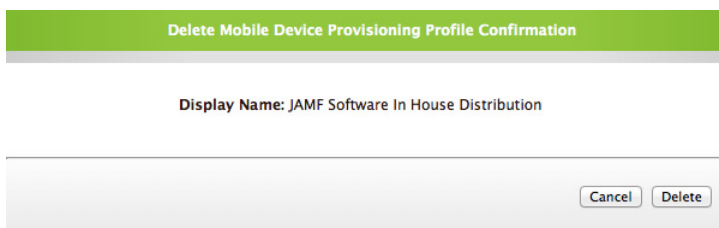
7. Click **Save**.

## Deleting Provisioning Profiles

Deleting a provisioning profile from the JSS removes it from devices that have it installed.

### To delete a provisioning profile from the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device Profiles** link.
4. Click the **Provisioning Profiles** tab.
5. Click the **Delete** link across from the profile, and then click the **Delete** button to confirm.



## Distributing In-House Apps

In-house apps are enterprise apps developed through Apple's iOS Developer Enterprise Program that are not available in the App Store.

For more information on Apple's iOS Developer Enterprise Program or to register, visit the following website:

<https://developer.apple.com/programs/ios/enterprise/>

To distribute an in-house app, add it to the Mobile Device App Catalog in the JSS by uploading the archived app (.ipa) file or entering the URL where the app is hosted. Then, choose how you want to distribute the app and associate it with a provisioning profile. Lastly, specify which devices will receive the app.

Before distributing an in-house app, make sure you have:

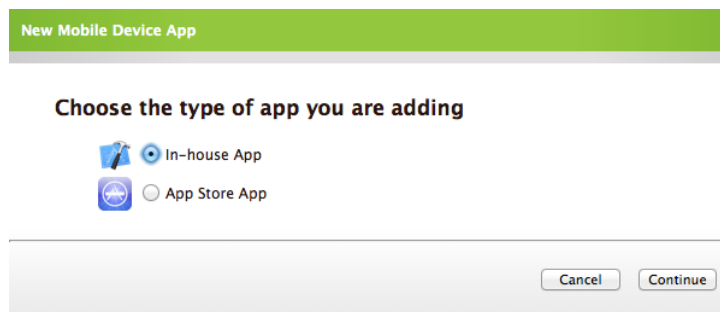
- The bundle identifier for the app  
The bundle identifier is the unique identifier for the app. It is located in the PLIST file for the app.
- The archived app file or the URL where the app is hosted on a web server

**Note:** If you are hosting the app from a web server, the MIME type for the archived app file must be "application/octet-stream".

- The provisioning profile (.mobileprovision) uploaded to the JSS (See the "Provisioning Profiles" section for instructions and more information.)  
The provisioning profile only needs to be uploaded to the JSS if it is not bundled in the archived app file.

### To distribute an in-house app:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device App Catalog** link.
4. Click the **Add App** button.
5. Select **In-house App**, and then click **Continue**.



6. Enter the app name, bundle identifier, and version number.

**Important:** The bundle identifier must match the bundle identifier in the PLIST file for the app.

**Edit Mobile Device App**

App Info | Scope

App Name:

Bundle ID:

Version:

Deployment: **Make Available in Self Service** ▾

Deploy as managed app (when possible)

Remove app when MDM profile is removed

Prevent backup of the app data

Description:

Icon: [Upload icon...](#)

Hosting Location: **Upload to JSS** ▾

App Archive File: [Upload App Archive...](#)

Provisioning Profile: **Bundled in IPA** ▾

Cancel Save

7. Choose a distribution method.

- To prompt users to install the app, choose "Prompt User to Install" from the **Deployment** pop-up menu.
- To display the app in the Self Service web clip and manage it when possible, choose "Make Available in Self Service" from the **Deployment** pop-up menu and leave the **Deploy as managed app (when possible)** checkbox selected.
- To display the app in the Self Service web clip and not manage it, choose "Make Available in Self Service" from the **Deployment** pop-up menu and deselect the **Deploy as managed app (when possible)** checkbox.

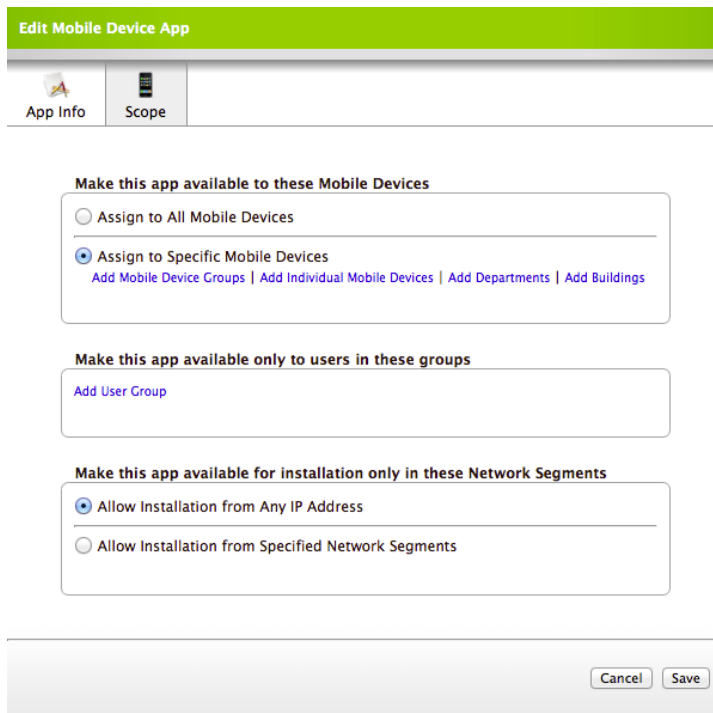
For more information on unmanaged and managed apps and devices that support managed apps, see the "Understanding Unmanaged and Managed Apps" section.

For more information on each distribution method, see the "Understanding App Distribution Methods" section.

8. If you chose to prompt users to install the app or display the app in the Self Service web clip and manage it when possible, select the following management options as needed:
  - Remove app when MDM profile is removed
  - Prevent backup of the app data
9. If desired, enter a description and upload an icon to display in the Self Service web clip.



10. Choose a hosting location for the app.
  - To host the app from the JSS, choose "Upload to JSS" from the **Hosting Location** pop-up menu. Then, upload the archived app file (.ipa).
  - If the app is hosted on a web server, choose "Host on web server (recommended for large apps)" from the **Hosting Location** pop-up menu. Then, enter the URL where the app is hosted.
11. Choose the provisioning profile that authorizes the app from the **Provisioning Profile** pop-up menu. If the provisioning profile is bundled in the archived app file, choose "Bundled in IPA".
12. Click the **Scope** tab and assign devices to the scope.



13. Click **Save**.

The app is distributed the next time devices in the scope contact the JSS.

## Distributing App Store Apps

The JSS allows you to distribute App Store apps to enrolled mobile devices. To distribute an App Store app, add it to the Mobile Device App Catalog in the JSS by browsing the App Store or entering information about the app manually. Then, choose how you want to distribute the app and specify which devices receive it.

To install an App Store app, users must enter an Apple ID.

The JSS also allows you to distribute Apple's Volume Purchase Program (VPP) codes and view their redemption status.

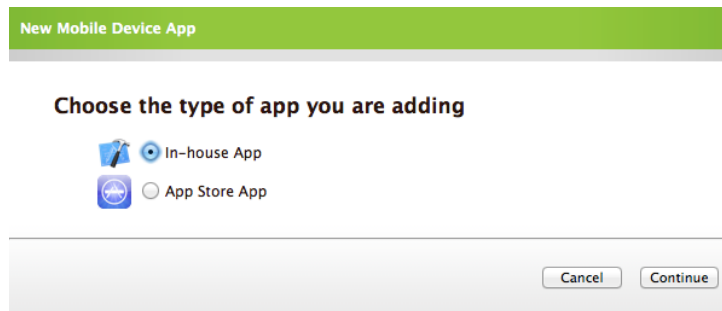
For more information on Apple's Volume Purchase Program, visit one of the following websites:

- App Store Volume Purchasing for Business:  
<https://www.apple.com/business/vpp/>
- App Store Volume Purchasing for Education:  
<https://www.apple.com/education/volume-purchase-program/>

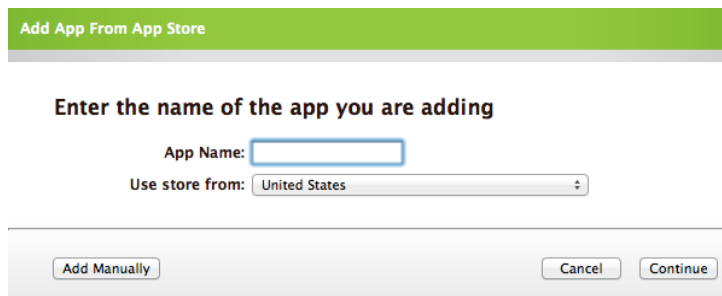
To distribute VPP codes for the app, upload the Excel spreadsheet (.xls or .xlsx) that contains the VPP codes to the Mobile Device App Catalog. Each time a user installs the app, a VPP code is redeemed.

### To distribute an App Store app:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device App Catalog** link.
4. Click the **Add App** button.
5. Select **App Store App**, and then click **Continue**.



6. Add the app to the Mobile Device App Catalog.
  - To browse the App Store, enter the name of the app and choose an App Store country. Then, click **Continue**.
  - To add the app manually, click **Add Manually**, and then skip to step 8.



7. Click the **Add** link across from the app.  
To preview an app, click the **View Page** link. The iTunes Preview page opens in a separate browser window.

- Enter or verify the app name, version number, and URL.  
The version number must match the version number for the app exactly.

**Note:** The **Bundle ID** field may be blank. The JSS populates the bundle identifier after the app is distributed.

- If you manually added a free app, select the **Free** checkbox.  
The **Free** checkbox is selected automatically if you added a free app by browsing the App Store.
- (Optional) If you manually added the app, upload an icon to display in the Self Service web clip.
- To distribute VPP codes with a paid app, click the **VPP Codes** tab and upload the Excel spreadsheet (.xls or .xlsx) that contains the VPP codes.

**Note:** The **VPP Codes** tab is not displayed when the **Free** checkbox is selected.

12. Click the **App Info** tab and choose a distribution method.
  - To prompt users to install the app, choose "Prompt User to Install" from the **Deployment** pop-up menu.

**Note:** The "Prompt User to Install" option is only displayed for free apps and paid apps with VPP codes.

- To display the app in the Self Service web clip and manage it when possible, choose "Make Available in Self Service" from the **Deployment** pop-up menu and leave the **Deploy as managed app (when possible)** checkbox selected.
- To display the app in the Self Service web clip and not manage it, choose "Make Available in Self Service" from the **Deployment** pop-up menu and deselect the **Deploy as managed app (when possible)** checkbox.

**Note:** The **Deploy as managed app (when possible)** checkbox is only displayed for free apps and paid apps with VPP codes.

For more information on unmanaged and managed apps and devices that support managed apps, see the "Understanding Unmanaged and Managed Apps" section.

For more information on each distribution method, see the "Understanding App Distribution Methods" section.

13. If you chose to prompt users to install the app or display the app in the Self Service web clip and manage it when possible, select the following management options as needed:
  - Remove app when MDM profile is removed
  - Prevent backup of the app data

**Edit Mobile Device App**

App Info | Scope | VPP Codes

App Name: UNO? HD

Version: 1.3.1

Bundle ID: com.gameloft.unoiPad

Free:

Deployment: Make Available in Self Service

- Deploy as managed app (when possible)
- Remove app when MDM profile is removed
- Prevent backup of the app data

Icon: Change icon...

App URL: http://itunes.apple.com/us/app/uno-hd/id364368518?mt

Cancel Save

14. Click the **Scope** tab and assign devices to the scope.

The screenshot shows the 'Edit Mobile Device App' dialog box with the 'Scope' tab selected. The dialog has a green header bar with the title 'Edit Mobile Device App'. Below the header, there are two tabs: 'App Info' and 'Scope', with 'Scope' being the active tab. The main content area is divided into three sections, each with a title and a list of options:

- Make this app available to these Mobile Devices**
  - Assign to All Mobile Devices
  - Assign to Specific Mobile Devices
    - [Add Mobile Device Groups](#) | [Add Individual Mobile Devices](#) | [Add Departments](#) | [Add Buildings](#)

- Make this app available only to users in these groups**
- [Add User Group](#)
- Make this app available for installation only in these Network Segments**
- Allow Installation from Any IP Address
- Allow Installation from Specified Network Segments

At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Save'.

15. Click **Save**.

The app is distributed the next time devices in the scope contact the JSS.

## Updating Apps

To distribute an app update, you must update the version number and URL for the app in the Mobile Device App Catalog. For an in-house app, you must also upload the new archived app file to the Mobile Device App Catalog or to the web server where the app is hosted.

To install an App Store app update, users must enter an Apple ID.

Updates are distributed in the same way that you distributed the app. For a detailed explanation, see the "Understanding App Distribution Methods" section.

### To update an app:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device App Catalog** link.
4. Click the **Edit** link across from the app.

**Important:** Do not change the bundle identifier. The JSS uses the existing bundle identifier to distribute the update.

5. Enter the new version number.  
If you are updating an App Store app, the version number must match the version number for the app exactly.
6. If you are updating an in-house app that is hosted from the JSS, click the **Upload New App Archive** link and upload the new archived app file (.ipa).
7. Enter the new app URL.
8. Click **Save**.

The update is distributed the next time devices in the scope contact the JSS.

## Removing Apps

To remove an app, remove one or more devices from the scope.

App removal is based the distribution method you chose for the app. For a detailed explanation, see the "Understanding App Distribution Methods" section.

### To remove an app:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device App Catalog** link.
4. Click the **Edit** link across from the app.

5. Click the **Scope** tab and remove devices from the scope as needed.

**Edit Mobile Device App**

App Info | **Scope**

**Make this app available to these Mobile Devices**

Assign to All Mobile Devices

Assign to Specific Mobile Devices  
[Add Mobile Device Groups](#) | [Add Individual Mobile Devices](#) | [Add Departments](#) | [Add Buildings](#)

**Individual Mobile Devices** | [Back to top](#)

Mobile Device Name	User	Remove
QA-Table3-iPod		<a href="#">Remove</a>
QA-Table1-iPad		<a href="#">Remove</a>
QA-Table2-iPad		<a href="#">Remove</a>

**Make this app available only to users in these groups**

[Add User Group](#)

**Make this app available for installation only in these Network Segments**

Allow Installation from Any IP Address

Allow Installation from Specified Network Segments

[Cancel](#) [Save](#)

6. Click **Save**.

The app is removed the next time devices that you removed from the scope contact the JSS.

## Deleting Apps

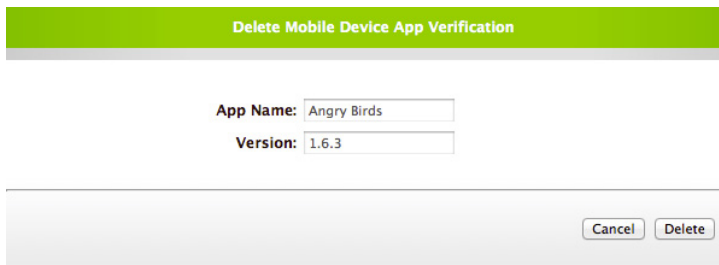
Deleting an app from the Mobile Device App Catalog removes the app from devices or from the Self Service web clip.

App removal is based the distribution method you chose for the app. For a detailed explanation, see the “Understanding App Distribution Methods” section.

### To delete an app from the Mobile Device App Catalog:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device App Catalog** link.

4. Click the **Delete** link across from the app, and then click the **Delete** button to confirm.



The image shows a dialog box titled "Delete Mobile Device App Verification". It has a green header bar with the title in white text. Below the header, there are two input fields: "App Name" with the value "Angry Birds" and "Version" with the value "1.6.3". At the bottom right of the dialog, there are two buttons: "Cancel" and "Delete".

The app is removed the next time devices in the scope contact the JSS.



# eBooks

The JAMF Software Server (JSS) allows you to distribute eBooks to enrolled mobile devices. Distributing an eBook displays it in the Self Service web clip for users to install. After users install an eBook, they can view it with Apple's iBooks app.

This section explains how to distribute eBooks that are hosted internally on a web server (in-house eBooks) and eBooks that are available in the iBookstore. It also explains how to edit and delete eBooks.

## Requirements

The Casper Suite supports the following eBook file formats:

- ePub (.epub)
- iBooks (.ibooks)
- PDF

Installing an ePub file requires a mobile device with iOS 4 or later and iBooks 1.0 or later.

Installing an iBooks file requires an iPad with iOS 5 or later and iBooks 2.0 or later.

## Distributing In-House eBooks

In-house eBooks are eBooks that are hosted internally on a web server. To distribute an in-house eBook, add it to the Mobile Device eBook Catalog in the JSS by entering information about the eBook, including the URL where it is hosted. Then specify which devices display the eBook in the Self Service web clip.

### To distribute an in-house eBook:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device eBook Catalog** link.
4. Click the **Add eBook** button.

5. Click the **Add Manually** button.

The screenshot shows a dialog box titled "Add eBook From iBookstore". It has a green header bar with the title. Below the header, the text "Enter the name or ISBN of the eBook you are adding" is centered. There is a text input field for "eBook Name or ISBN:" and a dropdown menu for "Use store from:" which is currently set to "United States". At the bottom of the dialog, there are three buttons: "Add Manually", "Cancel", and "Continue".

6. Enter the eBook name and the URL where the eBook is hosted.
7. Upload an icon to display in the Self Service web clip.

The screenshot shows the "Edit eBook" form. It has a green header bar with the title. Below the header, there are three tabs: "eBook Info", "Scope", and "VPP Codes". The "eBook Info" tab is selected. The form contains the following fields: "eBook Name:" with the value "CK-12 Basic Algebra,"; "URL:" with the value "http://itunes.apple.com/us/book/ck-12-basic-algebra-vol"; "Free:" with an unchecked checkbox; and "Icon:" with a small icon and a "Change icon..." link. At the bottom right, there are "Cancel" and "Save" buttons.

8. Click the **Scope** tab and assign devices to the scope.

The screenshot shows the "Edit eBook" form with the "Scope" tab selected. The form is divided into three sections: "Make this eBook available to these Mobile Devices", "Make this eBook available only to users in these groups", and "Make this eBook available for installation only in these Network Segments". The first section has two radio buttons: "Assign to All Mobile Devices" (unselected) and "Assign to Specific Mobile Devices" (selected). Below the second radio button are links: "Add Mobile Device Groups", "Add Individual Mobile Devices", "Add Departments", and "Add Buildings". The second section has a link "Add User Group". The third section has two radio buttons: "Allow Installation from Any IP Address" (selected) and "Allow Installation from Specified Network Segments" (unselected). At the bottom right, there are "Cancel" and "Save" buttons.

9. Click **Save**.

The eBook is distributed the next time devices in the scope contact the JSS.

## Distributing eBooks Available in the iBookstore

To distribute an eBook that is available in the iBookstore, add it to the Mobile Device eBook Catalog in the JSS by browsing the iBookstore or entering information about the eBook manually. Then specify which devices display the eBook in the Self Service web clip.

The JSS also allows you to distribute Apple's Volume Purchase Program (VPP) codes and view their redemption status.

For more information on Apple's Volume Purchase Program, visit one of the following websites:

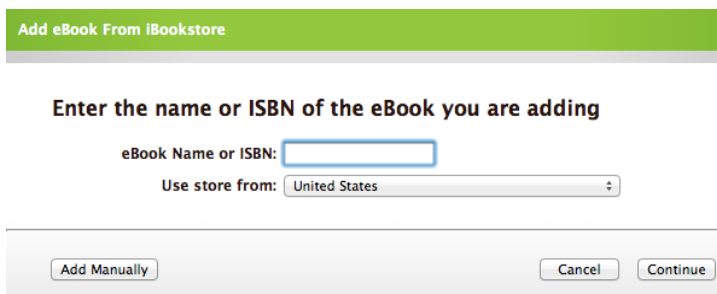
- App Store Volume Purchasing for Business:  
<https://www.apple.com/business/vpp/>
- App Store Volume Purchasing for Education:  
<https://www.apple.com/education/volume-purchase-program/>

To distribute VPP codes for the eBook, upload the Excel spreadsheet (.xls or .xlsx) that contains the VPP codes to the Mobile Device eBook Catalog. Each time a user installs the eBook, a VPP code is redeemed.

### To distribute an eBook available in the iBookstore:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device eBook Catalog** link.
4. Click the **Add eBook** button.
5. Add the eBook to the Mobile Device eBook Catalog.
  - To browse the iBookstore, enter the name or International Standard Book Number (ISBN) for the eBook and choose an iBookstore country. Then, click **Continue**.
  - To add the eBook manually, click **Add Manually**, and then skip to step 7.

**Note:** iBooks files (.ibooks) may need to be added manually.



Add eBook From iBookstore

Enter the name or ISBN of the eBook you are adding


eBook Name or ISBN:

Use store from:

- Click the **Add** link across from the eBook that you want to distribute.  
To preview an eBook, click the **View Page** link. The iTunes Preview page opens in a separate browser window.
- Enter or verify the eBook name and URL.

**Edit eBook**

eBook Info   Scope   VPP Codes

eBook Name: CK-12 Basic Algebra,  
 URL: http://itunes.apple.com/us/book/ck-12-basic-algebra-vol  
 Free:   
 Icon:  [Change icon...](#)

Cancel   Save

- If you manually added a free eBook, select the **Free** checkbox.  
The **Free** checkbox is selected automatically if you added a free eBook by browsing the iBookstore.
- If you manually added the eBook, upload an icon to display in the Self Service web clip.
- To distribute VPP codes with a paid eBook, click the **VPP Codes** tab and upload the Excel spreadsheet (.xls or .xlsx) that contains the VPP codes.

**Note:** The **VPP Codes** tab is not displayed when the **Free** checkbox is selected.

**Edit eBook**

eBook Info   Scope   VPP Codes

**Volume Purchase Codes**

Volume Purchase Codes allow educational institutions to purchase multiple copies of the same eBook at once and make them available to end users.

[Upload VPP Codes...](#)  
[Clear VPP Codes...](#)

Total Codes: 0  
 Redeemed Codes: 0  
 Available Codes: 0

Code	Status	Date	Username	Device
No VPP Codes				

Cancel   Save

11. Click the **Scope** tab and assign devices to the scope.

The screenshot shows the 'Edit eBook' dialog box with the 'Scope' tab selected. The dialog has a green header bar with the text 'Edit eBook'. Below the header are three tabs: 'eBook Info', 'Scope', and 'VPP Codes'. The 'Scope' tab is active and contains three sections:

- Make this eBook available to these Mobile Devices**: This section has two radio button options. The first is 'Assign to All Mobile Devices' (unselected). The second is 'Assign to Specific Mobile Devices' (selected). Below the second option are four links: 'Add Mobile Device Groups', 'Add Individual Mobile Devices', 'Add Departments', and 'Add Buildings'.
- Make this eBook available only to users in these groups**: This section has a single text input field with the placeholder text 'Add User Group'.
- Make this eBook available for installation only in these Network Segments**: This section has two radio button options. The first is 'Allow Installation from Any IP Address' (selected). The second is 'Allow Installation from Specified Network Segments' (unselected).

At the bottom right of the dialog are two buttons: 'Cancel' and 'Save'.

12. Click **Save**.

The eBook is distributed the next time devices in the scope contact the JSS.

## Editing eBooks

Editing an eBook in the Mobile Device eBook Catalog allows you to:

- Change the eBook name and icon displayed in the Self Service web clip
- Change the URL
- Modify the scope
- Clear VPP codes

### To edit an eBook:

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device eBook Catalog** link.

4. Click the **Edit** link across from the eBook and make the necessary changes.

The screenshot shows a web interface for editing an eBook. The title bar is green and says "Edit eBook". There are three tabs: "eBook Info", "Scope", and "VPP Codes". The "eBook Info" tab is active and shows the following information: "eBook Name: CK-12 Basic Algebra,", "URL: http://itunes.apple.com/us/book/ck-12-basic-algebra-vol", "Free: ", and "Icon: [icon] Change icon...". At the bottom right, there are "Cancel" and "Save" buttons.

5. Click **Save**.

The changes are applied the next time devices in the scope contact the JSS.

## Deleting eBooks

Deleting an eBook from the Mobile Device eBook Catalog removes the eBook from the Self Service web clip.

**To delete an eBook from the Mobile Device eBook Catalog:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **Mobile Device eBook Catalog** link.
4. Click the **Delete** link across from the eBook, and then click the **Delete** button to confirm.

The eBook is removed the next time devices in the scope contact the JSS.