Casper Suite Administrator's Guide

Version 9.2

JAMF software

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

Contents

Preface

About This Guide

This guide contains overviews about Casper Suite features and instructions for performing administrative tasks using the Casper Suite. It does not prescribe administrative workflows or strategies but is intended to be used as a reference.

Before using the instructions in this guide, the JAMF Software Server (JSS) must be installed.

To learn about the other Casper Suite-related documentation, including documentation about installing and configuring the JSS, see the following section in this guide:

Additional Resources

Additional Resources

For more information on Casper Suite-related topics, see the following resources:

- *Casper Suite Release Notes*

  The release notes include a list of new features, bug fixes, and known issues. They also explain how to upgrade the JSS, and what you need to do to take advantage of new features. Release notes for the most recent version of the Casper Suite are available in the Casper Suite DMG, and at:

  http://www.jamfsoftware.com/product-documentation/release-notes

- JAMF Software Server installation and configuration guides

  These guides provide information on installing and setting up the JSS on supported Mac, Linux, and Windows platforms. They also explain how to perform advanced configuration and troubleshooting tasks. They are available at:

  http://www.jamfsoftware.com/product-documentation/installation-guides

- *Manually Installing the JAMF Software Server*

  This technical paper explains how to manually install the JSS on Linux and Windows platforms. You can download it from:

  http://www.jamfsoftware.com/product-documentation/installation-guides

- QuickStart Guides

  The *QuickStart Guide for Managing Computers* and the *QuickStart Guide for Managing Mobile Devices* serve as a starting point for new Casper Suite administrators. They provide simplified workflows for performing basic administrative tasks, such as inventory and software distribution, and they reference related sections in the *Casper Suite Administrator's Guide*. Both QuickStart Guides are available in the Casper Suite DMG, and at:

  http://www.jamfsoftware.com/product-documentation/quickstart-guides

- Technical papers

  JAMF Software technical papers provide best-practice, step-by-step workflows for using the Casper Suite to administer third-party software, such as Adobe Creative Suite or FileVault 2. They are available at:

  http://www.jamfsoftware.com/technical-papers

- JAMF Nation

  The JAMF Nation community website contains several different types of resources related to the Casper Suite. It allows you communicate with other users via discussions, submit feature requests, and access the Knowledge Base. The Knowledge Base contains hundreds of articles that address frequently asked questions and common issues. You can access JAMF Nation at:

  https://jamfnation.jamfsoftware.com

Overview of Technologies

Applications and Utilities

This section provides an overview of the applications and utilities that make up the Casper Suite.

Casper Admin

The Casper Admin application is a repository that allows you to add and manage packages, scripts, printers, and Dock items. It also allows you to create configurations (images) using these items and replicate files to distribution points.

Casper Focus

The Casper Focus app is designed to be used by teachers in the classroom. It gives teachers control over the devices used during class time by allowing the teacher to "focus" the devices on a single app. Focusing a device locks it on the app, preventing students from accessing any other screens or applications. Teachers can also switch the focus from one app to another, or remove the focus from student devices. In addition, teachers can clear passcodes on student devices during class time as needed.

Casper Focus is available for free from the App Store.

Casper Imaging

The Casper Imaging application allows you to image computers by deploying configurations to them.

Casper Remote

The Casper Remote application allows you to immediately perform remote management tasks on computers, such as installing packages, running scripts, and binding to directory services. While policies allow you to automate these tasks so that they run on a schedule, Casper Remote allows you to perform them immediately over a Secure Shell (SSH) connection.

Composer

The Composer application allows you to build packages (PKG or DMG) of software, applications, preference files, or documents. Composer also allows you to build a DMG of an operating system.

jamf agent

The jamf agent collects application usage data and restricts software on managed computers. It also displays policy messages in the Notification Center in OS X.

The jamf agent is installed and updated on managed computers automatically. It is installed in the following location:

```
/usr/sbin/jamfAgent
```

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, it is installed, updated, and run on managed computers automatically. It is stored in the following location on managed computers:

```
/usr/sbin/jamf
```

JAMF Helper

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

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

JAMF Software Server

The JAMF Software Server (JSS) is a web application that functions as the administrative core of the Casper Suite. The JSS allows you to perform inventory and remote management and configuration tasks on managed computers and mobile devices. All other administrative applications in the Casper Suite communicate with the JSS.

JDS Installers

The JDS Installer for Mac (.pkg) and the JDS Installer for Linux (.run) allow you to install JDS instances on OS X or supported Linux operating systems.

A JDS instance is a distribution point that is managed by the JSS, similar to a computer or mobile device. For more information on JDS instances, see JAMF Distribution Server Instances.

To obtain the JDS Installers, log in to JAMF Nation and go to the following page:

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

Recon

The Recon application allows you to enroll OS X computers. Enrollment is the process of adding computers to the JSS. When OS X computers are enrolled, inventory information for the computers is submitted to the JSS, and the computers are managed.

Recon.exe

The Recon.exe application allows you to enroll Windows computers. Enrollment is the process of adding computers to the JSS. Enrolling Windows computers allows you to search and report on the computers as part of your inventory. Windows computers cannot be managed by the JSS.

Self Service

The Self Service application allows users to browse and run policies, access webpages, and utilize plug-ins developed with the Self Service API. Users can point-and-click their way through Self Service using an intuitive interface similar to iTunes.

You can make any policy available in Self Service and customize how it is displayed to users. You can also make two types of plug-ins available in Self Service: URL plug-ins and Self Service Plug-in bundles. URL plug-ins give users easy access to webpages right from the application. Self Service Plug-in bundles are custom plug-ins developed with the Self Service API.

Self Service Web Clip

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

By default, the Self Service web clip is installed on all managed mobile devices.

Ports

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

Port	Used for	Direction
22	The standard port for SSH (known as remote login in OS X). Default port used by Casper Remote and Recon to connect to computers.	Outbound from Casper Remote and Recon, and inbound to computers
80	The standard port for HTTP. When you use HTTP to deploy files, they are downloaded on this port.	Inbound to the distribution point, and outbound from computers
443	The standard port for HTTPS. When you use HTTPS to deploy files, they are downloaded on this port.	Inbound to the distribution point, and outbound from computers and mobile devices
548	The standard port for Apple File Protocol (AFP). If you use an AFP share to deploy files, computers mount the AFP share on this port.	Inbound to the share, and outbound from computers
3306	The default port used by the JSS to connect to MySQL.	Outbound from the JSS, and inbound to MySQL
8443	The SSL port for the JSS. Default port used by applications and computers and mobile devices to connect to the JSS.	Inbound to the JSS, and outbound from computers and mobile devices

The following table describes other commonly used ports:

Port	Used for	Direction
25	The standard port for SMTP. The JSS connects to an SMTP server to send email notifications to JSS users.	Outbound from the JSS, and inbound to the SMTP server
139	If you use an SMB share to deploy files, computers mount the SMB share on this port.	Inbound to the share, and outbound from computers
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.	Outbound from the JSS, and inbound to the LDAP server
636	The standard port for LDAPS. Any LDAP connections—even those coming from other applications—go through the JSS. This means that only the JSS connects to your LDAP server.	Outbound from the JSS, and inbound to the LDAP server
445	If you have an SMB client, such as "DAVE", installed on computers, they may mount the SMB share on this port.	Inbound to the share, and outbound from computers
514	The default port used by the JSS to write to Syslog servers.	Outbound from the JSS, and inbound to Syslog servers

Port	Used for	Direction
2195	The port used to send messages from the JSS to Apple Push Notification service (APNs).	Outbound from the JSS, and inbound to the APNs server
2196	The port used by the JSS to connect to APNs for feedback.	Outbound from the JSS, and inbound to the APNs server
5223	The port used to send messages from APNs to the mobile devices and computers in your network.	Outbound from computers and mobile devices, and inbound to the APNs server
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.	N/A
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.	N/A

On the Mac platform, the JSS runs on ports 8443 and 9006 by default. On Windows and Linux 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 managed computers and reset the passwords if necessary.

Passwords stored in the database are encrypted using a standard 256-bit AES encryption algorithm.

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 computers over Secure Shell (SSH), or Remote Login.

Secure Shell (SSH)

SSH is a network security protocol built into 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.

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 includes a preconfigured PKI that uses a built-in CA. The built-in CA is used by default to issue certificates to both computers and mobile devices.

You can also configure your own PKI if you have access to an external CA that supports SCEP. The external CA can be a CA hosted by your organization or by a trusted third-party vendor. If you integrate an external CA with the JSS, this CA will be used to issue certificates to mobile devices.

Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol (SCEP) obtains certificates from the CA and distributes them to managed mobile devices, providing a simplified way of handling large-scale certificate distribution.

The CA hosted by the JSS (the "built-in CA") supports SCEP. If you plan to use an external CA hosted by your organization or by a third-party vendor, this CA must support SCEP as well.

Certificates

The Casper Suite uses the following certificates to ensure security:

- **SSL Certificate—**The JSS requires a valid SSL certificate to ensure that computers and mobile devices communicate with the JSS and not an imposter server. The SSL certificate that you can create from the built-in CA secures communication using a 2048-bit RSA encryption.
- **Device Certificates**—Device certificates allow the JSS to verify the identity of OS X computers and mobile devices each time they communicate with the JSS.
- **CA Certificate**—This certificate establishes trust between the CA and OS X computers, and between the CA and mobile devices.
- **Signing Certificate—**This certificate is used to sign messages passed between the JSS and OS X computers, and between the JSS and mobile devices.
- **Push Certificate—**The JSS requires a valid push certificate to communicate with Apple Push Notification service (APNs).

Signed Applications

The following applications are signed by JAMF Software:

- Casper Admin
- Casper Imaging
- Casper Remote
- Composer
- jamf binary
- JAMF Helper
- JDS Installer for Mac
- Recon
- Recon.exe
- Self Service

Requirements

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

- JAMF Software Server (JSS)
- Package building
- Inventory
- Imaging
- Remote management
- Self Service
- Managing mobile devices
- Casper Focus
- JDS Installers

JAMF Software Server

You can host the JSS on any server that meets the following minimum requirements:

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

Tested operating systems include:

- OS X Server v10.7
- OS X Server v10.8
- OS X Server v10.9
- Ubuntu 10.04 LTS Server
- Ubuntu 12.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6
- Windows Server 2008 R2

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. For more information, see the JSS installation and configuration guide for your platform. These guides are available at:

http://www.jamfsoftware.com/product-documentation/installation-guides

Browser requirements for the JSS are as follows:

- Safari
- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 9 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
- OS X v10.9.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
- OS X v10.9.x
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Recon can enroll 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
- OS X v10.9.x

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

- OS v8.6
- 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

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
- OS X v10.9.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, OS X v10.8.x, or v10.9.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
- OS X v10.9.x

Managing Mobile Devices

The Casper Suite can be used to enroll and manage the following types of mobile devices:

- iPads with iOS 4 or later
- iPhones with iOS 4 or later
- iPod touches with iOS 4 or later
- Apple TV devices with iOS 7 or later

For information on the mobile device management capabilities available by device type and iOS version, see Mobile Device Management Capabilities.

Casper Focus

Casper Focus can run on teacher mobile devices with iOS 5.1.1 or later.

Student mobile devices that are assigned to classes in Casper Focus must have iOS 5.1.1 or later and must be managed by the Casper Suite v8.7 or later.

For information on feature-specific Casper Focus requirements for student mobile devices, see Preparing to Use Casper Focus.

JDS Installer for Mac

The JDS Installer for Mac requires a computer with:

- An Intel processor
- 2 GB of RAM
- 100 GB of disk space available
- OS X Server v10.7 or later
- Server.app 1.4.3 or later

JDS Installer for Linux

The JDS Installer for Linux requires a computer with:

- An Intel processor
- 2 GB of RAM
- 100 GB of disk space available
- One of the following operating systems:
  - Ubuntu 10.04 LTS Server
  - Ubuntu 12.04 LTS Server
  - Red Hat Enterprise Linux (RHEL) 6

Mobile Device Management Capabilities

The Casper Suite can be used to enroll and manage the following types of mobile devices:

- iPads with iOS 4 or later
- iPhones with iOS 4 or later
- iPod touches with iOS 4 or later
- Apple TV devices with iOS 7 or later

The following table provides an overview of the mobile device management capabilities available with the Casper Suite by device type and iOS version:

Device Type	iPad				iPhone				iPod touch				Apple TV	
iOS Version	4	5	6	7	4	5	6	7	4	5	6	7	7	
Enrollment														
Via user-initiated enrollment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Via an enrollment profile and Apple Configurator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Via an enrollment profile and Apple's iPCU	✓	✓	✓		✓	✓	✓		✓	✓	✓			
Inventory														
Submit inventory to the JSS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Mobile Device Groups														
Static groups	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Smart groups	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Configuration														
iOS configuration profiles	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓[1]	
iOS Remote Commands														
Update inventory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Lock device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Clear passcode	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Wipe device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Unmanage device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Send blank push	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Enable/disable voice or data roaming[2]		✓	✓	✓		✓	✓	✓						
Self Service														
Self Service web clip	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		

Device Type	iPad				iPhone				iPod touch				Apple TV	
iOS Version	**4**	**5**	**6**	**7**	**4**	**5**	**6**	**7**	**4**	**5**	**6**	**7**	**7**	
App Distribution														
Unmanaged apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Managed apps		✓	✓	✓		✓	✓	✓		✓	✓	✓		
In-house apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
App Store apps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
eBook Distribution														
Install ePub file	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Install iBooks file		✓	✓	✓										
Install PDF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Casper Focus[3]														
Focus on app			✓	✓			✓	✓			✓	✓		
Clear passcodes		✓	✓	✓		✓	✓	✓		✓	✓	✓		
Mirror device on Apple TV				✓				✓				✓		

Notes:

1. Wi-Fi, Certificate, SCEP, and Global HTTP Proxy are the only iOS configuration profile payloads that work on Apple TV devices.
2. iOS remote commands for voice or data roaming are only available for devices with cellular capability.
3. Management capabilities available for Casper Focus apply only to student mobile devices, not teacher devices.

Before You Begin

Setting Up the JSS

The first time you connect to the JAMF Software Server (JSS), the JSS Setup Assistant guides you through the following setup tasks:

- Accept the license agreement.
- Enter your activation code.
- Create your first JSS user account.
- Enter your JSS URL.

  The JSS URL is the URL that client applications, computers, and mobile devices will connect to when communicating with the JSS.

After you complete the JSS Setup Assistant, you can click the setup tips that are displayed onscreen to start configuring commonly used settings.

You may also want to make changes to the following preconfigured settings to ensure they meet the needs of your organization. These settings are important because over time, they can significantly affect the size of your database and your levels of network traffic:

- **"Update Inventory" policy—**Determines how often computers submit inventory to the JSS.

  For more information, see Computer Inventory Collection.
- **Recurring check-in frequency—**Determines the interval at which computers check in with the JSS for available policies.

  For more information, see Recurring Check-in Frequency.
- **Mobile device inventory collection frequency—**Determines how often mobile devices submit inventory to the JSS.

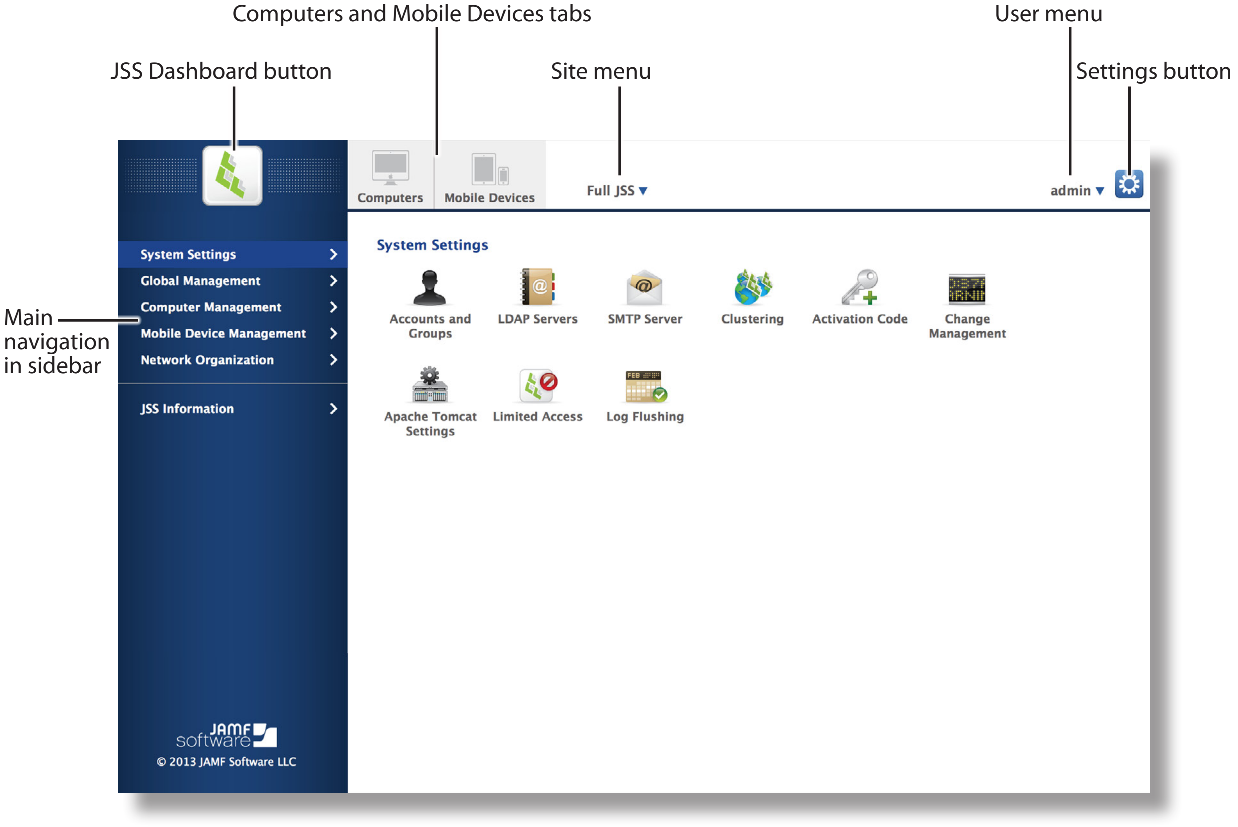
  For more information, see Mobile Device Inventory Collection Settings.

Viewing the JSS on Computers, Tablets, and Smartphones

The JAMF Software Server (JSS) interface automatically adjusts to the width of your web browser to provide the best possible display for the device on which it is viewed. This allows you to seamlessly transition from a computer to a tablet to a smartphone—all providing an optimal viewing experience so you can navigate the JSS with minimal scrolling and panning.

The screen shots below show examples of how navigational elements in the JSS are displayed when viewed on a computer, tablet, or smartphone.

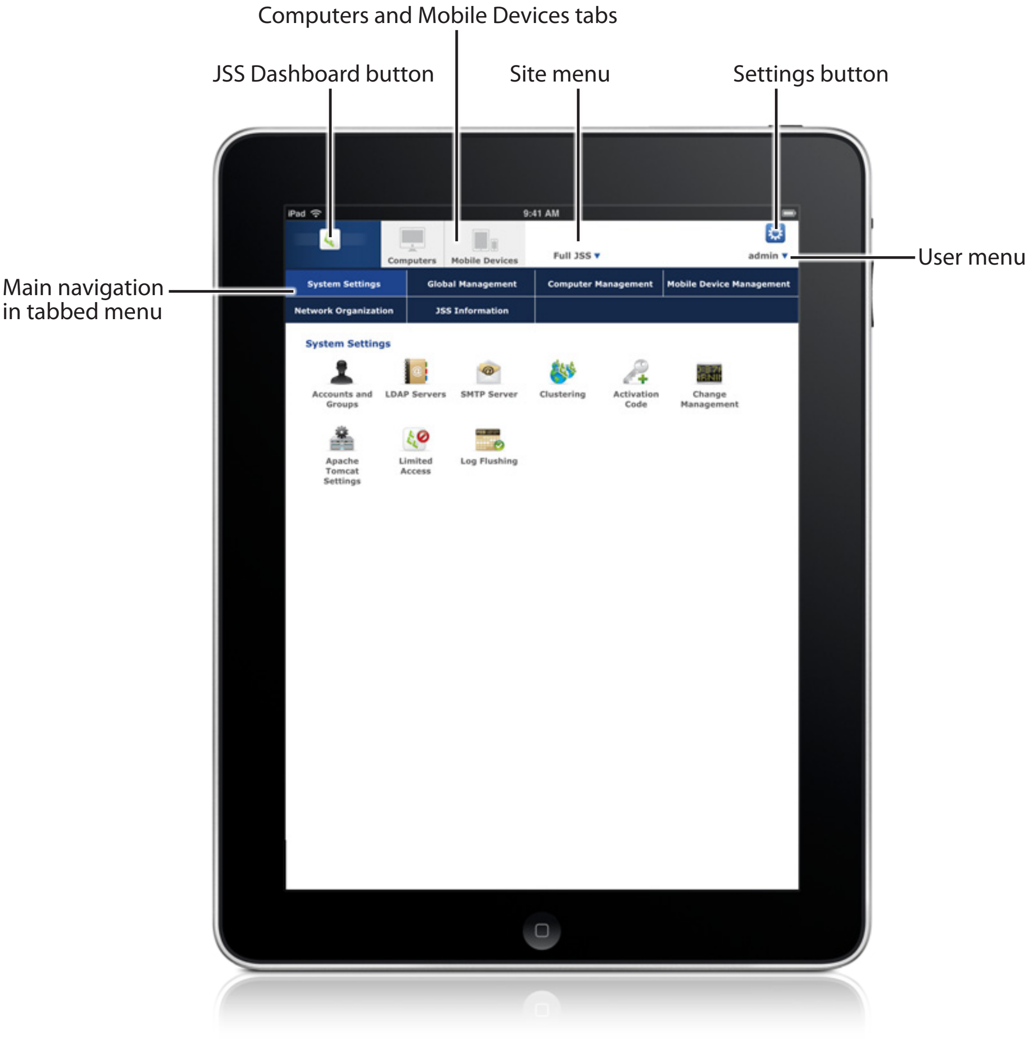
Computer Display



Note: When viewing the JSS on a computer, navigational elements display differently if the web browser is resized.

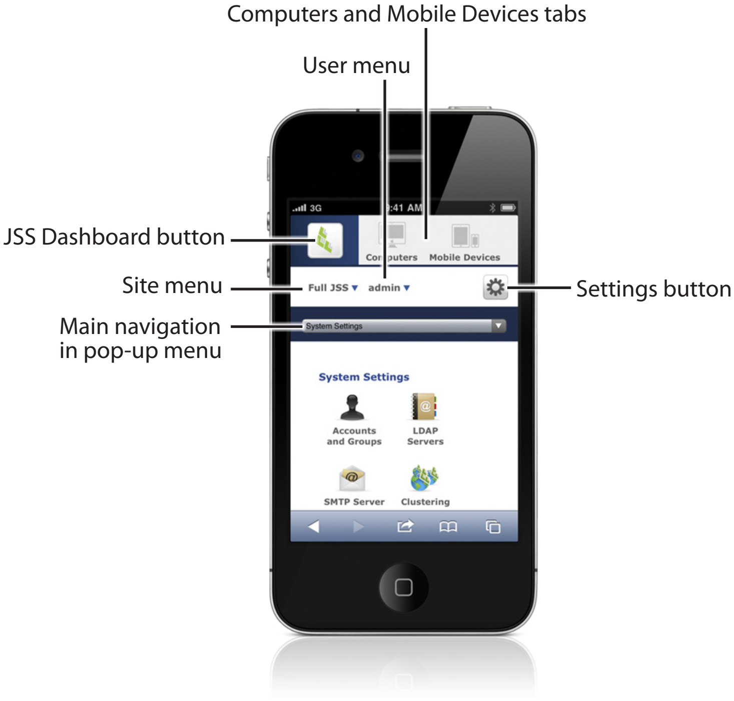
Tablet Display

The screen shot below shows the JSS displayed on a tablet in portrait orientation. For landscape orientation, the navigational elements display the same as they do in the computer view. (For more information, see Computer Display.)



Smartphone Display

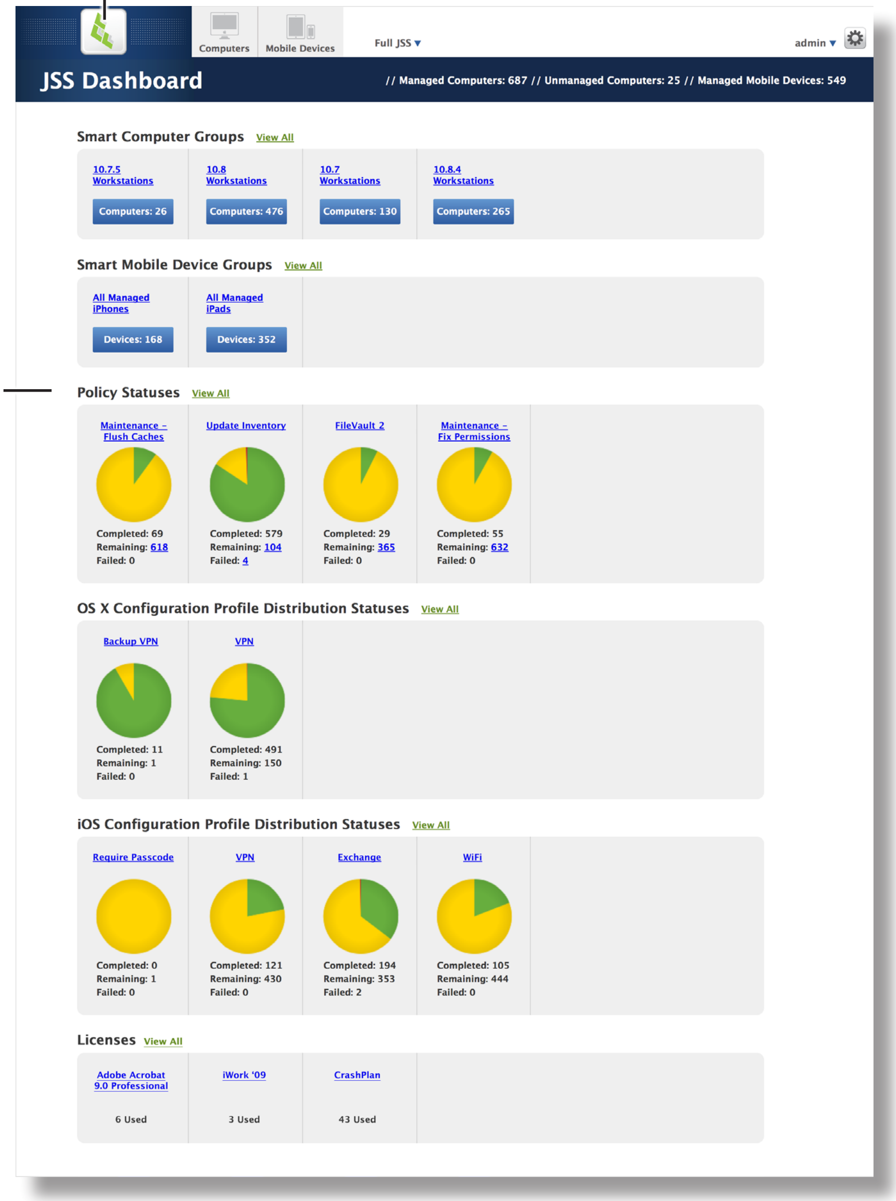
On a smartphone, the JSS navigational elements display the same for both landscape and portrait orientation.



The JSS Dashboard

The JSS Dashboard allows you to monitor the status of commonly viewed items in the JAMF Software Server (JSS), such as smart groups, policies, configuration profiles, and licensed software—all in one central location.

You can access the JSS Dashboard while using the JSS by clicking the **JSS Dashboard** button in the top-left corner of the page.



JSS Dashboard button

JSS Dashboard

JSS Dashboard

// Managed Computers: 687 // Unmanaged Computers: 25 // Managed Mobile Devices: 549

Smart Computer Groups View All

10.7.5 Workstations	10.8 Workstations	10.7 Workstations	10.8.4 Workstations
Computers: 26	Computers: 476	Computers: 130	Computers: 265

Smart Mobile Device Groups View All

All Managed iPhones	All Managed iPads
Devices: 168	Devices: 352

Policy Statuses View All

Maintenance – Flush Caches	Update Inventory	FileVault 2	Maintenance – Fix Permissions
Completed: 69 Remaining: 618 Failed: 0	Completed: 579 Remaining: 104 Failed: 4	Completed: 29 Remaining: 365 Failed: 0	Completed: 55 Remaining: 632 Failed: 0

OS X Configuration Profile Distribution Statuses View All

Backup VPN	VPN
Completed: 11 Remaining: 1 Failed: 0	Completed: 491 Remaining: 150 Failed: 1

iOS Configuration Profile Distribution Statuses View All

Require Passcode	VPN	Exchange	WiFi
Completed: 0 Remaining: 1 Failed: 0	Completed: 121 Remaining: 430 Failed: 0	Completed: 194 Remaining: 353 Failed: 2	Completed: 105 Remaining: 444 Failed: 0

Licenses View All

Adobe Acrobat 9.0 Professional	iWork '09	CrashPlan
6 Used	3 Used	43 Used

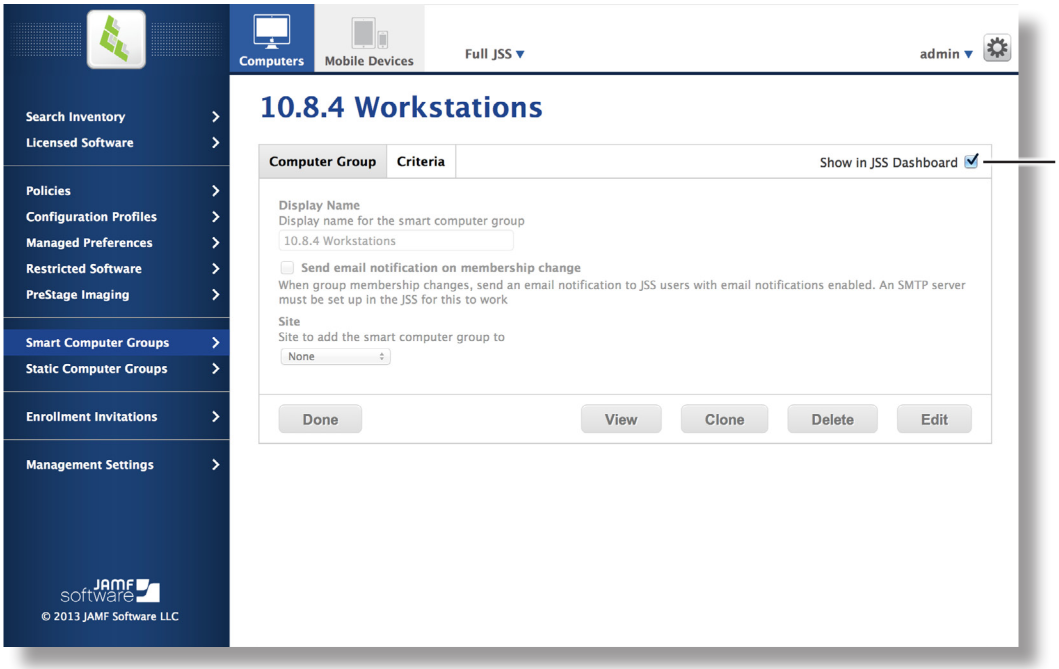
Note: Until you add one or more items to the JSS Dashboard, it displays setup tips that you can use to configure commonly used settings.

Adding Items to the JSS Dashboard

You can add the following types of items to the JSS Dashboard:

- Smart computer groups
- Smart mobile device groups
- Policies
- OS X configuration profiles
- iOS configuration profiles
- Licensed software

To add an item to the JSS Dashboard, select the **Show in JSS Dashboard** checkbox in the upper-right corner of the pane when viewing the item in the JSS.



10.8.4 Workstations

Show in JSS Dashboard ☑

Display Name
Display name for the smart computer group
10.8.4 Workstations

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

Site
Site to add the smart computer group to
None

Show in JSS Dashboard checkbox

JSS System Settings

JSS User Accounts and Groups

The JAMF Software Server (JSS) is a multi-user application. JSS user accounts and groups allow you to grant different privileges and levels of access to each user.

When configuring a JSS user account or group, you can grant access to the full JSS or to a specific site. You can grant privileges by choosing one of the following privilege sets:

- **Administrator**—Grants all privileges.
- **Auditor**—Grants all read privileges.
- **Enrollment Only**—Grants all privileges required to enroll computers and mobile devices.
- **Custom**—Requires you to grant privileges manually.

If there are multiple users that should have the same access level and privileges, you can create a group with the desired access level and privileges and add accounts to it. Members of a group inherit the access level and privileges from the group. Adding an account to multiple groups allows you to grant a user access to multiple sites.

There are two ways to create JSS user accounts and groups: you can create standard accounts or groups, or you can add them from an LDAP directory service.

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

Requirements

To add accounts or groups from an LDAP directory service, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

Creating a JSS User Group

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Accounts and Groups** 👤 .
5. Click **New** + .
6. Do one of the following:
   - To create a standard JSS user group, select **Create Standard Group** and click **Next**.
   - To add a JSS user group from an LDAP directory service, select **Add LDAP Group** and click **Next**. Then follow the onscreen instructions to search for and add the group.

7. Use the Group pane to configure basic settings for the group.

8. If you chose "Custom" from the **Privilege Set** pop-up menu, click the **Privileges** tab and select the checkbox for each privilege that you want to grant the group.

9. Click **Save**.

Creating a JSS User Account

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

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

   On a smartphone, this option is in the pop-up menu.

4. Click **Accounts and Groups** 👤 .

5. Click **New** + .

6. Do one of the following:

   - To create a standard JSS user account, select **Create Standard Account** and click **Next**.
   - To add a JSS user account from an LDAP directory service, select **Add LDAP Account** and click **Next**. Then follow the onscreen instructions to search for and add the account.

7. On the Account pane, enter information about the account as needed.

8. Choose an access level from the **Access Level** pop-up menu:

   - To grant full access to the JSS, choose "Full Access".
   - To grant access to a site, choose "Site Access".

> ***Note:*** The "Site Access" option is only displayed if there are sites in the JSS. For more information on adding sites to the JSS, see Sites.

   - To add the account to a standard group, choose "Group Access".

> ***Note:*** The "Group Access" option is only displayed if there are standard groups in the JSS. For more information on creating groups, see Creating a JSS User Group.

9. Do one of the following:

   - If you granted the account full access or site access, choose a privilege set from the **Privilege Set** pop-up menu. Then, if you chose "Custom", click the **Privileges** tab and select the checkbox for each privilege that you want to grant the account.
   - If you added the account to a group, click the **Group Membership** tab and select the group(s) you want to add the account to.

10. Click **Save**.

Cloning, Editing, or Deleting a JSS User Account or Group

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Accounts and Groups** .
5. Click the JSS user account or group you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the account or group, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the account or group, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the account or group, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Sites
Learn about sites and how to add them to the JSS.

Integrating with LDAP Directory Services

Integrating with an LDAP directory service allows you to do the following:

- Look up and populate user information from the directory service for inventory purposes.
- Add JSS user accounts or groups from the directory service.
- Require users to log in to Self Service or the enrollment portal using their LDAP directory accounts.
- Base the scope of remote management tasks on users or groups from the directory service.

To integrate with an LDAP directory service, you need to add the LDAP server to the JAMF Software Server (JSS). There are two ways to add LDAP servers to the JSS: using the LDAP Server Assistant or manually.

The LDAP Server Assistant guides you through the process of entering information about the LDAP server and ensuring that LDAP attributes are mapped properly. It allows you to integrate with the following directory services:

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

Manually adding an LDAP server involves entering detailed information about the LDAP server and manually configure attribute mappings. This allows you to integrate with LDAP additional directory services.

Adding an LDAP Server Using the LDAP Server Assistant

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **LDAP Servers** @.
5. Click **New** +.
6. Follow the onscreen instructions to add the LDAP server.

Manually Adding an LDAP Server

Before manually adding an LDAP server, 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 Assistant to ensure that attributes are mapped correctly.

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

2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **LDAP Servers**.
5. Click **New** +.
6. Select **Configure Manually** and click **Next**.
7. Use the Connection pane to configure how the JSS connects to the LDAP server.
8. Use the Mappings pane to specify object class and search base data, and map attributes.
9. Click **Save**.

Cloning, Editing, or Deleting an LDAP Server

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **LDAP Servers**.
5. Click the LDAP server you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the LDAP server, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the LDAP server, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the LDAP server, click **Delete** and then click **Delete** again to confirm.

Testing LDAP Attribute Mappings

You can test the following LDAP attribute mappings:

- User mappings
- User group mappings
- User group membership mappings

If the JSS returns the appropriate information, the attributes are mapped correctly.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.

3. Click **System Settings**.

   On a smartphone, this option is in the pop-up menu.

4. Click **LDAP Servers** .

5. Click the LDAP server you want to test.

6. Click **Test**.

7. Click the appropriate tab and enter information in the field(s) provided.

8. Click **Test** again.

Related Information

For related information, see the following sections in this guide:

- JSS User Accounts and Groups

  Find out how to add JSS user accounts or groups from an LDAP directory service.

- User Authentication Settings for Self Service

  Find out how to require users to log in to the Self Service application using their LDAP directory accounts.

- Self Service Web Clip

  Find out how to require users to log in to the Self Service web clip using their LDAP directory accounts.

- User-Initiated Enrollment for Computers

  Find out how to require users to log in to the enrollment portal using their LDAP directory accounts before enrolling their computers.

- User-Initiated Enrollment for Mobile Devices

  Find out how to require users to log in to the enrollment portal using their LDAP directory accounts before enrolling their mobile devices.

- Scope

  Learn how to configure scope based on users or groups from an LDAP directory service.

For related information, see the following Knowledge Base article:

Configuring the JSS to Use LDAP Over SSL When Authenticating with Active Directory
Find out how to configure the JSS to perform authentication with Active Directory using LDAP over SSL (LDAPS).

Integrating with an SMTP Server

Integrating with an SMTP server allows you to do the following:

- Send email notifications to JAMF Software Server (JSS) users when certain events occur.
- Send enrollment invitations via email.
- Send mass emails to end users.

To integrate with an SMTP server, you need to configure the SMTP Server settings in the JSS.

Configuring the SMTP Server Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **SMTP Server** ✉ .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Testing the SMTP Server Settings

Once the SMTP Server settings are configured, you can send a test email from the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **SMTP Server** ✉ .
5. Click **Test**.
6. Enter a test email address and click **Test** again.

A message displays, reporting whether or not the email was sent successfully.

Related Information

For related information, see the following sections in this guide:

- Email Notifications

  Learn about the different email notifications that can be sent JSS users.

- User-Initiated Enrollment for Computers

  Find out how to send computer enrollment invitations via email.

- User-Initiated Enrollment for Mobile Devices

  Find out how to send mobile device enrollment invitations via email.

- Sending a Mass Email to Computer Users

  Find out how to send a mass email to computer users.

- Sending a Mass Email to Mobile Device Users

  Find out how to send a mass email to mobile device users.

Email Notifications

Email notifications can be sent from the JAMF Software Server (JSS) to JSS users when the following events occur:

- A computer is enrolled using a PreStage.
- An error occurs during imaging.
- An error occurs while a policy is running.
- A restricted software violation occurs.

Note: For this to work, email notifications must also be enabled for the individual restricted software records. (For more information, see Restricted Software.)

- The license limit for a licensed software record is exceeded.

Note: For this to work, email notifications must also be enabled for the individual licensed software records. (For more information, see Licensed Software Records.)

- Smart computer group membership changes.
- Smart mobile device group membership changes.
- Tomcat is started or stopped.
- The database is backed up successfully.
- A database backup fails.
- The JSS fails to add a file to a JDS instance or the cloud distribution point.

Each JSS user can choose which email notifications they want to receive.

Requirements

To enable email notifications, you need:

- An SMTP server set up in the JSS (For more information, see Integrating with an SMTP Server.)
- An email address specified for the JSS user account you want to enable email notifications for (For more information, see JSS User Accounts and Groups.)

Enabling Email Notifications

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

2. At the top of the page, click the disclosure triangle next to your username and then click **Email Notifications**.

3. Select the checkbox for each event that you want to receive email notifications for.

4. Click **Save**.

Activation Code

The Activation Code settings in the JAMF Software Server (JSS) allow you to update the activation code for your license. You can also change the organization name associated with the license and view licensing information.

Updating the Activation Code

Every time you receive a new activation code, it must be updated in the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Activation Code** 🔑.
5. Click **Edit**.
6. Enter the new activation code.
7. Click **Save**.

Change Management

Change Management allows you to track the following information:

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

The Change Management settings in the JAMF Software Server (JSS) allow you to log this information to a log file on the JSS host server and/or to a syslog server.

Logging changes to a log file stores them in a file named `jamfChangeManagement.log` on the JSS host server.

Requirements

To log changes to a log file, the account used to run Tomcat must have write permissions for the directory where the `jamfChangeManagement.log` file is located.

Configuring the Change Management Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Change Management** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Related Information

For related information, see the following Knowledge Base article:

Change Management with the Casper Suite: Mac OS X Setup Guide
If you are hosting the JSS on OS X Server, learn about setting up the syslogd utility so you can log changes to a syslog server.

SSL Certificate

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

The Apache Tomcat settings in the JSS allow you to create an SSL certificate from the CA that is built into the JSS. You can also upload the certificate keystore for an SSL certificate that was obtained from an internal certificate authority (CA) or a trusted third-party vendor.

Requirements

To create or upload an SSL certificate, 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.

Creating or Uploading an SSL Certificate

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **System Settings**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Apache Tomcat Settings** .
5. Click **Edit**.
6. Select **Change the SSL certificate used for HTTPS** and click **Next**.
7. Follow the onscreen instructions to upload or create an SSL certificate.
8. Restart Tomcat for the changes to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   Starting and Stopping Tomcat

Related Information

For related information, see the following Knowledge Base article:

Using OpenSSL to Create a Certificate Keystore for Tomcat
Find out how to use OpenSSL to create a certificate keystore that you can upload to the JSS.

Flushing Logs

Flushing logs reduces the size of the database and can speed up searches. You can flush the following types of logs:

- Application Usage logs
- Computer Usage logs
- Policy logs
- Casper Remote logs
- Screen sharing logs
- Casper Imaging logs
- Computer and mobile device management history
- JDS management history
- Computer inventory reports (computer inventory information from past inventory submissions)
- Mobile device inventory reports (mobile device inventory information from past inventory submissions)

You can schedule log flushing to take place daily, or you can manually flush logs as needed. You can also choose to flush logs that are older than a certain number of days, weeks, or months.

Scheduling Log Flushing

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **System Settings**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Log Flushing** .
5. Click **Edit**.
6. Use the pop-up menus to choose the number of days, weeks, or months after which each type of log should be flushed.
7. Choose a time of day from the **Time to Flush Logs Each Day** pop-up menu.
8. Click **Save**.

Manually Flushing Logs

1. Log in to any of the JSS web applications with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

   On a smartphone, this option is in the pop-up menu.

4. Click **Log Flushing** .

5. Click **Flush Manually**.

6. Select the checkbox for each type of log you want to flush.

7. From the **Flush Logs Older Than** pop-up menu, choose the choose the number of days, weeks, or months after which logs should be flushed.

8. Click **Flush**.

   A message displays, reporting the success or failure of the flush.

Related Information

For related information, see the following sections in this guide:

- Viewing and Flushing Policy Logs for a Single Computer

  Find out how to view and flush policy logs for a single computer.

- Viewing and Flushing Logs for a Single Policy

  Find out how to view and flush logs for a single policy.

- Viewing the History for a Single Computer

  Find out how to view the logs and the management history for a single computer.

- Viewing Management History for a Single Mobile Device

  Find out how to view the management history for a single mobile device.

JSS Summary

The JSS Summary is a custom report that allows you to view information about your JAMF Software Server (JSS). The JSS Summary can be useful for troubleshooting JSS issues, and for providing information to JAMF Software for purposes of support or license renewal.

By default, the JSS Summary includes the following information about the JSS:

- Number of managed and unmanaged computers
- Number of managed mobile devices
- Operating system on the JSS host server
- Path to the JSS web application
- Apache Tomcat version
- Information about the version of Java installed on the JSS host server
- Information about the MySQL connection and configuration

You can also add information to the JSS Summary from the following categories as needed:

- Computers
- Mobile Devices
- System Settings
- Global Management
- Computer Management
- Computer Management–Server Infrastructure
- Computer Management–Management Framework
- Mobile Device Management
- Network Organization
- Database

You can view the JSS Summary in a browser window or send the JSS Summary to JAMF Software.

Requirements

To send the JSS Summary to JAMF Software, you need a valid JAMF Nation account.

To create a JAMF Nation account, go to:

https://jamfnation.jamfsoftware.com/createAccount.html

Viewing the JSS Summary

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **JSS Information.**
   On a smartphone, this option is in the pop-up menu.
4. Click **JSS Summary** 📋.

5. Select the checkboxes next to the items you want to include.
6. Click **Create**.
   The JSS Summary displays in a browser window.
7. Click the **Back** button in the web browser to return to the JSS Summary pane in the JSS.

Sending the JSS Summary to JAMF Software

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **JSS Information**.
   On a smartphone, this option is in the pop-up menu.
4. Click **JSS Summary** 📋 .
5. Select the checkboxes next to the items you want to include.
6. Click **Send Summary to JAMF Software**.
7. Enter your JAMF Nation credentials, and then click **Send**.

   The JSS Summary is sent to JAMF Software via JAMF Nation.

Global Management Settings

Push Certificates

The JAMF Software Server (JSS) requires a valid push certificate to communicate with Apple Push Notification service (APNs). This communication is required do the following:

- Send OS X configuration profiles and OS X remote commands to computers.
- Enroll and manage mobile devices.

An assistant in the JSS guides you through the following steps to create a new push certificate (.pem) and upload it to the JSS:

1. Obtain a signed certificate request (CSR) from JAMF Nation.
2. Create the push certificate in Apple's Push Certificates Portal by logging into the portal, uploading the signed CSR obtained from JAMF nation, and downloading the resulting push certificate.
3. Upload the push certificate to the JSS.

If you have a push certificate in .p12 format, you do not have to create a new one. You can simply upload the .p12 file to the JSS.

You can also use the JSS to renew your push certificate when needed.

Requirements

To create or renew a push certificate, you need:

- A valid JAMF Nation account

  To create a JAMF Nation account, go to:

  https://jamfnation.jamfsoftware.com/createAccount.html
- A valid Apple ID (A corporate Apple ID is recommended.)

  If you are renewing a push certificate that was originally obtained from Apple's iOS Developer Program (iDEP), you must use the Apple ID for the iDEP Agent account used to obtain the certificate.

Creating a Push Certificate

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Push Certificates** ☁.

5. Click **New** + and do one of the following:
   - If the server hosting the JSS has an outbound connection, select **Download signed CSR from JAMF Nation**.

     The JSS connects to JAMF Nation over port 443 and obtains the signed CSR.
   - If the server hosting the JSS does not have an outbound connection, select **Download CSR and sign later using JAMF Nation**.
6. Follow the onscreen instructions to create and upload the push certificate (.pem).

Uploading a Push Certificate (.p12)

If you have a push certificate that's in .p12 format, you can upload it to the JSS.

> ***Note:*** You will only have a push certificate in .p12 format if the CSR used to create the certificate was not issued by the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Push Certificates** ☁.
5. Click **New** +.
6. Select **Upload push certificate (.p12)**.
7. Follow the onscreen instructions to upload the push certificate.

Renewing the Push Certificate

> ***Important:*** It is recommended that you do not delete the existing push certificate from the JSS when renewing a push certificate.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Push Certificates** ☁.
5. Click the push certificate and then click **Renew**.

6. Choose a method for renewing the push certificate:
   - If the server hosting the JSS has an outbound connection, select **Download signed CSR from JAMF Nation**.

     The JSS connects to JAMF Nation over port 443 and obtains the signed CSR.
   - If the server hosting the JSS does not have an outbound connection, select **Download CSR and sign later using JAMF Nation**.
   - If you have a new push certificate in .p12 format, select **Upload push certificate (.p12)**.
7. Follow the onscreen instructions to renew the push certificate.

Deleting the Push Certificate

Deleting the push certificate from the JSS disables communication between the JSS and APNs. This prevents the JSS from sending OS X configuration profiles and OS X remote commands to computers and managing mobile devices. To restore these capabilities, you must create a new push certificate, and then re-enroll your computers and mobile devices with the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Push Certificates** .
5. Click the push certificate and click **Delete.** Then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Security Settings

  Find out how to enable certificate-based authentication and push notifications so you can send OS X configuration profiles and OS X remote commands to managed computers.
- Public Key Infrastructure

  Learn how to configure the public key infrastructure (PKI) to ensure secure communication with APNs.
- Ports

  Find out which ports the JSS uses to communicate with APNs.

Integrating with GSX

Integrating with Apple's Global Service Exchange (GSX) allows you to look up and populate the following purchasing information for computers and mobile devices:

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

> ***Note:*** GSX may not always return complete purchasing information. Only the information found in GSX is returned.

To integrate with GSX, you need to configure the GSX Connection settings in the JSS.

Requirements

To configure the GSX Connection settings, you need a GSX account with the "Manager" role and access to Web Services. (For information, see the Integrating with Apple's Global Service Exchange (GSX) Knowledge Base article.)

Configuring the GSX Connection Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.
   On a smartphone, this option is in the pop-up menu.
4. Click **GSX Connection** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Testing the GSX Connection

Once the GSX Connection settings are configured, you can test the connection.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.

4. Click **GSX Connection** .

5. Click **Test**.

6. Click **Test** again.

   A message displays, reporting the success or failure of the connection.

Related Information

For related information, see the following sections in this guide:

- Mass Looking up and Populating Purchasing Information for Computers

  Find out how to mass look up and populate purchasing information for computers from GSX.

- Mass Looking up and Populating Purchasing Information for Mobile Devices

  Find out how to mass look up and populate purchasing information for mobile devices from GSX.

- Viewing and Editing Inventory Information for a Single Computer

  You can look up and populate purchasing information for a single computer by editing the computer's inventory information in the JSS.

- Viewing and Editing Inventory Information for a Single Mobile Device

  You can look up and populate purchasing information for a single mobile device by editing the device's inventory information in the JSS.

- Local Enrollment Using Recon

  Find out how to look up and populate purchasing information when enrolling a computer by running Recon locally.

- Remote Enrollment Using Recon

  Find out how to look up and populate purchasing information when enrolling a computer by running Recon remotely.

JSS URL

The JSS URL is the URL that client applications, computers, and mobile devices connect to when communicating with the JAMF Software Server (JSS). You can view and configure the JSS URL in the JSS.

> ***Important:*** In general, you should not change the JSS URL in a production environment with managed computers and mobile devices. If the JSS URL is incorrect or not specified, client applications, computers, and mobile devices are unable to connect to the server.

You can also view or configure the JSS URL that's used for enrolling mobile devices with an enrollment profile and Apple's iPhone Configuration Utility (iPCU).

Viewing or Configuring the JSS URLs

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **JSS URL** .

   The JSS URLs are displayed on the pane.
5. To configure the JSS URLs:
   a. Click **Edit**.
   b. Enter the new URLs in the fields on the pane.
   c. Click **Save**.

Related Information

For related information, see the following section in this guide:

Enrollment Profiles
Find out how to create and downlaod enrollment profiles so you can enroll mobile devices by connecting them to a computer via USB.

Public Key Infrastructure

To ensure secure communication with the Apple Push Notification service (APNs), the JAMF Software Server (JSS) requires a public key infrastructure (PKI) that supports certificate-based authentication. The PKI must include the following components:

- A certificate authority (CA) that supports Simple Certificate Enrollment Protocol (SCEP)
- A signing certificate
- A CA certificate

For more information on the PKI and its components, see Security.

The JSS includes a preconfigured PKI that uses a built-in CA with support for SCEP. There is no configuration necessary to use the built-in CA—the signing and CA certificates are created and stored for you. The built-in CA is used by default to issue certificates to both computers and mobile devices.

You can use the PKI settings in the JSS to perform the following tasks related to the built-in CA:

- Download the CA certificate.
- View and revoke certificates issued by the built-in CA.
- Create a certificate using a Certificate Signing Request (CSR).
- Create a backup of the CA certificate.

You can also configure your own PKI if you have access to an external CA that supports SCEP. The external CA can be a CA hosted by your organization or by a trusted third-party vendor. If you integrate an external CA with the JSS, this CA will be used to issue certificates to mobile devices.

Downloading the CA Certificate

You can use the PKI settings in the JSS to download the CA certificate issued by the built-in CA.

Note: The CA certificate issued by the built-in CA is also stored in the System keychain in Keychain Access.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **PKI** .
5. On the **Built-in CA** pane, click **Download CA Certificate**.

   The certificate (.pem) downloads immediately.

Viewing or Revoking Certificates

You can view the following information for a certificate issued by the built-in CA:

- Serial number
- Subject name
- Date/time issued
- Expiration date/time
- Status
- Date/time revoked (if applicable)

You can also revoke a certificate issued by the built-in CA.

> ***Warning:*** Revoking a certificate stops communication between the JSS and the computer or mobile device that the certificate was issued to. You will need to re-enroll the computer or device to restore communication.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.
   On a smartphone, this option is in the pop-up menu.
4. Click **PKI** .
5. On the **Built-in CA** pane, click **Issued Certificates**.
   A list of certificates issued by the built-in CA is displayed.
6. Click the serial number of the certificate you want to view or revoke.
   Information about the certificate is displayed.
7. To revoke the certificate, click **Revoke**.
   The status of the certificate is changed to Revoked.
8. Click **Done** twice to return to the **Built-in CA** pane.

Manually Creating a Certificate from a CSR

Depending on your environment, you may need to manually create a certificate from a certificate signing request (CSR). For example, you may need to do this if you have a clustered environment with Tomcat configured for working behind a load balancer. You can create this certificate using the PKI settings in the JSS.

> ***Note:*** The certificate created from the CSR is intended solely for purposes of communication between the JSS and a managed computer or mobile device.

To create a certificate from a CSR, you need a request in Base64-encoded PEM format.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **PKI** .
5. On the **Built-in CA** pane, click **Create Certificate from CSR**.
6. In the **CSR** field, paste the CSR.

   The request must begin with

   ----BEGIN CERTIFICATE REQUEST----

   and end with

   ----END CERTIFICATE REQUEST----
7. Click **Create**.

   The certificate (.pem) is downloaded immediately.
8. Click **Back** to return to the **Built-in CA** pane.

Creating a Backup of the CA Certificate

It is recommended that you create a password-protected backup of the CA certificate issued by the built-in CA and store it in a secure location.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **PKI** .
5. On the **Built-in CA** pane, click **Create CA Backup**.
6. Create and verify a password to secure the backup CA certificate.

   You will need to enter this password to restore the certificate backup.
7. Click **Create Backup**.

   The backup file (.p12) is downloaded immediately.
8. Click **Back** to return to the **Built-in CA** pane.

Integrating with an External CA

If you are using an organizational or third-party CA that supports SCEP, you can use it to issue management certificates to mobile devices.

> ***Note:*** The external CA will be used for issuing certificates to mobile devices only. The built-in CA will be used to issue certificates to computers.

Integrating an external CA with the JSS involves the following steps:

- Specify SCEP parameters for the external CA.
- Upload a signing certificate and CA certificate for the external CA.

Specifying SCEP Parameters for an External CA

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **PKI** .
5. Click the **External CA** tab.
6. Click **Edit**.
7. Select the **Use External Certificate Authority** checkbox.
8. Use the **External CA** pane to specify SCEP parameters.
9. Choose the type of challenge password to use from the **Challenge Type** pop-up menu:
   - If you want all mobile devices to use the same challenge password, choose "Static" and specify a challenge password.

     The challenge password will be used as the pre-shared secret for automatic enrollment.
   - If you are using a non-Microsoft CA and you want each mobile device to use a unique challenge password, choose "Dynamic".

     The Dynamic challenge type 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 are using a Microsoft CA and you want each mobile device to use a unique challenge password, choose "Dynamic-Microsoft CA".

> ***Note:*** If you choose the "Dynamic" or "Dynamic-Microsoft CA" challenge type, you must use user-initiated enrollment to enroll mobile devices so that a unique challenge password is used for each device. For more information, see User-Initiated Enrollment for Mobile Devices.

10. Click **Save**.

Uploading Signing and CA Certificates for an External CA

To integrate an external CA with the JSS, you need to provide the signing and CA certificates for the external CA. This is done by uploading a signing certificate keystore (.jks or .p12) to the JSS that contains both certificates.

> ***Note:*** By default, the JSS uses the signing and CA certificates for the JSS's built-in CA. You must replace these certificates with the ones for the external CA when you initially set up the integration.

An assistant guides you through the process of uploading the keystore that contains the signing and CA certificates.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Global Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **PKI** .
5. Click the **External CA** tab.
6. At the bottom of the **External CA** pane, click **Change Signing and CA Certificates.**
7. Follow the onscreen instructions to upload the signing and CA certificates for the external CA.

Related Information

For related information, see the following section in this guide:

Push Certificates
Learn how to create a push certificate and upload it to the JSS so the JSS can communicate with Apple Push Notification service (APNs).

For related information, see the following Knowledge Base articles:

- Certificate-Based Authentication for OS X Computers

  Learn how the JSS uses certificate-based authentication to verify the identity of OS X computers.
- Using OpenSSL to Create a Certificate Keystore for Tomcat

  Find out how to use OpenSSL to create a certificate keystore that you can upload to the JSS.

Server Infrastructure

About Distribution Points

Distribution points are servers used to host files for distribution to computers and mobile devices. The following types of files can be distributed from a distribution point using the Casper Suite:

- Packages
- Scripts
- In-house apps
- In-house eBooks

The Casper Suite supports three types of distribution points:

- File share distribution points
- A cloud distribution point
- JAMF Distribution Server (JDS) instances

You can use any combination of these types of distribution points.

By default, the first distribution point you add to the JAMF Software Server (JSS) is the master distribution point. The master distribution point is used by all other distribution points as the authoritative source for all files during replication. You can change the master distribution point at any time.

When planning your distribution point infrastructure, it is important to understand the differences between each type of distribution point. The following table explains the key differences:

	File Share Distribution Point	**Cloud Distribution Point**	**JDS Instance**
Description	Standard server that is configured to be a distribution point	Distribution point that uses one of the following cloud services to host files: • Rackspace Cloud Files • Amazon Web Services (S3 and CloudFront) • Akamai	Distribution point that is managed by the JSS, similar to a computer or mobile device
Maximum Number per JSS	Unlimited	One	Unlimited
Server/Platform Requirements	Any server with an Apple Filing Protocol (AFP) or Server Message Block (SMB) share	None	OS X or Linux
Protocol	AFP, SMB, HTTP, or HTTPS	HTTPS	HTTPS
Ports	• AFP: 548 • SMB: 139 • HTTP: 80 • HTTPS: 443	443	443

	File Share Distribution Point	**Cloud Distribution Point**	**JDS Instance**
Authentication Options	• AFP or SMB: • No authentication • Username and password • HTTP or HTTPS: • No authentication • Username and password • Certificate-based authentication	None	• No authentication • Certificate-based authentication
Files that Can Be Hosted	• Packages • Scripts	• Packages • In-house apps • In-house eBooks ***Note:*** If you use the cloud distribution point, scripts are stored in the jamfsoftware database.	• Packages • In-house apps • In-house eBooks ***Note:*** If you use one or more JDS instances, scripts are stored in the jamfsoftware database.
Parent-Child Capabilities	No	No	Yes
File Replication Method	Replication to file share distribution points must be initiated from Casper Admin.	Replication to file share distribution points must be initiated from Casper Admin.	Replication to root JDS instances must be initiated from Casper Admin. Replication to non-root JDS instances happens automatically and immediately.
Selective Replication	Not available when replicating to file share distribution points.	Not available when replicating to file share distribution points.	Not available when replicating to root JDS instances. Available when replicating to non-root JDS instances.

Related Information

For related information, see the following sections in this guide:

- File Share Distribution Points

  Find out how to manage file share distribution points in the JSS.
- Cloud Distribution Point

  Find out how to manage the cloud distribution point.
- JAMF Distribution Server Instances

  Find out how to install and manage JDS instances.

File Share Distribution Points

Any server with an AFP or SMB share can be used as a file share distribution point. Before you can use a file share distribution point with the Casper Suite, you must set up the distribution point and add it to the JAMF Software Server (JSS).

For information on setting up a file share distribution point, see the following Knowledge Base article:

Setting Up a File Share Distribution Point

When you add a file share distribution point to the JSS, you can do the following:

- Make it the master distribution point.
- Choose a failover distribution point.
- Configure HTTP downloads.

Adding a File Share Distribution Point

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **File Share Distribution Points** .
5. Click **New** + .
6. Use the General pane to configure basic settings for the distribution point.
7. Click the **File Sharing** tab and enter information about the AFP or SMB share.
8. (Optional) Click the **HTTP** tab and configure HTTP downloads.
9. Click **Save**.

Cloning, Editing, or Deleting a File Share Distribution Point

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **File Share Distribution Points** .

5. Click the distribution point you want to clone, edit, or delete.

6. Do one of the following:
   - To clone the distribution point, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the distribution point, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the distribution point, click **Delete** and then click **Delete** again to confirm.

Replicating Files to a File Share Distribution Point

During replication, all files on the master distribution point are replicated to the file share distribution point that you choose.

1. Open Casper Admin and authenticate to the JSS.

2. In the sidebar, select the file share distribution point you want to replicate files to.

3. Click **Replicate**.

Related Information

For related information, see the following section in this guide:

Network Segments
You can use network segments to ensure that computers and mobile devices use the closest distribution point by default.

For related information, see the following Knowledge Base articles:

- Setting Up a File Share Distribution Point on Linux Using Samba

  Find out how to use Samba to set up a file share distribution point with an SMB share on a Linux server.
- Using Apache HTTP Server to Enable HTTP Downloads on a Linux File Share Distribution Point

  Find out how to use Apache HTTP Server to enable HTTP downloads on a Linux file share distribution point.
- Using IIS to Enable HTTP Downloads on a Windows Server 2008 File Share Distribution Point

  Find out how to activate Internet Information Services (IIS) and use it to enable HTTP downloads on a Windows Server 2008 file share distribution point.

Cloud Distribution Point

The cloud distribution point uses a cloud service to host packages, in-house apps, and in-house eBooks. The JAMF Software Server (JSS) supports the following cloud services:

- Rackspace Cloud Files

  For more information on this service, go to http://www.rackspace.com/cloud/public/files/.

- Amazon Web Services (S3 and CloudFront)

  For more information on these services, go to http://aws.amazon.com.

- Akamai cloud services

  For more information on Akamai cloud services, go to http://www.akamai.com.

When you configure the cloud distribution point in the JSS, you can choose to make it the master. You can also choose whether to replicate specific files or the entire contents of the master distribution point.

Requirements

If you plan to use Akamai for your cloud distribution point, Akamai must be configured to use File Transfer Protocol (FTP).

> ***Note:*** If you have upgraded from the Casper Suite v8.x, you must migrate the scripts and packages on your master distribution point before configuring the cloud distribution point. (For more information, see the Migrating Packages and Scripts Knowledge Base article.)

Configuring the Cloud Distribution Point

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **Cloud Distribution Point** ☁.
5. Click **Edit**.
6. Choose a service from the **Cloud Service** pop-up menu.
7. Configure the settings on the pane.
8. Click **Save**.

Testing the Cloud Distribution Point

Once the cloud distribution point is configured, you can test the connection to the cloud service.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **Cloud Distribution Point** ☁.
5. Click **Test**.
6. Click **Test** again.

A message displays, reporting the success or failure of the connection.

Replicating Files to the Cloud Distribution Point

During replication, files on the master distribution point are replicated to the cloud distribution point. The files that are replicated depend on whether the cloud distribution point is configured to replicate specific files or the entire contents of the master.

1. Open Casper Admin and authenticate to the JSS.
2. In the sidebar, select the cloud distribution point you want to replicate files to.
3. Click **Replicate**.

Related Information

For related information, see the following section in this guide:

Network Segments
You can use network segments to ensure that computers and mobile devices use the closest distribution point by default.

JAMF Distribution Server Instances

A JAMF Distribution Server (JDS) instance is a distribution point that is managed by the JAMF Software Server (JSS), similar to a computer or mobile device. It can be used to host packages, in-house apps, and in-house eBooks.

Before using a JDS instance, you must install it and configure it. JDS instances can be installed on OS X or Linux. When you install a JDS instance, it is enrolled with the JSS. You can install as many instances as your organization requires.

By default, the first JDS instance you install is the root. The root instance is used by other instances as the authoritative source for all files. The root instance can also be used as the master distribution point. You can make a different instance the root at any time.

You can define parent-child relationships between non-root JDS instances, making selective file replication more manageable.

When you configure a JDS instance, you can do the following:

- Make it the master distribution point.
- Choose a parent JDS instance (non-root JDS instances only).
- Enable certificate-based authentication.
- Limit the rate at which the JDS instance downloads files.
- Specify WebDAV accounts.
- Choose whether to replicate specific files or the entire contents of the parent JDS instance (non-root JDS instances only).

You can also view the progress of file replication and view inventory information for each JDS instance.

Requirements

The JDS Installer for Mac requires a computer with:

- An Intel processor
- 2 GB of RAM
- 100 GB of disk space available
- OS X Server v10.7 or later
- Server.app 1.4.3 or later

The JDS Installer for Linux requires a computer with:

- An Intel processor
- 2 GB of RAM

- 100 GB of disk space available
- One of the following operating systems:
  - Ubuntu 10.04 LTS Server
  - Ubuntu 12.04 LTS Server
  - Red Hat Enterprise Linux (RHEL) 6

To manage JDS instances in the JSS, you need a valid SSL certificate on the JSS host server. (For more information, see SSL Certificate.)

> ***Note:*** If you have upgraded from the Casper Suite v8.x, you must migrate the scripts and packages on your master distribution point before configuring JDS instances. (For more information, see the Migrating Packages and Scripts Knowledge Base article.)

Installing a JDS Instance on OS X

There are two ways to install a JDS instance on OS X: during a fresh installation of the JSS using the JSS Installer for Mac, or at any time using the JDS Installer for Mac.

For more information on installing a JDS instance using the JSS Installer for Mac, see the "Installing the JSS" section in the *JAMF Software Server Installation and Configuration Guide for OS X*.

To obtain the JDS Installer for Mac, log in to JAMF Nation and go to the following page:

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

To install a JDS instance using the JDS Installer for Mac (`JDS Installer.pkg`), copy the installer to the server. Then double-click the installer and follow the onscreen instructions.

Installing a JDS Instance on Linux

To obtain the JDS Installer for Linux, log in to JAMF Nation and go to the following page:

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

1. Copy the JDS Installer for Linux (`JDS Installer.run`) to the server on which you plan to install a JDS instance.
2. Log in to the server as a user with superuser privileges.
3. Initiate the installer by executing a command similar to the following:

```
sudo /path/to/JDS Installer.run
```

4. When prompted, enter the JDS hostname. For example, "jds.mycompany.com".
5. When prompted, enter the JSS URL. For example, "https://jss.mycompany.com:8443/".

6. When prompted, enter credentials for a JSS user account with the "JDS" privilege.
7. Follow the onscreen instructions to complete the installation.

Configuring a JDS Instance

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **JDS** .
5. Click the JDS instance you want to configure.
6. Click **Edit**.
7. Use the General pane to configure basic settings for the JDS instance.
8. Click the **Distribution Point** tab and configure distribution settings.
9. Click **Save**.

Replicating Files to the Root JDS Instance

During replication, all files on the master distribution point are replicated to the root JDS instance. Then, files are automatically and immediately replicated to non-root JDS instances. The files that are replicated to non-root JDS instances depend on whether each instance is configured to replicate specific files or the entire contents of their parent JDS instance.

1. Open Casper Admin and authenticate to the JSS.
2. In the sidebar, select the root JDS instance.
3. Click **Replicate**.

Viewing the Progress of File Replication

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **JDS** .

5. Click **Grid View** at the top of the list.

   The progress of file replication for each JDS instance is displayed. If your master distribution point is a JDS instance, it is marked with two asterisks (**). If your master distribution point is a different type of distribution point, the root instance is marked with a single asterisk (*).

Viewing Inventory Information for a JDS Instance

The JSS displays the following inventory information for each JDS instance:

- Whether or not it is the master distribution point
- Whether or not it is the root instance
- Hostname
- URL
- Reported IP address
- jamfds binary version
- Operating system
- Operating system version
- Total memory
- Available memory
- Hard drive size
- Hard drive used space

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **JDS** .
5. Click the JDS instance you want to view inventory information for.

Related Information

For related information, see the following section in this guide:

Network Segments
You can use network segments to ensure that computers and mobile devices use the closest distribution point by default.

For related information, see the following Knowledge Base articles:

- Components Installed on JDS Instances
  Find out what items are installed on JDS instances.
- Changing JDS Hierarchy
  Learn about the implications of changing your JDS hierarchy.
- Uninstalling a JDS Instance
  Find out how to uninstall a JDS instance.

Software Update Servers

Adding an internal software update server to the JAMF Software Server (JSS) is the first step to running Software Update from an internal software update server using a policy or Casper Remote.

Using an internal software update server allows you to reduce the amount of bandwidth used when distributing software updates from Apple. Instead of each computer downloading updates from Apple's Software Update server, updates are only downloaded from Apple once per server.

Using an internal software update server also allows you to control and approve updates before you make them available.

Adding a Software Update Server

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **Software Update Servers** 🌐.
5. Click **New** + .
6. Configure the settings on the pane.
7. Click **Save**.

Cloning, Editing, or Deleting a Software Update Server

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **Software Update Servers** 🌐.
5. Click the software update server you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the software update server, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the software update server, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the software update server, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

Running Software Update
Find out how to run Software Update using a policy or Casper Remote.

For related information, see the following document:

NetBoot/SUS Server User Guide
Find out how to host an internal software update server on Linux.

NetBoot Servers

Adding a NetBoot server to the JAMF Software Server (JSS) is the first step to booting computers to a NetBoot image using a policy or Casper Remote. NetBoot images are commonly used in place of recovery partitions or external drives when imaging.

Adding a NetBoot Server

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **NetBoot Servers** .
5. Click **New** + .
6. Configure the settings on the pane.
7. Click **Save**.

Cloning, Editing, or Deleting a NetBoot Server

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Server Infrastructure" section, click **NetBoot Servers** .
5. Click the NetBoot server you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the NetBoot server, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the NetBoot server, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the NetBoot server, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Booting Computers to NetBoot Images

  Find out how to boot computers to a NetBoot image using a policy or Casper Remote.
- Network Segments

  You can use network segments to ensure that computers use the closest NetBoot server by default.

For related information, see the following Knowledge Base article:

Creating a NetBoot Image and Setting Up a NetBoot Server
Find out how to host a NetBoot server on OS X Server.

For related information, see the following document:

NetBoot/SUS Server User Guide
Find out how to host a NetBoot server on Linux.

Organizing Your Network

Buildings and Departments

Buildings and departments are organizational components that allow you to group computers and mobile devices by physical location and organizational infrastructure. You can use them to perform inventory searches, create smart groups, and configure the scope of remote management tasks.

Adding a Building or Department

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Network Organization.**

   On a smartphone, this option is in the pop-up menu.
4. Click **Buildings** 🏢 or **Departments** 👥.
5. Click **New** + .
6. Enter a display name for the building or department.
7. Click **Save**.

Cloning, Editing, or Deleting a Building or Department

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Network Organization**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Buildings** 🏢 or **Departments** 👥.
5. Click the building or department you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the building or department, click **Clone** and change the display name. Then click **Save**.
   - To edit the building or department, click **Edit** and change the display name. Then click **Save**.
   - To delete the building or department, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Viewing and Editing Inventory Information for a Single Computer

  You can add a computer to a building or department by editing the computer's inventory information in the JSS.

- Viewing and Editing Inventory Information for a Single Mobile Device

  You can add a mobile device to a building or department by editing the mobile device's inventory information in the JSS.

- Mass Editing the Building or Department for Computers

  Find out how to use the mass edit function to add mutiple computers to a building or department.

- Network Segments

  You can use a network segment to update the building or department to which computers and mobile devices belong.

- Smart Computer Groups

  You can create smart computer groups based on buildings or departments.

- Smart Mobile Device Groups

  You can create smart mobile device groups based on buildings or departments.

- Simple Computer Searches

  You can perform simple computer searches based on buildings or departments.

- Simple Mobile Device Searches

  You can perform simple mobile device searches based on buildings or departments.

- Advanced Computer Searches

  You can create advanced computer searches based on buildings or departments.

- Advanced Mobile Device Searches

  You can create advanced mobile device searches based on buildings or departments.

- Scope

  Learn how to configure scope based on buildings or departments.

Network Segments

A network segment is a range of IP addresses that can be used to group computers and mobile devices based on their network location. Network segments can be class B or class C subnets, or any IP range therein.

Adding network segments to the JSS allows you to do the following:

- Ensure that computers and mobile devices use the closest distribution point by default.
- Ensure that computers use the closest NetBoot server by default.
- Specify a software update server for computers to use by default.
- Automatically update the building and department to which computers and mobile devices belong.
- Base the scope of remote management tasks on network segments.

If a computer belongs to multiple network segments, the JSS uses the network segment with the fewest IP addresses. If the number of IP addresses in each network segment is equal, the JSS uses the network segment with the lowest starting IP address.

Adding a Network Segment

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Network Organization**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Network Segments** 🌐.
5. Click **New** + .
6. Configure the network segment using the settings on the pane.
7. Click **Save**.

Cloning, Editing, or Deleting a Network Segment

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Network Organization**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Network Segments** 🌐.

5. Click the network segment you want to clone, edit, or delete.

6. Do one of the following:
   - To clone the network segment, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the network segment, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the network segment, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Scope
Learn how to configure scope based on network segments.

For related information, see the following Knowledge Base article:

Using the JSS Subnet Importer
Find out how to use the JSS Subnet Importer to import a CSV file that contains network segment information into the JSS.

Sites

Sites are organizational components that allow you to control which items each JSS user can manage. Implementing sites in your environment involves adding sites to the JSS, granting JSS users access to sites, and adding items to sites.

When a user logs in to the JSS with an account that has access to a site, the user sees only the items that belong to that site. If the user has access to multiple sites, a pop-up menu is displayed at the top of the page, allowing the user to switch between sites.

There are three ways to add sites to the JSS:

- Add each site manually
- Automatically create a site for each existing building
- Automatically create a site for each existing department

Note: You can only create sites from buildings or departments if you are adding sites for the first time and have buildings or departments set up in the JSS.

Creating sites from buildings or departments automatically adds computers and mobile devices to the site that corresponds with the building or department they belong to.

Adding a Site

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Network Organization**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Sites** ● .
5. Click **New** + .
6. If prompted, choose a method for adding sites:
   - To add sites manually, select **Add sites manually** and click **Next**.
   - To create a site for each existing building, select **Create sites from buildings** and click **Next**.
   - To create a site for each existing department, select **Create sites from departments** and click **Next**.
7. If prompted, enter a display name for the site and click **Save**.

Cloning, Editing, or Deleting a Site

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Network Organization**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Sites** .
5. Click the site you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the site, click **Clone** and change the display name. Then click **Save**.
   - To edit the site, click **Edit** and change the display name. Then click **Save**.
   - To delete the site, click **Delete** and then click **Delete** again to confirm.

Adding Items to a Site

The following items can be added to a site:

- Computers
- Mobile devices
- Peripherals
- Enrollment invitations
- Enrollment profiles
- Advanced searches
- Smart groups
- Static groups
- Policies
- Configuration profiles
- Managed Preference profiles
- PreStages
- Restricted software records
- Licensed software records
- Classes
- Apps
- eBooks

There are several ways to add computers to a site:

- Create sites from existing buildings and departments. This automatically adds computers to the site that corresponds with the building or department they belong to.
- Enroll computers using one of the following methods:
  - Send computer enrollment invitations. (For more information, see User-Initiated Enrollment for Computers.)
  - Use a Recon QuickAdd package. (For more information, see QuickAdd Packages Created Using Recon.)
  - Use the network scanner. (For more information, see Network Scanner.)
  - Run Recon remotely on a single computer. (For more information, see Remote Enrollment Using Recon.)
  - Run Recon locally. (For more information, see Local Enrollment Using Recon.)

- Mass edit **Site** field for computers that are already enrolled with the JSS. (For more information, see Mass Editing the Site for Computers.)
- Manually edit the **Site** field for individual computers that are already enrolled with the JSS. (For more information, see Viewing and Editing Inventory Information for a Single Computer.)

There are several ways to add mobile devices to a site:

- Create sites from existing buildings and departments. This automatically adds mobile devices to the site that corresponds with the building or department they belong to.
- Enroll mobile devices using one of the following methods:
  - Send mobile device enrollment invitations. (For more information, see User-Initiated Enrollment for Mobile Devices.)
  - Enroll mobile devices that are connected to a computer by USB. (For more information, see Enrollment Profiles.)
- Mass edit **Site** field for mobile devices that are already enrolled with the JSS. (For more information, see Mass Editing the Site for Mobile Devices.)
- Manually edit the **Site** field for individual mobile devices that are already enrolled with the JSS. (For more information, see Viewing and Editing Inventory Information for a Single Mobile Device.)

To add other items to a site, you choose a site from the **Site** pop-up menu when configuring the items in the JSS.

Related Information

For related information, see the following section in this guide:

JSS User Accounts and Groups
Find out how to grant site access to JSS user accounts and groups.

Scope

Scope gives you granular control over which users, computers, and mobile devices receive remote management tasks. For example, you can use scope to ensure that a policy to install desktop publishing software only runs on computers in the Design department, or that an eBook is only distributed to students in a particular class.

Scope can be based on the following items:

- Computers or mobile devices
- Computer or mobile device groups
- Departments
- Buildings
- LDAP or local users
- LDAP user groups
- Network segments
- Classes (eBooks only)

Target

The first step to configuring scope is to define the target. The target is the initial pool of computers or mobile devices that receive the remote management task. The target can be all computers or mobile devices, or a combination of specific computers or mobile devices, groups, buildings, or departments.

You can also define the target as one or more classes of student mobile devices when configuring the scope of an eBook.

After you define the target, you can add limitations and exclusions to the scope as needed.

Limitations

Adding limitations to the scope of a remote management task allows you to limit the task to specific users in the target. For example, if you want a certain application to open at login for specific users regardless of the computer they use, you can use all computers as the target and add specific users as limitations.

Adding limitations also allows you to limit the task to specific network segments in the target. For example, if you want each computer in a department to install a package but only while on the company's production network, you can use the department as the target and add a specific network segment as a limitation.

Exclusions

Adding exclusions to the scope of a remote management task allows you to exclude specific computers or mobile devices, groups, buildings, departments, users, user groups, or network segments. For example, if you want to restrict an application for everyone except the head of the department, you can add them as an exclusion.

Configuring Scope

1. Log in to the JSS with a web browser.
2. Create or edit a remote management task, such as a policy to map a printer.
3. Click the **Scope** tab.
4. Choose an option from the **Target Computers** pop-up menu.
5. If you chose "Specific Computers" from the pop-up menu, add specific computers:
   a. Click **Add** + .
   b. On each tab, click **Add** for the items you want to add.
   c. Click **Done**.

      The items you added are displayed in a list.
6. (Optional) Add limitations to the scope:
   a. Click the **Limitations** tab.
   b. Click **Add** + .
   c. Add items as needed:
      - To add a user, click the **Users** tab. Then enter the username in the search field and click **Add**.
      - To add a user group, click the **User Groups** tab, enter the name of the group in the search field, and click **Search**. Then click **Add** for the group you want to add.
      - To add a network segment, click the **Network Segments** tab and then click **Add** for the network segment.

   d. Click **Done**.

      The items you added are displayed in a list.

7. (Optional) Add exclusions to the scope:

   a. Click the **Exclusions** tab.

   b. Click **Add** + .

   c. Add items as needed:

      - To add an LDAP or local user, click the **Users** tab. Then enter the username in the search field and click **Add**.

      - To add an LDAP user group, click the **User Groups** tab, enter the name of the group in the search field, and click **Search**. Then click **Add** for the group you want to add.

      - To add another type of item, click the appropriate tab and then click **Add** for the item you want to add.

   d. Click **Done**.

      The items you added are displayed in a list.

8. When you are done configuring the remote management task, click **Save**.

Managing Computers

Building the Framework for Managing Computers

Recurring Check-in Frequency

The recurring check-in frequency is the interval at which computers check in with the JSS for available policies.

By default, the recurring check-in frequency is set to "Every 15 Minutes".

Configuring the Recurring Check-in Frequency

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Check-In** 🕒.
5. Click **Edit**.
6. Configure the recurring check-in frequency using the pop-up menu on the pane.
7. Click **Save**.

Each computer checks in at the specified interval, starting at the time the setting is applied to the computer. This means that check-in times will vary across computers.

Related Information

For related information, see the following section in this guide:

Managing Policies
You can create policies that are triggered at the recurring check-in frequency.

For related information, see the following Knowledge Base article:

Components Installed on Managed Computers
Find out where the files that control the recurring check-in frequency are stored on computers.

Startup Script

The Startup Script settings in the JAMF Software Server (JSS) allow you to create a startup script on computers and use it to perform the following actions at startup:

- Log Computer Usage information (date/time of startup).
- Check for policies triggered at startup.
- Enable computer-level Managed Preferences.
- Ensure SSH (Remote Login) is enabled on computers.

Configuring the Startup Script

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Check-In** 🕓.
5. Click the **Startup Script** tab.
6. Click **Edit**.
7. Configure the settings on the pane.
8. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- Computer Usage

  Find out how to view Computer Usage information logged at startup.
- Managing Policies

  You can create policies that are triggered at startup.
- Managed Preferences

  Learn about computer-level Managed Preferences and how to create Managed Preferences, in general.

For related information, see the following Knowledge Base article:

Components Installed on Managed Computers
Find out where the startup script is stored on computers.

Login and Logout Hooks

The Login/Logout Hooks settings in the JAMF Software Server (JSS) allow you to create login and logout hooks on computers and use them to perform the following actions:

- Log Computer Usage information (username and date/time) at login and logout.
- Check for policies triggered at login or logout.
- Enable user-level and user-level enforced Managed Preferences at login.
- Hide the Restore partition at login.

Warning: Creating login and logout hooks with the Casper Suite can disable existing login and logout hooks.

Configuring Login and Logout Hooks

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Check-In** 🕒.
5. Click the **Login/Logout Hooks** tab.
6. Click **Edit**.
7. Configure the settings on the pane.
8. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- Computer Usage
  Find out how to view Computer Usage information logged at login and logout.
- Managing Policies
  You can create policies that are triggered at login or logout.
- Managed Preferences
  Learn about user-level Managed Preferences and how to create Managed Preferences, in general.

For related information, see the following Knowledge Base article:

Components Installed on Managed Computers
Find out where login/logout hooks are stored on computers.

Security Settings

The Security settings in the JAMF Software Server (JSS) allow you to do the following:

- Enable certificate-based authentication.
- Enable push notifications.
- Enable SSL certificate verification.
- Specify a maximum clock skew between managed computers and the JSS host server.

When an OS X computer attempts to communicate with the JSS and the security requirements specified in the JSS are not met, communication is blocked.

Requirements

To enable push notifications, you must have a push certificate in the JSS. (For more information, see Push Certificates.)

Configuring Security Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Security** 🔒 .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- Certificates

  Learn about device certificates and the SSL certificate.
- SSL Certificate

  Find out how to create or upload an SSL certificate that OS X computers can use to verify the identity of the JSS.

For related information, see the following Knowledge Base article:

Certificate-Based Authentication for OS X Computers
Learn how the JSS uses certificate-based authentication to verify the identity of OS X computers.

Categories

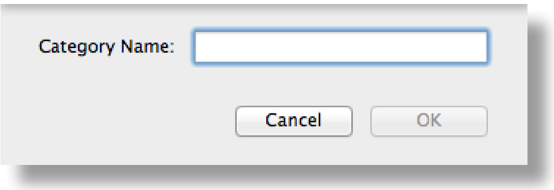
Categories are organizational components that allow you to group policies, packages, scripts, and printers in Casper Admin and the JAMF Software Server (JSS). You can also use categories to group policies in Self Service. This makes these items easier to locate.

You can add categories to Casper Admin or the JSS. When you add, edit, or delete a category in Casper Admin, the changes are reflected in the JSS and vice versa.

After you add a category to Casper Admin or the JSS, you can add items to the category when configuring them in Casper Admin or the JSS.

Adding a Category to Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. Click **New Category** .
3. Enter a display name for the category.



4. Click **OK**.

Adding a Category to the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Categories** .
5. Click **New** + .
6. Enter a display name for the category.
7. Click **Save**.

Editing or Deleting a Category in Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the "Categories" list above the main repository, select the category you want to edit or delete.
3. Do one of the following:
   - To edit the category, double-click it and make changes as needed. Then click **OK**.
   - To delete the category, click **Delete** 🚫 and then click **Delete** again to confirm.

Cloning, Editing, or Deleting a Category in the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Categories** 📁 .
5. Click the category you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the category, click **Clone** and change the display name. Then click **Save**.
   - To edit the category, click **Edit** and change the display name. Then click **Save**.
   - To delete the category, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Managing Packages
  You can add packages to a category.
- Managing Scripts
  You can add scripts to a category.
- Managing Printers
  You can add printers to a category.
- Managing Policies
  You can add policies to a category.
- Self Service Policies
  Find out how to display or feature policies in one or more categories in Self Service.

Enrollment

About Computer Enrollment

Enrollment is the process of adding OS X or Windows computers to the JAMF Software Server (JSS). When computers are enrolled, inventory information for the computers is submitted to the JSS.

Enrolling OS X computers makes them managed by the JSS. This allows you to perform inventory tasks and remote management and configuration tasks on the computers. When you enroll OS X computers, you specify a local administrator account that you want to use to manage them (called the "management account").

Enrolling Windows computers allows you to search and report on the computers as part of your inventory. Windows computers cannot be managed by the JSS.

There are several ways to enroll OS X computers with the JSS:

- **User-initiated enrollment**—You can allow users to enroll their own OS X computers by having them log in to an enrollment portal where they follow the onscreen instructions to download and install a QuickAdd package.
- **Use a QuickAdd package created with Recon**—You can use Recon to create a QuickAdd package that enrolls OS X computers when it is installed. This type of QuickAdd package can be deployed using almost any deployment tool, such as Apple Remote Desktop or the Casper Suite. You can also give the QuickAdd package to users to install.
- **Use the network scanner**—You can remotely enroll multiple OS X computers in specified IP ranges by using the network scanner in Recon. Recon scans the specified IP ranges and enrolls any computers that it can connect to over SSH (Remote Login).
- **Run Recon remotely on a single computer**—If you know the IP address of the OS X computer that you want to enroll and SSH (Remote Login) is enabled on the computer, you can enroll the computer by running Recon remotely.
- **Run Recon locally**—If you have physical access to the OS X computer that you want to enroll, you can run Recon locally on the computer.
- **Image computers**—You can enroll OS X computers by imaging them with a configuration that is associated with a management account.

There are two ways to enroll Windows computers with the JSS:

- **Use a Recon.exe QuickAdd package**—You can use Recon.exe to create a QuickAdd package that enrolls Windows computers when it is installed. This type of QuickAdd package can be deployed using almost any deployment tool. You can also give the QuickAdd package to users to install.
- **Run Recon.exe locally**—If you have physical access to the Windows computer that you want to enroll, you can run Recon.exe locally on the computer.

Related Information

For more information, see the following sections in this guide:

- User-Initiated Enrollment for Computers

  Find out how to allow users to enroll their own computers by having them log in to an enrollment portal.
- QuickAdd Packages Created Using Recon

  Find out how to use Recon to create a QuickAdd package that enrolls computers.
- Network Scanner

  Find out how to use the network scanner to remotely enroll multiple computers.
- Remote Enrollment Using Recon

  Find out how to enroll an OS X computer by running Recon remotely.
- Local Enrollment Using Recon

  Find out how to enroll an OS X computer by running Recon locally on the computer.
- About Imaging

  You can enroll computers by imaging them with a configuration associated with a management account. Learn about imaging and the different imaging methods.
- QuickAdd Packages Created Using Recon.exe

  Find out how to use Recon.exe to create a QuickAdd package that enrolls Windows computers.
- Local Enrollment Using Recon.exe

  Find out how to enroll a Windows computer by running Recon.exe locally on the computer.

For related information, see the following Knowledge Base articles:

- Components Installed on Managed Computers

  See a list of the components installed on managed computers.
- Removing JAMF Software Components from Computers

  Find out how to remove all Casper Suite-related components from computers that have been managed by the JSS.

User-Initiated Enrollment Settings for Computers

The User-Initiated Enrollment settings for computers allow you to enable user-initiated enrollment and configure the QuickAdd package used for user-initiated enrollment. When configuring the QuickAdd package, you can do the following:

- Specify a management account for computers.
- Ensure that SSH (Remote Login) is enabled on computers.
- Ensure that computers launch Self Service after they are enrolled.
- Customize the enrollment portal.
- Sign the QuickAdd package.

Signing the QuickAdd Package

Signing the QuickAdd package for user-initiated enrollment ensures that it appears as verified to users that install it. 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.

If you choose to sign the QuickAdd package, you need to upload an installer certificate (.p12) from Apple's Developer Certificate Utility. For instructions on how to obtain an installer certificate, see the following Knowledge Base article:

Obtaining an Installer Certificate from Apple's Developer Certificate Utility

Configuring the User-Initiated Enrollment Settings for Computers

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **User-Initiated Enrollment** 🖥.
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Related Information

For related information, see the following section in this guide:

User-Initiated Enrollment for Computers
Find out how to allow users to enroll their own computers by having them log in to an enrollment portal.

User-Initiated Enrollment for Computers

You can allow users to enroll their own computers by having them log in to an enrollment portal where they follow the onscreen instructions to download and install a QuickAdd package.

To direct users to the enrollment portal, you need to provide them with the enrollment URL. This is the full URL for the JAMF Software Server (JSS) followed by "/enroll". For example:

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

You can provide this URL by sending it in an email invitation from the JSS, or through any other means that fit your environment. Sending an invitation from the JSS allows you to add computers to a site during enrollment.

Users can log in to the enrollment portal using an LDAP directory account or a JSS user account. If users log in to the enrollment portal with an LDAP directory account, user and location information is submitted during enrollment.

Requirements

To send a computer enrollment invitation, you need:

- An SMTP server set up in the JSS (For more information, see Integrating with an SMTP Server.)
- User-initiated enrollment enabled and the QuickAdd package configured in the JSS (For more information, see User-Initiated Enrollment Settings for Computers.)

If the QuickAdd package is signed, computers must have a Certification Authority intermediate certificate from Apple in the System keychain in Keychain Access. For instructions on how to obtain this certificate and import it to the System keychain, see the following Knowledge Base article:

Importing a Certification Authority Intermediate Certificate from Apple to the System Keychain

For users to log in to the enrollment portal with their LDAP directory account, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

Sending a Computer Enrollment Invitation

Before you configure the invitation, make sure you have the email addresses of the users you want to send the invitation to.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Enrollment Invitations**.
   On a smartphone, this option is in the pop-up menu.

4. Click **New** + .
5. Follow the onscreen instructions to send the enrollment invitation.

   An enrollment invitation is immediately sent to email addresses you specified.

   You can view the status of the enrollment invitation in the list of invitations.

Viewing Computer Enrollment Invitation Usage

You can view a list of computers that were enrolled with a single enrollment invitation.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Enrollment Invitations**.
   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment invitation you want to view usage for.
5. Click **View Enrolled Computers**.

   A list of computers enrolled with the invitation is displayed.

Deleting a Computer Enrollment Invitation

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Enrollment Invitations**.
   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment invitation you want to delete.
5. Click **Delete**, and then click **Delete** again to confirm.

QuickAdd Packages Created Using Recon

You can use Recon to create a QuickAdd package that enrolls OS X computers when it is installed. This type of QuickAdd package can be deployed using almost any deployment tool, such as Apple Remote Desktop or the Casper Suite. You can also give the QuickAdd package to users to install.

When you create a QuickAdd package using Recon, you can do the following:

- Ensure that SSH (Remote Login) gets enabled on computers that have it disabled.
- Ensure that computers launch Self Service after they are enrolled.
- Sign the QuickAdd package.
- Choose a site to add computers to during enrollment.

To install a QuickAdd package, you double-click it and then follow the onscreen instructions.

Signing a QuickAdd Package

Signing a QuickAdd package ensures that it appears as verified to users that install it. 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.

There are some additional requirements for signing a QuickAdd package and installing a signed QuickAdd package. For more information, see the "Requirements" section below.

Requirements

To sign a QuickAdd package, the computer running Recon must have:

- OS X v10.7 or later
- An installer certificate (.p12) from Apple's Developer Certificate Utility in the System keychain in Keychain Access (For more information, see the Obtaining an Installer Certificate from Apple's Developer Certificate Utility Knowledge Base article.)

To install a signed QuickAdd package, computers must have a Certification Authority intermediate certificate from Apple in the System keychain in Keychain Access. For instructions on how to obtain this certificate and import it to the System keychain, see the following Knowledge Base article:

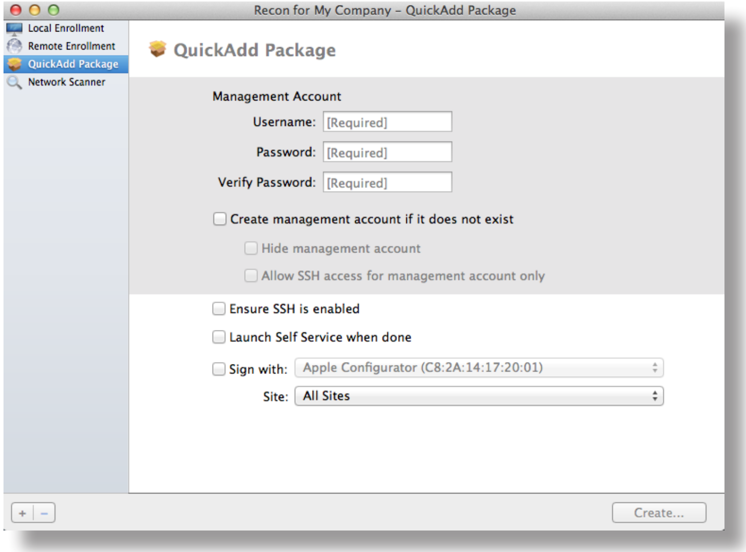
Importing a Certification Authority Intermediate Certificate from Apple to the System Keychain

Creating a QuickAdd Package Using Recon

1. Open Recon and authenticate to the JSS.
2. Select **QuickAdd Package** in the sidebar.

3. Enter credentials for a local administrator account.

   This account is used as the management account.



Recon for My Company – QuickAdd Package

QuickAdd Package

Management Account

Username: [Required]

Password: [Required]

Verify Password: [Required]

□ Create management account if it does not exist

□ Hide management account

□ Allow SSH access for management account only

□ Ensure SSH is enabled

□ Launch Self Service when done

□ Sign with: Apple Configurator (C8:2A:14:17:20:01)

Site: All Sites

4. If the management account you specified is a new account, select the **Create management account if it does not exist** checkbox and configure additional settings for the management account as needed.

5. To enable SSH on computers that have it disabled, select the **Ensure SSH is enabled** checkbox.

6. To launch Self Service on computers immediately after they are enrolled, select the **Launch Self Service when done** checkbox.

7. 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 choose an installer certificate, not an application certificate, to sign QuickAdd packages.

8. Click **Create** and save the package.

After creating the QuickAdd package, you can deploy it using a deployment tool or give the package to users to install. When the QuickAdd package is installed on computers, they are enrolled with the JSS.

Related Information

For related information, see the following section in this guide:

Installing Packages
Find out how to install a QuickAdd package using a policy or Casper Remote.

Network Scanner

The network scanner in Recon allows you to remotely enroll multiple OS X computers. It scans specified IP ranges and enrolls any computers that it can connect to over SSH (Remote Login).

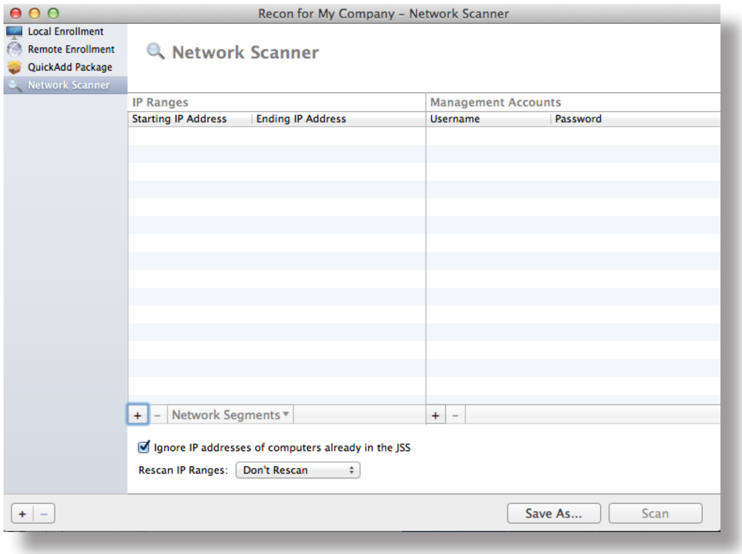
There are two ways to specify the IP ranges you want to scan: choose network segments that are set up in the JSS, or manually specify IP ranges. If you manually specify the IP ranges, you can choose a building, department, and site to add computers to during enrollment.

Requirements

To enroll computers using the network scanner, SSH must be enabled on the computers.

Enrolling Computers Using the Network Scanner

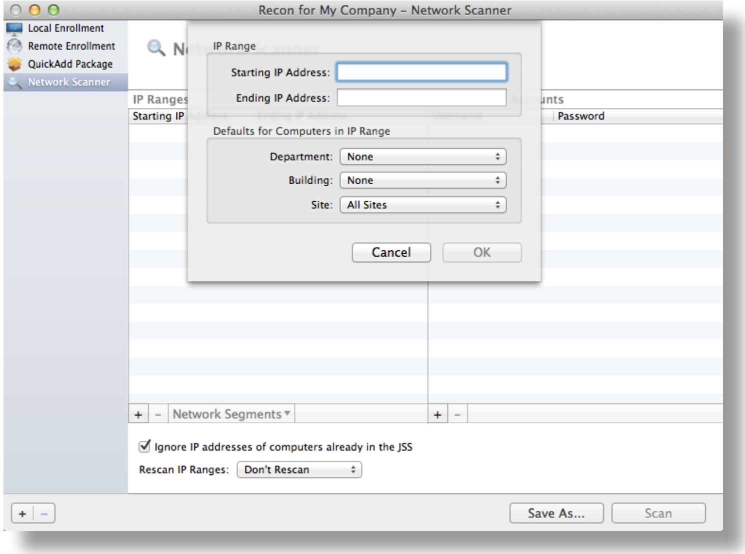
1. Open Recon and authenticate to the JSS.
2. Select **Network Scanner** in the sidebar.
3. Specify the IP ranges you want to scan:
   - To choose network segments that are set up in the JSS, click **Network Segments** below the list of IP ranges and select the network segment you want to scan. Repeat as needed.



☑ Ignore IP addresses of computers already in the JSS

Rescan IP Ranges: Don't Rescan

- To specify IP ranges manually, click **Add** (+) below the list of IP ranges and specify information about the IP range you want to scan. Click **OK** and repeat as needed.



Recon for My Company – Network Scanner

IP Range

Starting IP Address:

Ending IP Address:

Defaults for Computers in IP Range

Department: None

Building: None

Site: All Sites

☑ Ignore IP addresses of computers already in the JSS

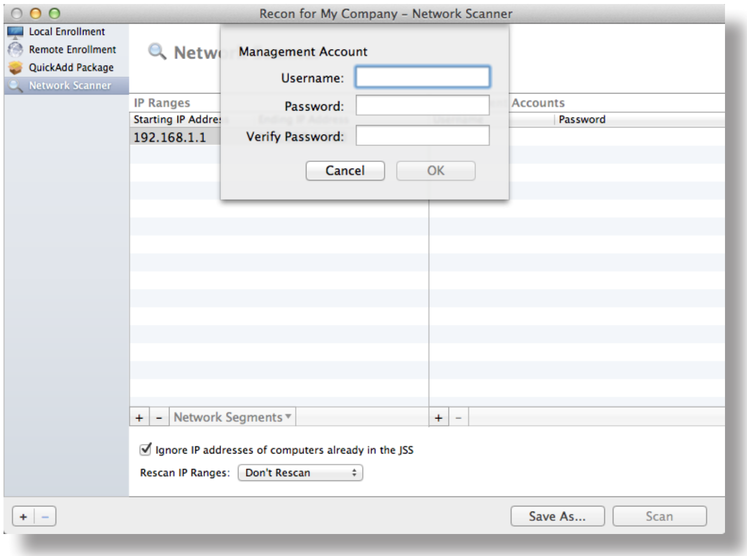
Rescan IP Ranges: Don't Rescan

4. Specify one or more local administrator accounts that have SSH access to computers in the IP range.

   When the network scanner finds a computer on the network, it tries each account until it finds one that can be used to connect to the computer over SSH. The first valid account is used as the management account.

   a. Click **Add** (+) below the list of accounts.

   b. Enter credentials for a local administrator account that has SSH access to computers.



Recon for My Company – Network Scanner

Management Account

Username:

Password:

Verify Password:

Starting IP Address: 192.168.1.1

☑ Ignore IP addresses of computers already in the JSS

Rescan IP Ranges: Don't Rescan

   c. Click **OK**.

   d. If there is more than one administrator account in the specified IP ranges, repeat steps a through c as needed.

5. To ignore computers that are already enrolled with the JSS, select the **Ignore IP addresses of computers already in the JSS** checkbox.

6. To continuously scan for new computers, use the **Rescan IP Ranges** pop-up menu to specify how often Recon should rescan.

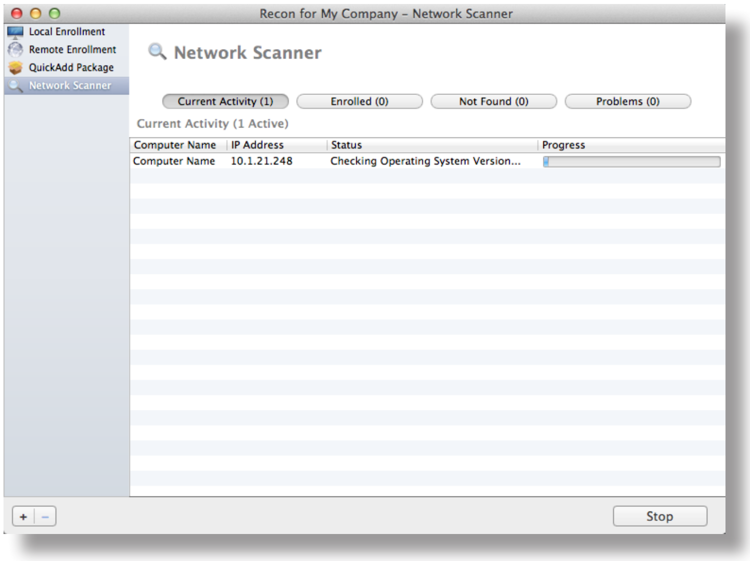
7. To create a .recon file that contains the network scanner settings you just configured, click **Save As**. Then specify a name and location for the file.

   Double-clicking the file opens Recon (if it is not already open) and populates the network scanner settings.

   You can open the file at any time to have Recon automatically configure the network scanner settings.

8. Click **Scan.**

   Recon scans the specified IP ranges and enrolls any computers that it can connect to over SSH. The progress of the scan is displayed on the Current Activity pane. The results of the scan are displayed on the Enrolled, Not Found, and Problems panes.



Current Activity (1 Active)

Computer Name	IP Address	Status	Progress
Computer Name	10.1.21.248	Checking Operating System Version...	

Remote Enrollment Using Recon

If you know the IP address of the OS X computer you want to enroll and SSH (Remote Login) is enabled on the computer, you can enroll the computer by running Recon remotely. This allows you to submit detailed inventory information for the computer. It also allows you to add computers to a site during enrollment.

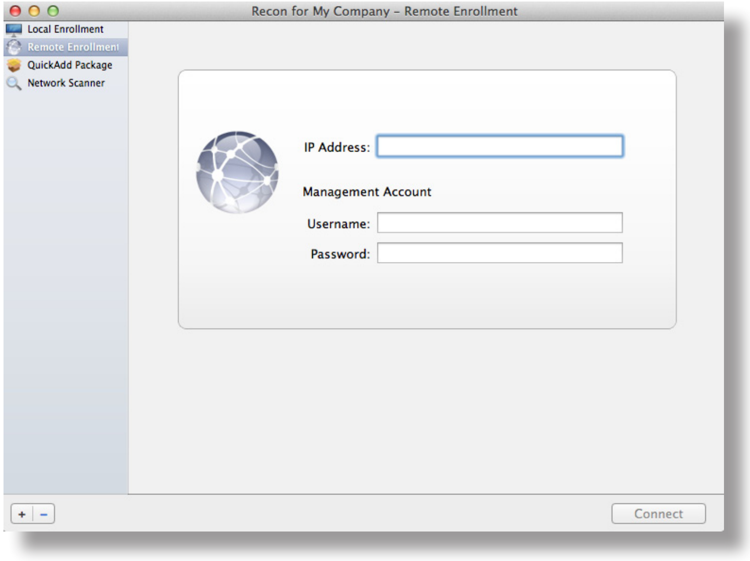
Requirements

To enroll a computer by running Recon remotely, you need:

- The IP address of the computer
- SSH (Remote Login) enabled on the computer

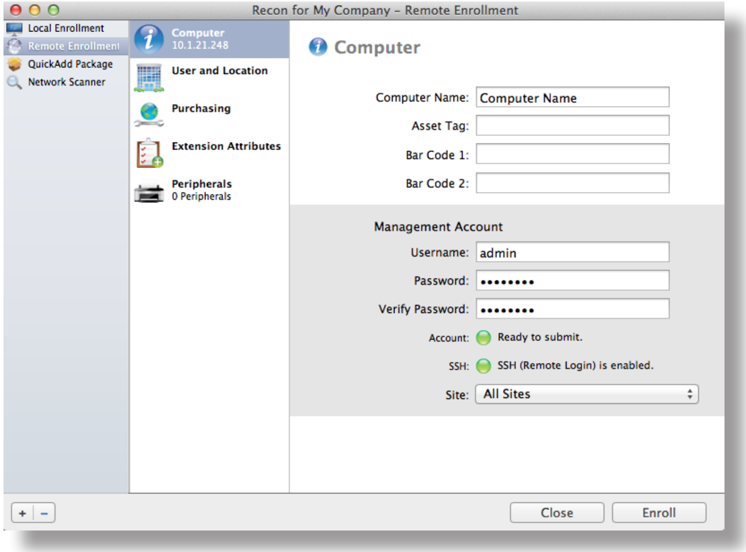
Enrolling a Computer by Running Recon Remotely

1. Open Recon and authenticate to the JSS.
2. Select **Remote Enrollment** in the sidebar.
3. Enter the IP address of the computer you want to enroll.



4. Enter credentials for a local administrator account that has SSH access.

   This account is used as the management account.



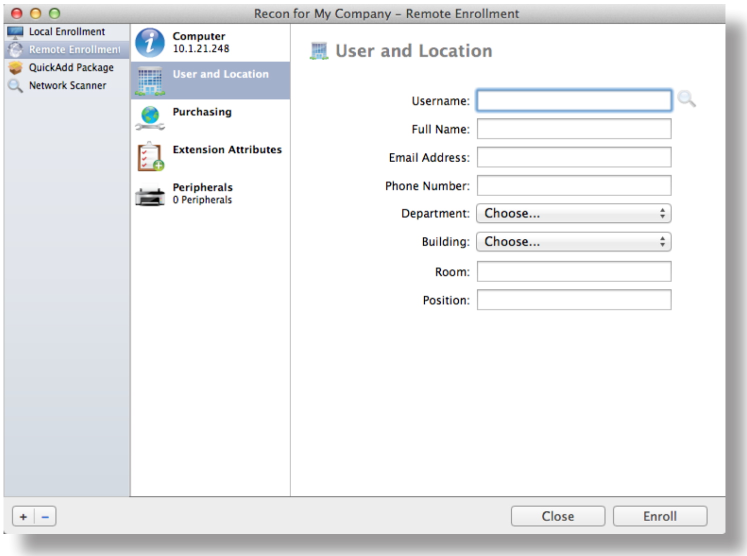
Computer

Computer Name: Computer Name
Asset Tag:
Bar Code 1:
Bar Code 2:

Management Account
Username: admin
Password: ••••••••
Verify Password: ••••••••
Account: Ready to submit.
SSH: SSH (Remote Login) is enabled.
Site: All Sites

5. (Optional) Select **User and Location** and specify user and location information for the computer.

   If an LDAP server is set up in the JSS, click **Search** 🔍 to populate information from the LDAP server. (For more information on setting up an LDAP server, see Integrating with LDAP Directory Services.)

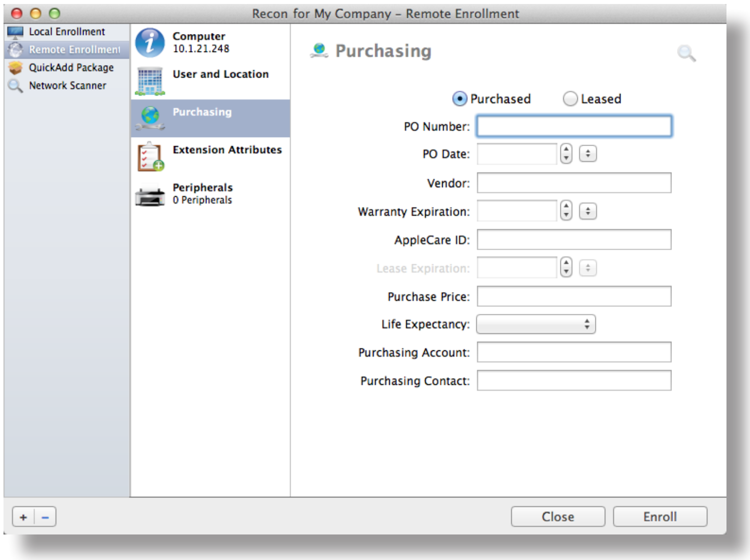


User and Location

Username:
Full Name:
Email Address:
Phone Number:
Department: Choose...
Building: Choose...
Room:
Position:

6. (Optional) Select **Purchasing** and specify purchasing information for the computer.

   If a GSX connection is set up in the JSS, click **Search** 🔍 to populate information from Apple's Global Service Exchange (GSX). (For more information on setting up a GSX connection, see Integrating with GSX.)



7. (Optional) Select **Extension Attributes** and specify information as needed.

8. (Optional) Select **Peripherals** and add peripherals as needed.

9. Click **Enroll**.

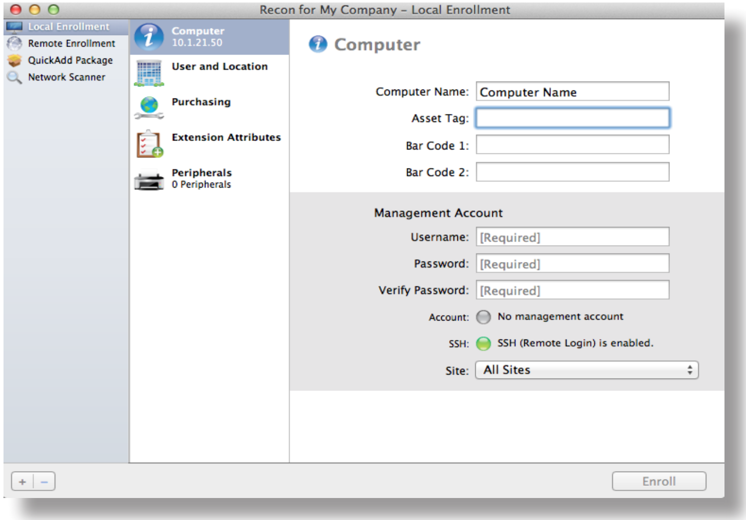
Local Enrollment Using Recon

If you have physical access to the OS X computer that you want to enroll, you can run Recon locally on the computer. This allows you to submit detailed inventory information for the computer. It also allows you to add computers to a site during enrollment.

Enrolling a Computer by Running Recon Locally

1. On the computer you want to enroll, open Recon and authenticate to the JSS.
2. (Optional) Enter an asset tag and/or use a bar code scanner to enter bar codes.

   The computer name is populated by default.



Computer Name: Computer Name

Asset Tag:

Bar Code 1:

Bar Code 2:

Management Account

Username: [Required]

Password: [Required]

Verify Password: [Required]

Account: No management account

SSH: SSH (Remote Login) is enabled.

Site: All Sites

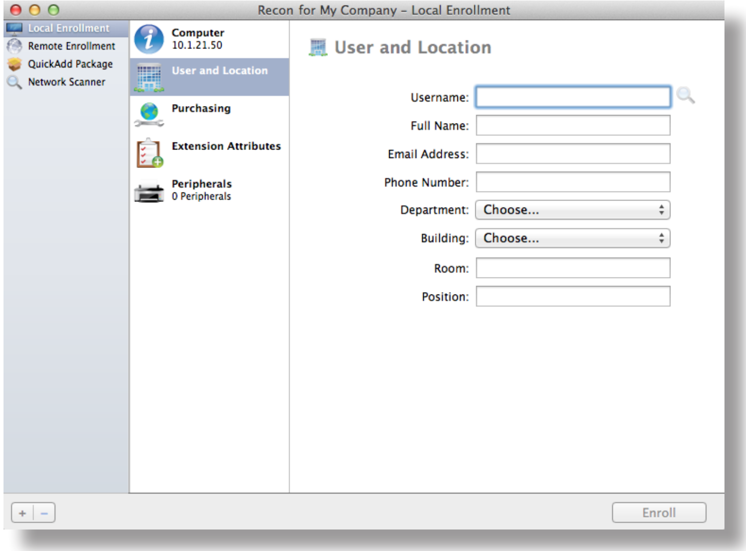
3. Enter credentials for a local administrator account that you want to use to manage computers.

   This can be an existing or new account. If the account does not already exist, Recon creates it.

> ***Note:*** If the account you specify does not have SSH (Remote Login) access to the computer, Recon enables SSH during enrollment.

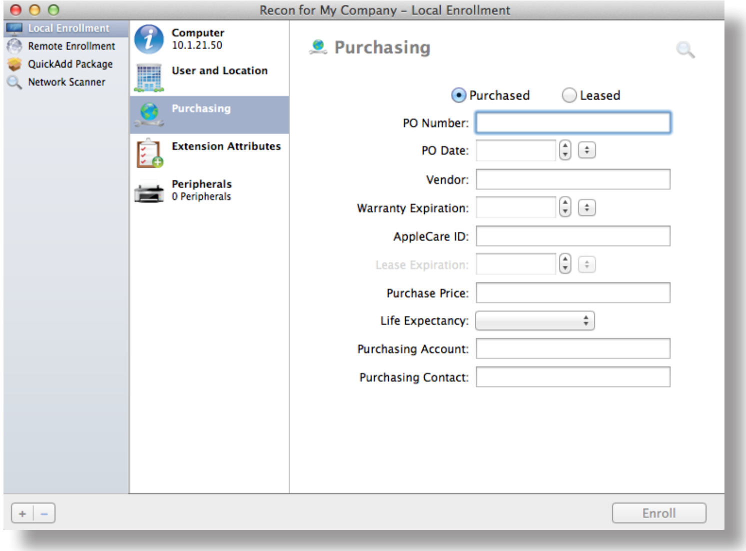
4. (Optional) Select **User and Location** and specify user and location information for the computer.

   If an LDAP server is set up in the JSS, click **Search** to populate information from the LDAP server. (For more information on setting up an LDAP server, see Integrating with LDAP Directory Services.)



5. (Optional) Select **Purchasing** and specify purchasing information for the computer.

   If a GSX connection is set up in the JSS, click **Search** to populate information from Apple's Global Service Exchange (GSX). (For more information on setting up a GSX connection, see Integrating with GSX.)



6. (Optional) Select **Extension Attributes** and specify information as needed.

7. (Optional) Select **Peripherals** and add peripherals as needed.

8. Click **Enroll**.

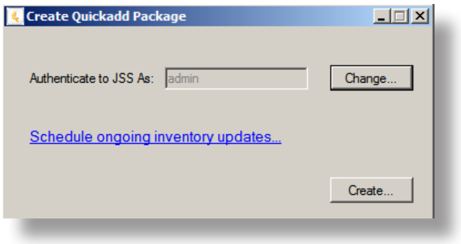
QuickAdd Packages Created Using Recon.exe

You can use Recon.exe to create a QuickAdd package (.mist) that enrolls Windows computers when it is installed. This type of QuickAdd package can be deployed using almost any deployment tool. You can also give the QuickAdd package created using Recon.exe to users to install.

When you create a QuickAdd package using Recon.exe, you can change the account that the QuickAdd package uses to authenticate to the JSS. You can also create a schedule for collecting inventory from Windows computers enrolled using the QuickAdd package.

Creating a QuickAdd Package Using Recon.exe

1. Open Recon.exe and authenticate to the JSS.
2. Click **QuickAdd Package** .
3. To change the account that the QuickAdd package uses to authenticate to the JSS, click **Change** and enter credentials for the account. Then click **OK**.



Create Quickadd Package

Authenticate to JSS As: admin

4. To create a schedule for collecting inventory, click **Schedule ongoing inventory updates**. Configure the schedule and click **Save**.
5. Click **Create** and save the package.

After creating the QuickAdd package, you can deploy it or give it to users to install. When the QuickAdd package is installed on computers, they are enrolled with the JSS.

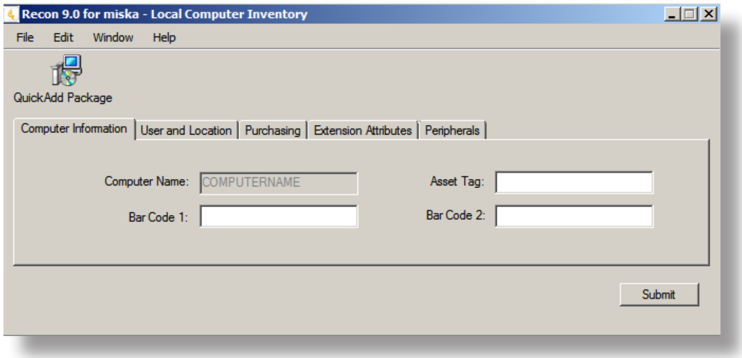
Local Enrollment Using Recon.exe

If you have physical access to the Windows computer that you want to enroll, you can run Recon.exe locally on the computer. This allows you to submit detailed inventory information for the computer.

Enrolling a Windows Computer by Running Recon.exe Locally

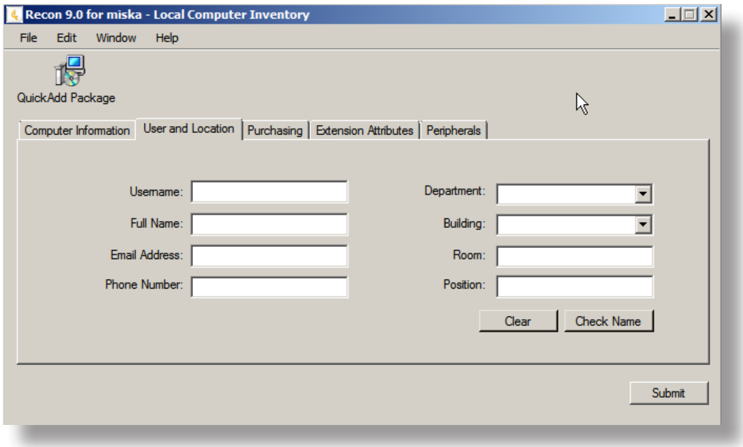
1. On the computer you want to enroll, open Recon.exe and authenticate to the JSS.
2. (Optional) Enter an asset tag and/or use a barcode scanner to enter bar codes.

   The computer name is populated by default.

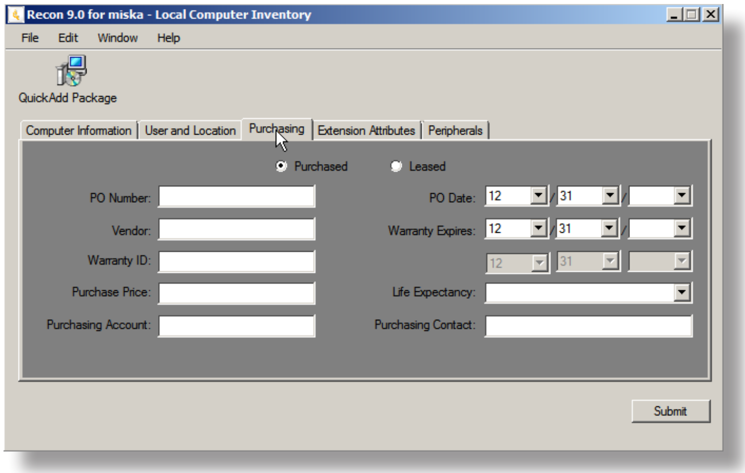


3. (Optional) Click the **User and Location** tab and specify user and location information for the computer.

   If an LDAP server is set up in the JSS, click **Check Name** to populate information from the LDAP server.



4. (Optional) Click the **Purchasing** tab and specify purchasing information for the computer.



● Purchased ○ Leased

PO Number:

Vendor:

Warranty ID:

Purchase Price:

Purchasing Account:

PO Date: 12 / 31 /

Warranty Expires: 12 / 31 /

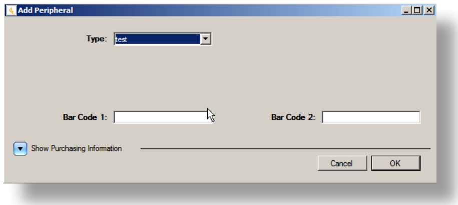
12 / 31 /

Life Expectancy:

Purchasing Contact:

5. (Optional) Click the **Extension Attributes** tab and specify information as needed.

6. (Optional) Click the **Peripherals** tab and add peripherals as needed.



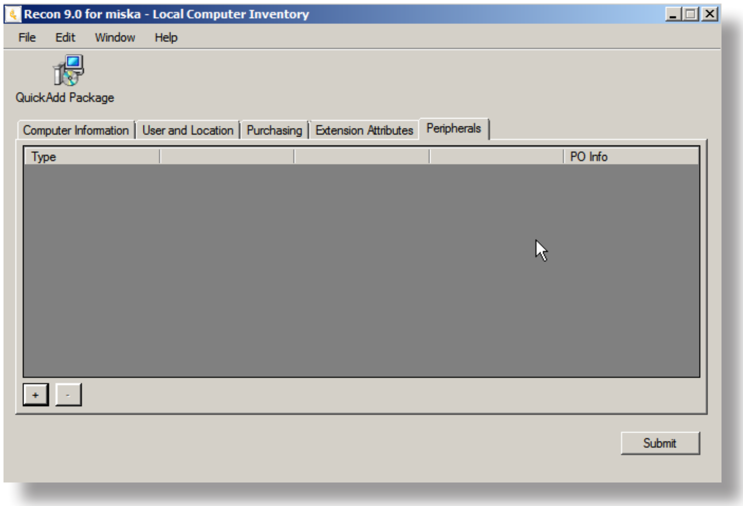
Type: test

Bar Code 1:

Bar Code 2:

Show Purchasing Information

7. Click **Submit**.



Type				PO Info

Composer

About Composer

Composer allows you to build packages of software, applications, preference files, or documents. A package is a self-contained group of files that can be deployed to remote computers or as part of the imaging process.

The first step to building a package is creating a package source. 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 the drive to create the package source.

After you create a package source, you can build a PKG or a DMG from the package source.

Composer also allows you to build a DMG of an operating system.

Related Information

For related information, see the following sections in this guide:

- Creating Package Sources

  Find out how to create a package source using several different methods.
- Building Packages from Package Sources

  Find out how to build a PKG or DMG from a package source.
- Building OS Packages

  Find out how to build a DMG of an operating system.

Creating Package Sources

A package source allows you to view and edit attributes of a package (such as files, scripts, privileges, 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.

There are several ways to create a package source:

- **Take 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.
- **Monitor the file system**—Composer uses the File System Events (FSEvents) framework to monitor any changes that are made to the file system during the installation process. Next, 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.
- **Use 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.
- **Use user environment settings—**Package manifests can also be used to capture settings configured on your computer, such as Dashboard, Display, and Global Preference settings.
- **Drag contents from the Finder—**A simple drag-and-drop process allows you to create a package source from files already installed on your computer.
- **Use an existing package—**Composer allows you to make modifications to an existing package or convert between the PKG and DMG package formats.

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:

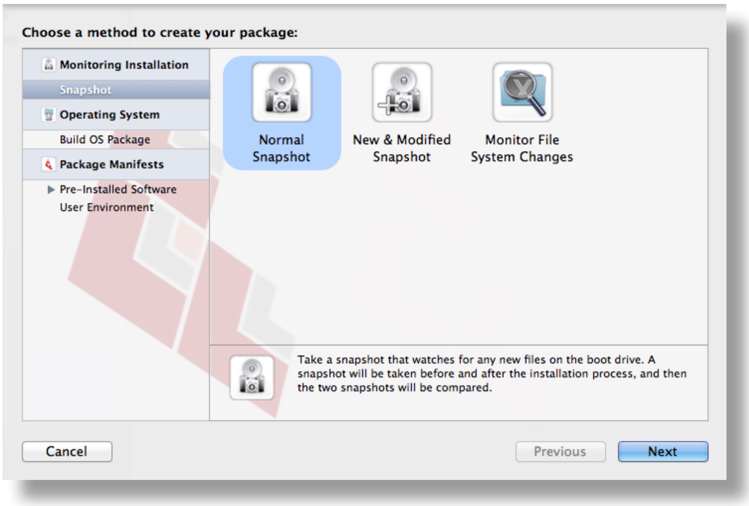
- **Normal snapshots**—These snapshots capture any new files on the drive. These snapshots can take anywhere from ten seconds to several minutes depending on your hardware and the number of files on the drive.
- **New and modified snapshots**—These snapshots capture any new files on the drive, as well 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.

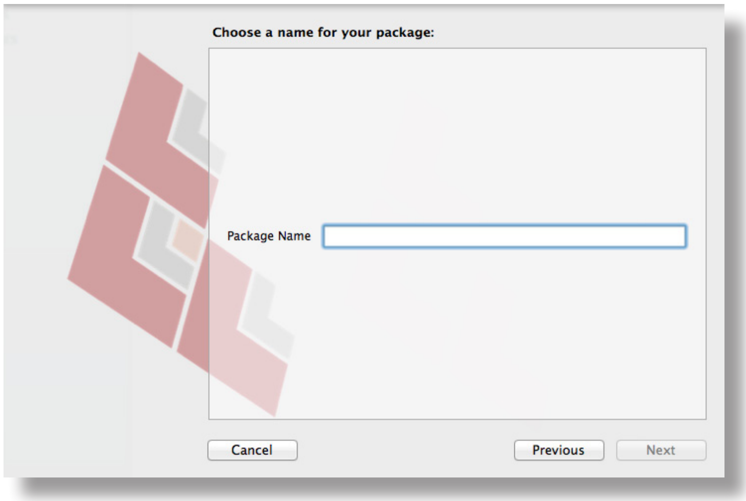
- If you delete a file while making modifications to a package source, it may be possible to restore the deleted file. For more information about restoring deleted files, see Adding Scripts to Package Sources.

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

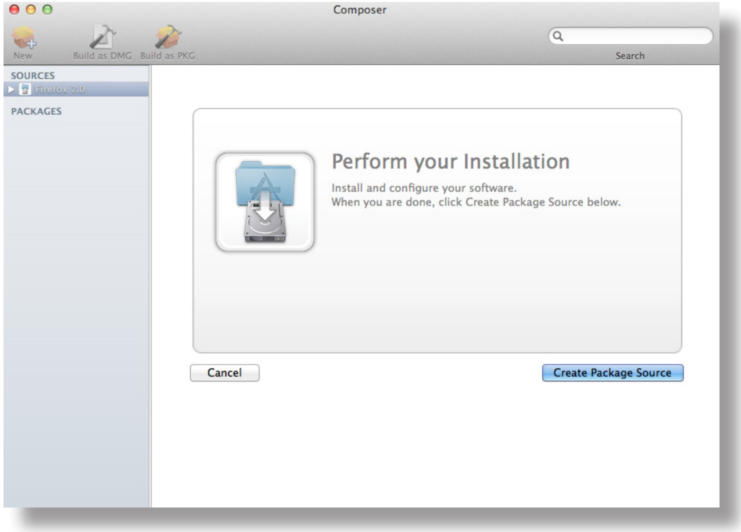


Take a snapshot that watches for any new files on the boot drive. A snapshot will be taken before and after the installation process, and then the two snapshots will be compared.

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



6. Install and configure your software, and then click **Create Package Source** to initiate the "after" snapshot.



Perform your Installation

Install and configure your software.
When you are done, click Create Package Source below.

Monitoring the File System

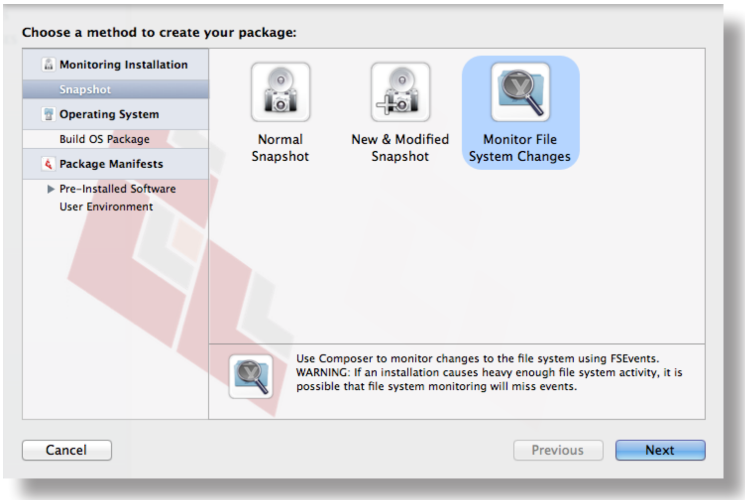
When creating a package source using file system monitoring, Composer uses the File System Events (FSEvents) framework that is built into OS X to monitor any changes that are made to the file system. Each time a change is made, FSEvents receives a notification. After your software is installed, Composer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

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

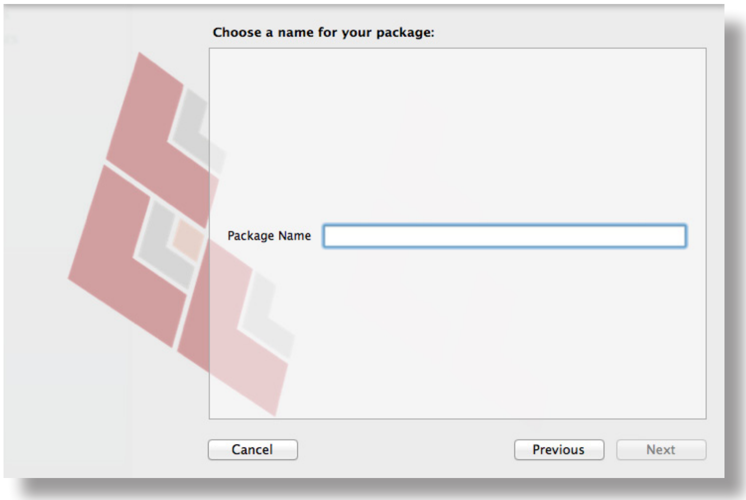
4. Select **Monitor File System Changes** and click **Next**.



Choose a method to create your package:

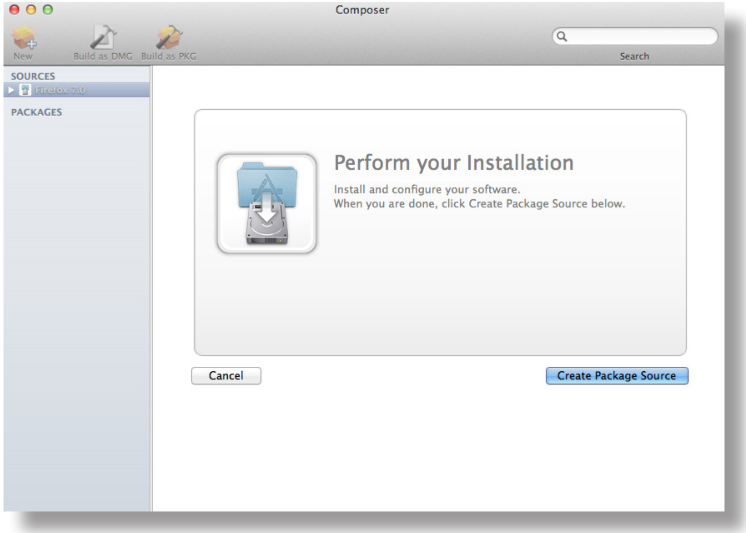
Use Composer to monitor changes to the file system using FSEvents.
WARNING: If an installation causes heavy enough file system activity, it is possible that file system monitoring will miss events.

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



Choose a name for your package:

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



Perform your Installation

Install and configure your software.
When you are done, click Create Package Source below.

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.

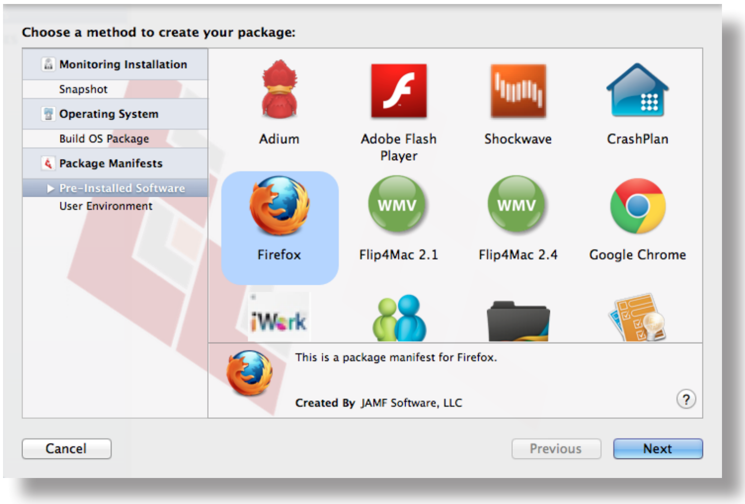
> ***Note:*** If there is software you would like added to the package manifest options in Composer, email your recommendations to diffs@jamfsoftware.com.

1. Open Composer and authenticate locally.
2. In the toolbar, click **New** .
3. Under the Package Manifests heading in the sidebar, select **Pre-Installed Software**.

   Composer scans the file system and displays icons for the software it can package.

> ***Note:*** 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**.

4. Select the item(s) you want to create a package source from and click **Next**.



Choose a method to create your package:

This is a package manifest for Firefox.

Created By JAMF Software, LLC

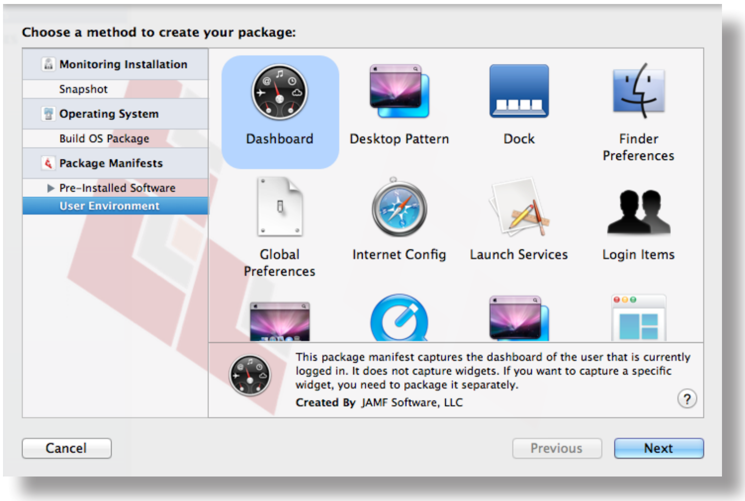
Creating Package Sources from the User Environment Settings

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.

1. Open Composer and authenticate locally.
2. In the toolbar, click **New** .
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 click **Next**.



This package manifest captures the dashboard of the user that is currently logged in. It does not capture widgets. If you want to capture a specific widget, you need to package it separately.

Created By JAMF Software, LLC

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.

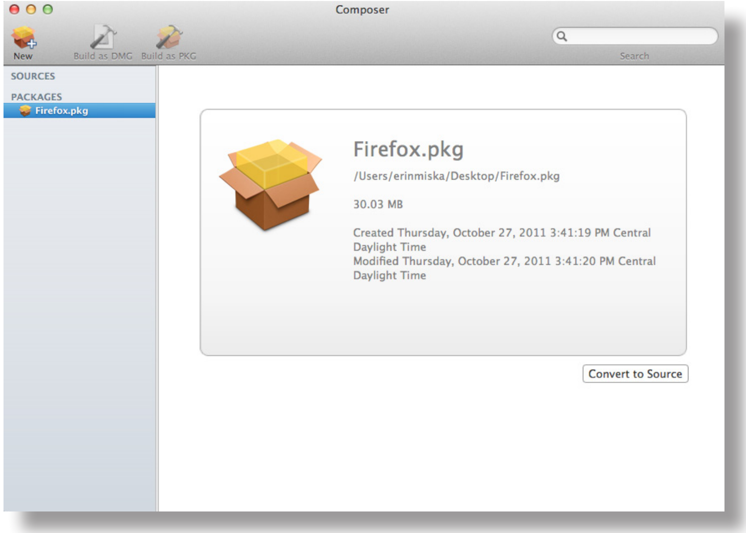
> ***Note:*** This is the equivalent of a PreBuilt package in earlier versions of Composer.

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.

1. Open Composer and authenticate locally.
2. Drag the package you want to convert from the Finder to the sidebar in Composer.

   The package appears under the Packages heading.
3. Select the package and click **Convert to Source**.



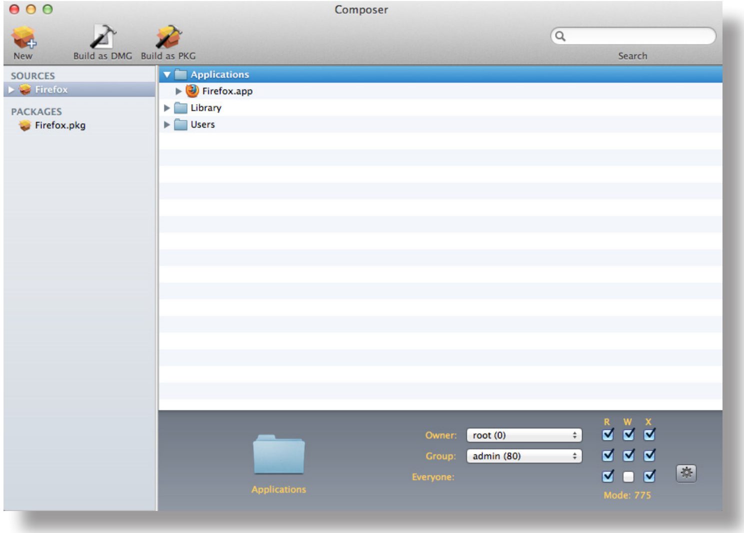
Firefox.pkg

/Users/erinmiska/Desktop/Firefox.pkg

30.03 MB

Created Thursday, October 27, 2011 3:41:19 PM Central Daylight Time
Modified Thursday, October 27, 2011 3:41:20 PM Central Daylight Time

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



Owner: root (0) ☑ ☑ ☑

Group: admin (80) ☑ ☑ ☑

Everyone: ☑ □ ☑

Mode: 775

Related Information

For related information, see the following sections in this guide:

- Package Manifests

  Find out how to create package manifests, update the package manifests available, and import package manifests.

- Building Packages from Package Sources

  Find out how to build a PKG or DMG from a package source.

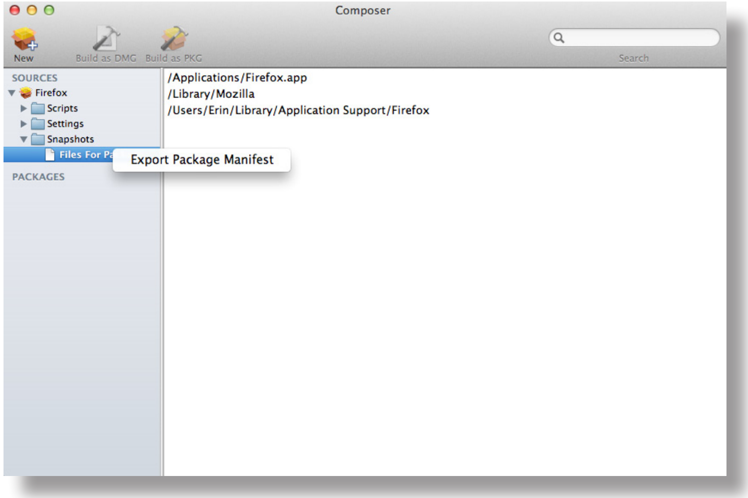
Package Manifests

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.

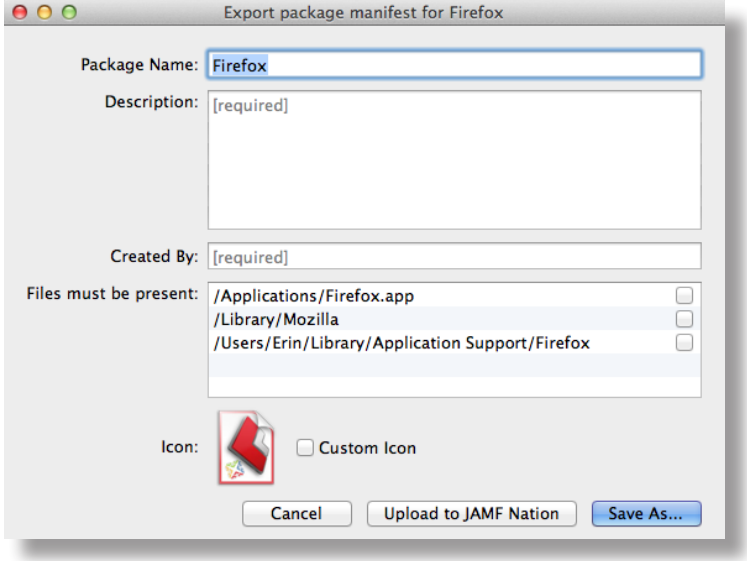
Creating Package Manifests

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**.



```
/Applications/Firefox.app
/Library/Mozilla
/Users/Erin/Library/Application Support/Firefox
```

5. Enter a name for the package manifest.



Export package manifest for Firefox

Package Name: Firefox

Description: [required]

Created By: [required]

Files must be present:
- /Applications/Firefox.app □
- /Library/Mozilla □
- /Users/Erin/Library/Application Support/Firefox □

Icon: □ Custom Icon

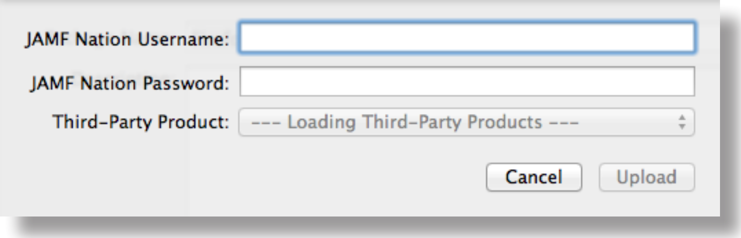
6. Enter a description of the package manifest and the name of the person who is creating it.

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.



JAMF Nation Username:

JAMF Nation Password:

Third-Party Product: --- Loading Third-Party Products ---

   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 and 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/
```

Viewing and Editing the Contents of Package Sources

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

- Delete files that should not be included in the package.
- Add files by dragging them into Composer from the Finder.
- Change privileges 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 from a Package Source

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

Adding Files to a Package Source

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

Changing Privileges on Files or Folders in a Package Source

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

Restoring Deleted Files or Folders to a Package Source

If you delete a file or folder from the Package Contents pane, it may be possible to restore the item. When you restore a deleted file or folder, Composer copies the item from its original location on the drive.

Note: Deleted files and folders can only be restored if a snapshot was used to create the package source.

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.

3. Click the disclosure triangle next to **Snapshots**.

4. Select **Files for Package** to display a list of files, folders, and directories from the snapshot.

5. Select the item you want to restore.

6. Control-click (or right-click) the selected item and choose **Restore**.

Viewing Files or Folders in a Package Source Using the Finder

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

Viewing Files or Folders in a Package Source Using Quick Look

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

Adding Scripts to Package Sources

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 a PKG. For more information on flat PKGs, see 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**.

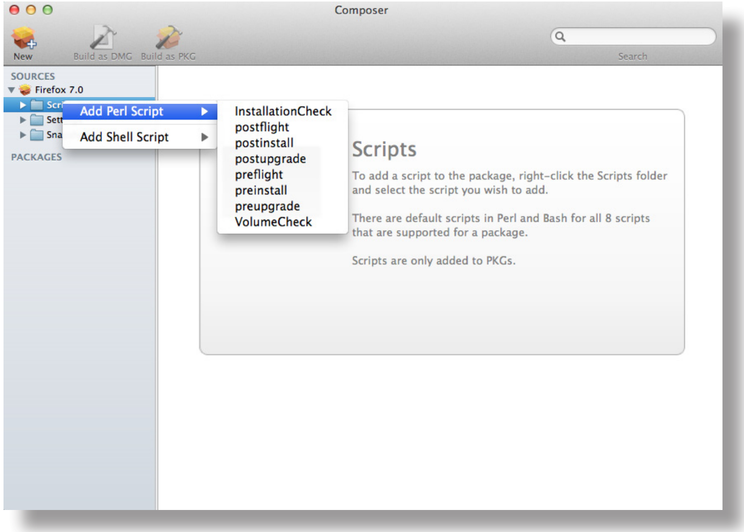
> ***Note:*** `InstallationCheck` and `VolumeCheck` scripts have warning and failure messages that can be localized according to the needs of the user. To localize these messages, the corresponding .strings file (`InstallationCheck.strings` or `VolumeCheck.strings`) must be created for each localization.

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

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.
3. Do one of the following:
   - To add a postflight script that removes deleted files from computers, click the disclosure triangle next to **Snapshots**. Then Control-click (or right-click) the Deleted Files heading and choose **Add postflight Shell Script**.

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

- To add another type of script, Control-click (or right-click) **Scripts** and choose the script you want to add.



Scripts

To add a script to the package, right-click the Scripts folder and select the script you wish to add.

There are default scripts in Perl and Bash for all 8 scripts that are supported for a package.

Scripts are only added to PKGs.

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

4. (Optional) Select the script in the sidebar to view or change its contents.

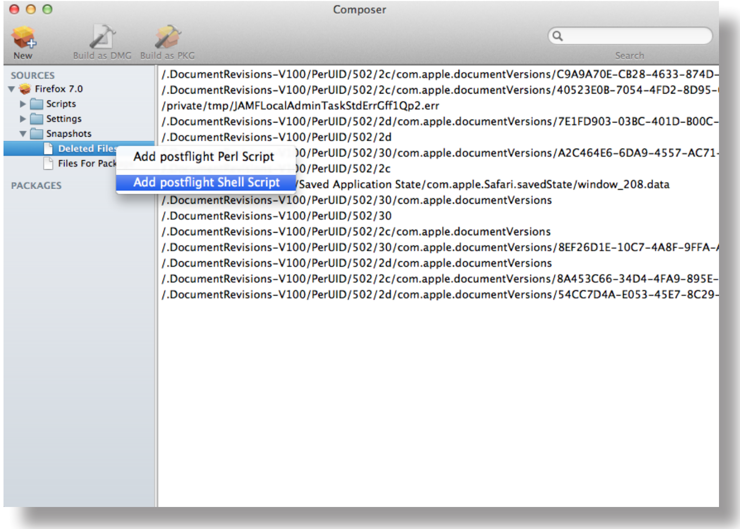
Adding a Postflight Script that Removes Deleted Files from Computers

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

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

1. Open Composer and authenticate locally.
2. Click the disclosure triangle next to the package source in the sidebar.
3. Click the disclosure triangle next to **Snapshots**.
4. Select the Deleted Files heading to view the deleted files captured by the snapshot.

5. Control-click (or right-click) the Deleted Files heading and choose **Add postflight Shell Script**.



```
/.DocumentRevisions-V100/PerUID/502/2c/com.apple.documentVersions/C9A9A70E-CB28-4633-874D-
/.DocumentRevisions-V100/PerUID/502/2c/com.apple.documentVersions/40523E0B-7054-4FD2-8D95-
/private/tmp/JAMFLocalAdminTaskStdErrGff1Qp2.err
/.DocumentRevisions-V100/PerUID/502/2d/com.apple.documentVersions/7E1FD903-03BC-401D-B00C-
/.DocumentRevisions-V100/PerUID/502/2d
00/PerUID/502/30/com.apple.documentVersions/A2C464E6-6DA9-4557-AC71-
00/PerUID/502/2c
/Saved Application State/com.apple.Safari.savedState/window_208.data
/.DocumentRevisions-V100/PerUID/502/30/com.apple.documentVersions
/.DocumentRevisions-V100/PerUID/502/30
/.DocumentRevisions-V100/PerUID/502/2c/com.apple.documentVersions
/.DocumentRevisions-V100/PerUID/502/30/com.apple.documentVersions/8EF26D1E-10C7-4A8F-9FFA-
/.DocumentRevisions-V100/PerUID/502/2d/com.apple.documentVersions
/.DocumentRevisions-V100/PerUID/502/2c/com.apple.documentVersions/8A453C66-34D4-4FA9-895E-
/.DocumentRevisions-V100/PerUID/502/2d/com.apple.documentVersions/54CC7D4A-E053-45E7-8C29-
```

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

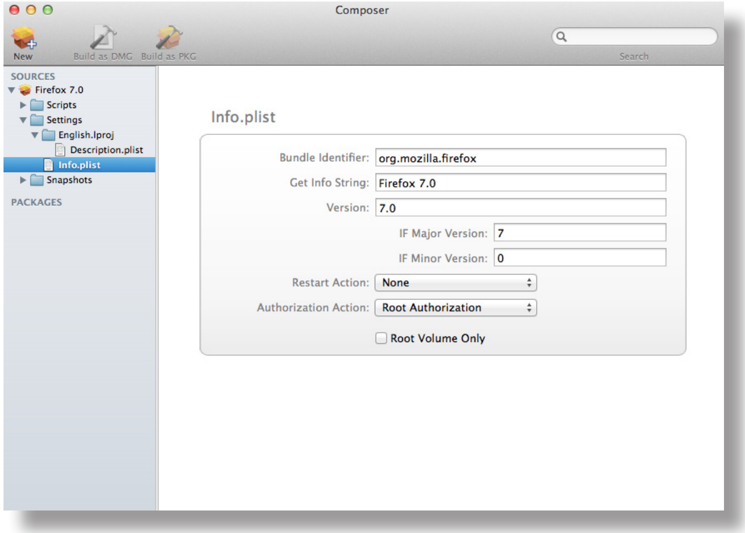
6. (Optional) Select the script in the sidebar to view or change its contents.

Editing PLIST Files in Package Sources

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.

Editing the Info.plist File in a Package Source

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.



Info.plist

Bundle Identifier: org.mozilla.firefox
Get Info String: Firefox 7.0
Version: 7.0
IF Major Version: 7
IF Minor Version: 0
Restart Action: None
Authorization Action: Root Authorization
☐ Root Volume Only

Bundle Identifier
Identifies what kind of package it is. 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.

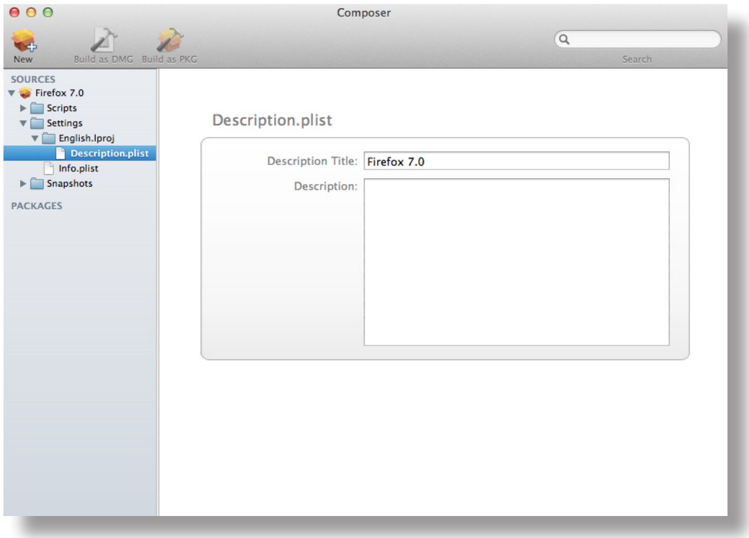
Root Volume Only
Indicates the package can only be installed to the root volume.

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.

Editing the Description.plist File in a Package Source

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.



Description Title: Firefox 7.0
Description:

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.

Localizations

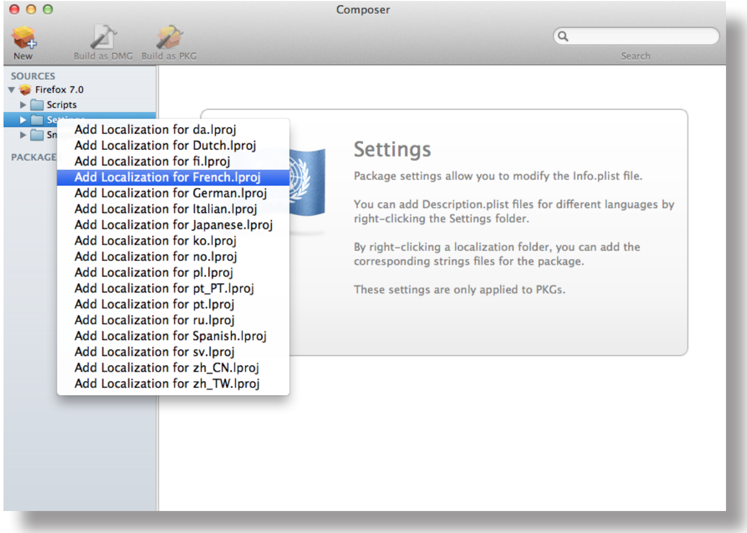
Localizations allow you to customize the language used when displaying package information to a user. By default, a package source only includes an English localization.

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`

Adding Localizations to Package Sources

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


Composer
New
Build as DMG
Build as PKG
Search
SOURCES
Firefox 7.0
Scripts
Settings
Sn
PACKAGE
Add Localization for da.lproj
Add Localization for Dutch.lproj
Add Localization for fi.lproj
Add Localization for French.lproj
Add Localization for German.lproj
Add Localization for Italian.lproj
Add Localization for Japanese.lproj
Add Localization for ko.lproj
Add Localization for no.lproj
Add Localization for pl.lproj
Add Localization for pt_PT.lproj
Add Localization for pt.lproj
Add Localization for ru.lproj
Add Localization for Spanish.lproj
Add Localization for sv.lproj
Add Localization for zh_CN.lproj
Add Localization for zh_TW.lproj

Settings

Package settings allow you to modify the Info.plist file.

You can add Description.plist files for different languages by right-clicking the Settings folder.

By right-clicking a localization folder, you can add the corresponding strings files for the package.

These settings are only applied to PKGs.

Adding and Editing Files for a Localization

You can include two kinds of files in a localization:

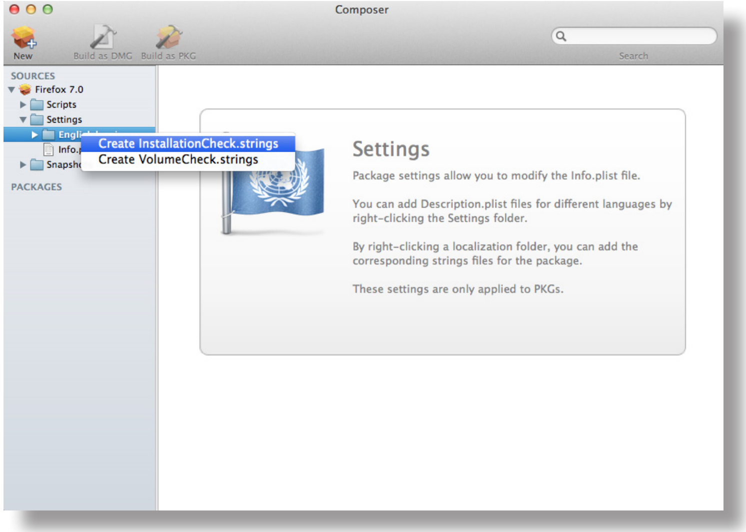
- **Description.plist files**—These files display the title of a package and its description in the Installer application. Each localization contains a `description.plist` file by default. For instructions on how to edit these files, see Editing PLIST Files in Package Sources.
- **Strings files**—`VolumeCheck.strings` 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 Package Sources.

1. Open Composer and authenticate locally.

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

2. Click the disclosure triangle next to **Settings**.

3. 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**.



Settings

Package settings allow you to modify the Info.plist file.

You can add Description.plist files for different languages by right-clicking the Settings folder.

By right-clicking a localization folder, you can add the corresponding strings files for the package.

These settings are only applied to PKGs.

4. Click the .strings file to change 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 kinds 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.

Building a PKG

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 Composer Preferences.

1. Open Composer and authenticate locally.
2. Select the package source you want to build as a PKG from the Sources list in the sidebar.
3. In the toolbar, click **Build as PKG** .

> ***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 to Package Sources.

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

Building a DMG

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.

1. Open Composer and authenticate locally.
2. Select the package source you want to build as a DMG from the Sources list in the sidebar.
3. In the toolbar, click **Build as DMG** .
4. 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 preconfigured 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 System Keychain
This option removes the System keychain from the OS to ensure that a new System keychain is created. This can prevent the "This computer already exists" error when binding a computer to a directory service.

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.

Installing and Configuring the OS

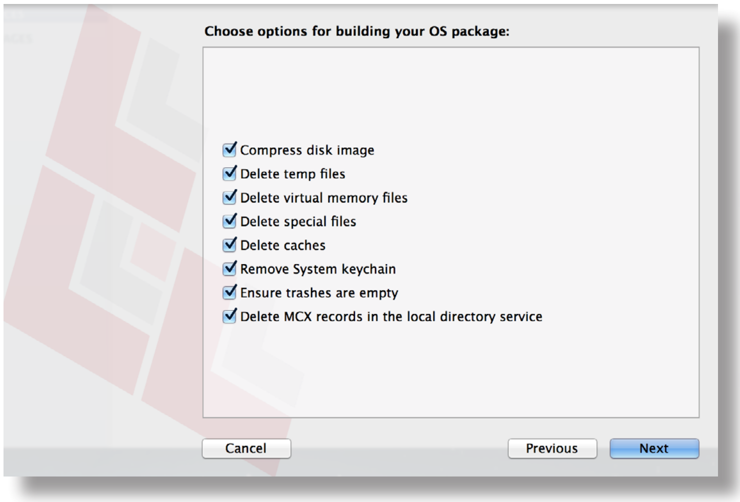
For instructions on how to install and configure the OS before building an OS package, see the following Knowledge Base article:

Creating a Minimal Base OS Image

Packaging the OS

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

1. Open Composer and authenticate locally.
2. In the toolbar, click **New** .
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 click **Next**.



Choose options for building your OS package:

☑ Compress disk image
☑ Delete temp files
☑ Delete virtual memory files
☑ Delete special files
☑ Delete caches
☑ Remove System keychain
☑ Ensure trashes are empty
☑ Delete MCX records in the local directory service

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

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.

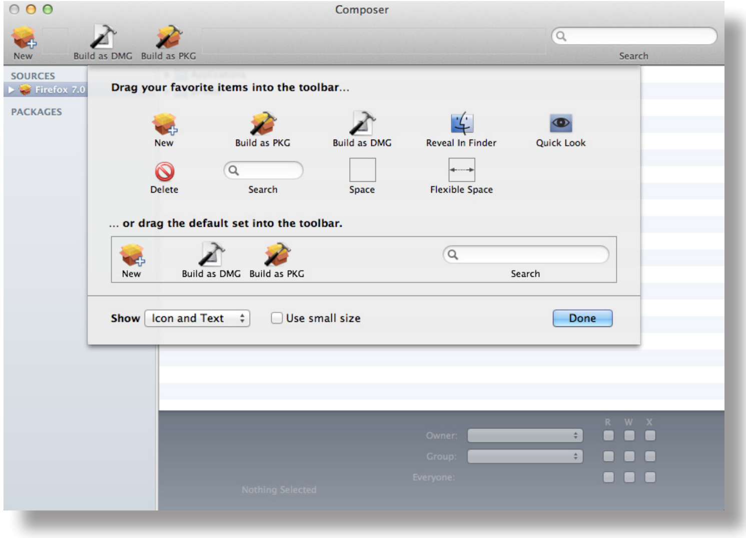
This section provides a detailed explanation of Composer preferences.

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**, and then drag desired items to the toolbar.

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



Drag your favorite items into the toolbar...

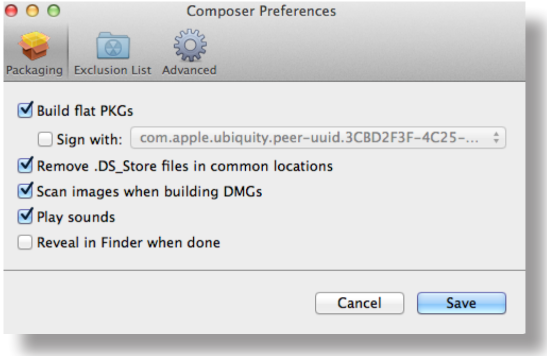
... or drag the default set into the toolbar.

Show Icon and Text

□ Use small size

Package Preferences

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



☑ Build flat PKGs

□ Sign with: com.apple.ubiquity.peer-uuid.3CBD2F3F-4C25-...

☑ Remove .DS_Store files in common locations

☑ Scan images when building DMGs

☑ Play sounds

□ Reveal in Finder when done

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 change 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.

For instructions on how to obtain an installer certificate from Apple's Developer Certificate Utility, see the following Knowledge Base article:

Obtaining an Installer Certificate from Apple's Developer Certificate Utility

To install a signed PKG, computers must have a Certification Authority intermediate certificate from Apple in the System keychain in Keychain Access.. For instructions on how to obtain this certificate and import it to the System keychain on managed computers, see the following Knowledge Base article:

Importing a Certification Authority Intermediate Certificate from Apple to the System Keychain

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

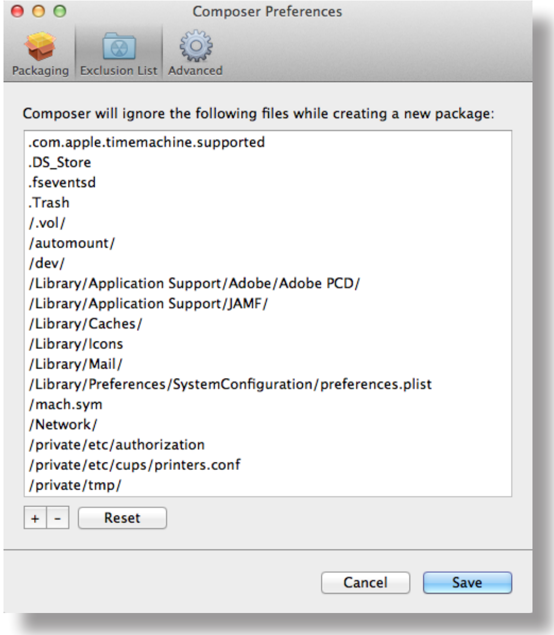
When this option is enabled, Composer reveals newly built packages in a Finder window.

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 **Exclusion List** 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.

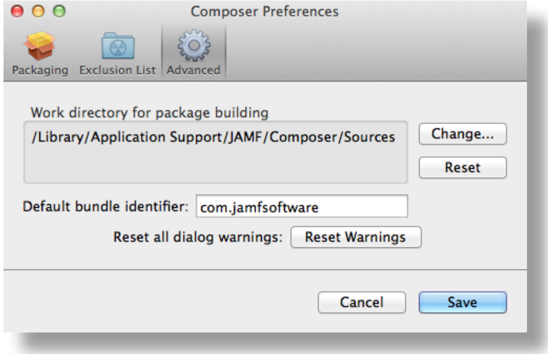


Composer will ignore the following files while creating a new package:

```
.com.apple.timemachine.supported
.DS_Store
.fseventsd
.Trash
/.vol/
/automount/
/dev/
/Library/Application Support/Adobe/Adobe PCD/
/Library/Application Support/JAMF/
/Library/Caches/
/Library/Icons
/Library/Mail/
/Library/Preferences/SystemConfiguration/preferences.plist
/mach.sym
/Network/
/private/etc/authorization
/private/etc/cups/printers.conf
/private/tmp/
```

Advanced Preferences

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



Work directory for package building: /Library/Application Support/JAMF/Composer/Sources

Default bundle identifier: com.jamfsoftware

Reset all dialog warnings:

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 privileges enabled.

To change this directory, click **Change**, 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`".

Inventory

Computer Inventory Collection

By default, inventory is collected from computers using the "Update Inventory" policy that is created automatically when you install the JAMF Software Server (JSS). This policy collects inventory from all computers once every week.

You can make changes to the default inventory collection policy at any time. In addition, if you want more control over inventory collection, you can create additional inventory collection policies as needed.

Related Information

For related information, see the following sections in this guide:

- Managing Policies

  Find out how to create and edit policies.
- Policy Payload Reference

  Learn about each payload in the policy interface.

Computer Inventory Collection Settings

Computers can submit many types of inventory information to the JAMF Software Server (JSS). Basic inventory information—such as hardware, operating system, user and location information, storage, and applications—is collected automatically.

The Computer Inventory Collection settings in the JSS allow you to collect the following additional items:

- Local user accounts, with the option to include home directory sizes and/or hidden system accounts
- Printers
- Active services
- Last backup date/time for managed mobile devices that are synced to computers
- User and location from an LDAP directory service (only available if an LDAP server is set up in the JSS)
- Package receipts
- Available software updates
- Application Usage information
- Fonts
- Plug-ins

You can also use the Computer Inventory Collection settings to specify custom search paths to use when collecting applications, fonts, and plug-ins.

For descriptions of the information collected for each of these items, as well as information on the items that are collected automatically, see Viewing and Editing Inventory Information for a Single Computer.

Time and Traffic Estimates for Collecting Additional Items

Collecting additional inventory items may add reporting time and network traffic to the inventory process.

The following table provides estimates of how much time and traffic may be added when collecting user home directory sizes, available software updates, fonts, and plug-ins. These estimates are based on a MacBook Pro with approximately 300 GB of user home directories, 100 applications, 300 fonts, and 900 plug-ins.

Additional Inventory Item	Time (Seconds)	Traffic (KB)
(No additional items)	9	102
Home directory sizes	25	104
Available software updates	110	104
Fonts	10	128
Plug-ins	13	248

The following table provides estimates of how much time and traffic may be added when collecting Application Usage information. These estimates are based on a MacBook Pro with eight applications used per day, one week between inventory reports, and one computer user.

Additional Inventory Item	Time (Seconds)	Traffic (KB)
(No additional items)	16	24
Application Usage information	17	48

Search Paths for Collecting Applications, Fonts, and Plug-ins

The following table lists the default search paths that are used when collecting applications, fonts, and plug-ins from computers on the Mac and Windows platforms.

Collected Item	Mac Platform Default Search Paths	Windows Platform Default Search Paths
Applications (and Application Usage information, if collecting)	/Applications/	C:\Program Files\
Fonts	/Library/Fonts/ /System/Library/Fonts/ /Library/Application Support/Adobe/Fonts/ ~/Library/Fonts/ (collected at the user level for each account)	C:\Windows\Fonts\
Plug-ins	/Library/Internet Plug-Ins/	--

If you store these items in locations not listed in the table, you can use the Computer Inventory Collection settings to specify custom search paths for those locations.

Configuring the Computer Inventory Collection Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Inventory Collection** .
5. Click **Edit**.
6. On the General pane, select the checkbox for each inventory item you want to collect.

7. To collect Application Usage information or add custom paths in which to search for applications, do the following:
    a. Click the **Software** tab, and then click **Applications**.
    b. To collect Application Usage information, select the **Collect Application Usage Information** checkbox.
    c. To add a custom search path, click **Add** + . Then enter the full path for the location you want to search and the platform to which it applies.
    d. Repeat step c to specify additional custom search paths as needed.
8. To collect fonts and add custom paths in which to search for fonts, do the following:
    a. Click the **Software** tab, and then click **Fonts**.
    b. Select the **Collect Fonts** checkbox.
    c. To add a custom search path, click **Add** + . Then enter the full path for the location you want to search and the platform to which it applies.
    d. Repeat step c to specify additional custom search paths as needed.
9. To collect plug-ins and add custom paths in which to search for plug-ins, do the following:
    a. Click the **Software** tab, and then click **Plug-ins**.
    b. Select the **Collect Plug-ins** checkbox.
    c. To add a custom search path, click **Add** + . Then enter the full path for the location you want to search and the platform to which it applies.
    d. Repeat step c to specify additional custom search paths as needed.
10. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- Extension Attributes

  Find out how to create extension attributes that allow you to collect almost any type of data from computers.

- Simple Computer Searches

  Learn how to quickly search the items in your inventory for a general range of results.

- Advanced Computer Searches

  Learn how to create and save an advanced computer search.

- Viewing and Editing Inventory Information for a Single Computer

  Find out how to view and edit inventory information for a single computer.

- Viewing Application Usage Logs for a Single Computer

  Find out how to view Application Usage logs for a single computer.

Computer Extension Attributes

Computer extension attributes are custom fields that you can create to collect almost any type of data from a computer. For example, you can create an extension attribute to collect the host name of a computer or collect data about the activity of the company's antivirus software.

There are several ways to create a computer extension attribute in the JAMF Software Server (JSS). You can manually create the extension attribute, use an extension attribute template available in the JSS, or upload an extension attribute template obtained from JAMF Nation.

When you create a computer extension attribute, you specify the following information:

- Type of data being collected, such as string, integer, or date
- Inventory category in which to display the extension attribute in the JSS, such as Hardware or Operating System
- Input type, which determines how the extension attribute is populated with data
- Pane on which to display the extension attribute in Recon (text field and pop-up menu input types only)
- Script to use to collect data from computers (script input type only)

Extension attributes can add time and network traffic to the inventory process depending on the type of data you choose to collect and the input type used to collect it.

Computer Extension Attribute Input Types

You can choose to populate the value of a computer extension attribute using any of the following input types:

- **Text field—**This displays a text field in Recon and in computer inventory information. You can enter a value in the field when enrolling a computer using Recon, or at any time using the JSS. Only extension attributes created manually can be populated using a text field.
- **Pop-up menu—**This displays a pop-up menu in Recon and in computer inventory information. You can choose a value from the pop-up menu when enrolling a computer using Recon, or at any time using the JSS. Only extension attributes created manually can be populated using a pop-up menu.
- **Script—**This allows you to run a script that populates the extension attribute each time a computer submits inventory to the JSS. Extension attributes created manually can be populated by a script. Extension attributes created from a template are always populated by a script.
- **LDAP Attribute Mapping**—This populates the extension attribute with the value for an LDAP attribute. It also generates a variable that can be used to populate configuration profile settings with values for the LDAP attribute. The variable is `$EXTENSIONATTRIBUTE_<#>`, where <#> is the extension attribute ID. For more information on payload variables for configuration profiles, see OS X Configuration Profiles.

Computer Extension Attributes Populated by a Script

When an extension attribute is populated by a script, the text between the `<result></result>` tag is stored in the JSS.

For OS X computers, scripts can be written in any language that has an interpreter installed. The most common interpreters are:

```
/bin/bash
/bin/sh
/usr/bin/perl
/usr/bin/python
```

All scripts must start with a shebang (`#!`) followed by the absolute path to the interpreter. For example, the script for an extension attribute that collects the host name from OS X computers looks like this:

```
#!/bin/sh
echo "<result>`hostname 2>&1`</result>"
```

For Windows computers, scripts can be written in VBScript, Batch file, and PowerShell.

Note: PowerShell scripts only run on computers that have the components necessary to run the script.

Requirements

To create a computer extension attribute with the "LDAP Attribute Mapping" input type, you need:

- An LDAP server set up in the JSS (For more information, see Integrating with LDAP Directory Services.)
- The Computer Inventory Collection settings configured to collect user and location information from LDAP (For more information, see Computer Inventory Collection Settings.)

Manually Creating a Computer Extension Attribute

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Extension Attributes** 📋.
5. Click **New** + .
6. Configure the settings on the pane.
7. Click **Save**.

If the extension attribute has the "LDAP Attribute Mapping" input type, the LDAP attribute variable is displayed on the pane.

Creating a Computer Extension Attribute From a Template

The JSS has built-in templates for many commonly used extension attributes.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the ”Computer Management–Management Framework” section, click **Extension Attributes** .
5. Click **New From Template** .
6. Click the extension attribute template you want to use.
7. Make changes to the settings as needed.
8. Click **Save**.

Uploading a Template for Computer Extension Attribute

You can create an extension attribute by uploading an extension attribute template obtained from JAMF Nation. Extension attribute templates are available in JAMF Nation at:

https://jamfnation.jamfsoftware.com/extensionAttributes.html

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the ”Computer Management–Management Framework” section, click **Extension Attributes** .
5. Click **Upload** ↑ and upload the extension attribute template.
6. Make changes to the settings as needed.
7. Click **Save**.

Cloning, Editing, or Deleting a Computer Extension Attribute

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.

3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.

4. In the "Computer Management–Management Framework" section, click **Extension Attributes** .

5. Click the extension attribute you want to clone, edit, or delete.

6. Do one of the following:

   - To clone the extension attribute, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the extension attribute, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the extension attribute, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Computer Inventory Display Settings

  You can display extension attributes in the results of a simple computer search.

- Viewing and Editing Inventory Information for a Single Computer

  You can view the extension attributes collected from a single computer and edit non-script extension attribute values for that computer.

- Smart Computer Groups

  You can create smart computer groups based on extension attributes.

Computer Inventory Display Settings

The Computer Inventory Display settings allow you to choose which attribute fields to display in the results of a simple computer search.

Configuring the Computer Inventory Display Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Inventory Display** .
5. On each pane, select or deselect the checkbox for each attribute field you want to display or remove.
6. Click **Save**.

Related Information

For related information, see the following section in this guide:

Simple Computer Searches
Find out how to quickly search the items in your inventory for a general range of results.

Peripherals

Peripherals are miscellaneous items, such as keyboards or scanners, for which you can store information in the JAMF Software Server (JSS).

The first step to storing peripheral information is to create one or more peripheral types. You can add custom text fields and pop-up menus to each peripheral type, allowing you to customize the information that is stored. For example, if you plan to store the serial numbers of keyboards, you can create a peripheral type called "Keyboard" and add a "Serial Number" text field. Peripheral types also serve as categories that allow you to group peripherals in inventory.

After creating one or more peripheral types, you can add peripherals to the JSS. When you add a peripheral, you specify the type of peripheral you are adding. Then you can do the following:

- Enter user and location information
- Assign the peripheral to a computer
- Enter purchasing information
- Attach files

Creating a Peripheral Type

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management - Management Framework" section, click **Peripheral Types** .
5. Click **New** + .
6. Enter a display name for the peripheral type.
7. Add one or more custom fields:

   a. Click **Add** + .

   b. Enter a label for the field.

   c. Choose "Text" or "Menu" from the **Type** pop-up menu.

   If you chose "Menu", click **Edit Menu** and configure pop-up menu options as needed.

   d. Choose a position number from the **Order** pop-up menu.

   A field with a position number of "1" is displayed first when adding or viewing a peripheral.

   e. Repeat steps a through d as needed.
8. Click **Save**.

Adding a Peripheral

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Choose "Peripherals" from the **Search** pop-up menu and press the Enter key.
5. Click **New** + .
6. Choose a peripheral type and click **Next**.
7. Specify information about the peripheral using the fields and options in each category.
8. Click **Save**.

Cloning, Editing, or Deleting a Peripheral Type

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management - Management Framework" section, click **Peripheral Types** .
5. Click the peripheral type you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the peripheral type, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the peripheral type, click **Edit** and make changes as needed. Then click **Save**.
   - To delete peripheral type, click **Delete** and then click **Delete** again to confirm.

Cloning, Editing, or Deleting a Peripheral

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.

4. Choose “Peripherals” from the **Search** pop-up menu.

5. Enter one or more search terms in the field provided.

   You can base peripheral searches on peripheral type, customizable peripheral fields, or bar code.

   For information on the syntax to use to refine your search, see Search Syntax.

6. Press the Enter key.

   The list of search results is displayed.

7. Click the peripheral you want to clone, edit, or delete.

8. Do one of the following:

   - To clone the peripheral, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the peripheral, click **Edit** and make changes as needed. Then click **Save**.
   - To delete peripheral, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

- Simple Computer Searches

  Learn how to quickly search the peripherals in your inventory for a general range of results.
- Viewing and Editing Inventory Information for a Single Computer

  You can view the peripherals associated with a single computer.

Simple Computer Searches

A simple computer search functions like a search engine, allowing you to quickly search the items in your inventory for a general range of results.

The following table shows the items that you can search by and the attributes on which you can base each search:

Inventory Item	Searchable Attributes
Computers (This includes both managed and unmanaged computers.)	Computer name MAC address Bar code IP address Asset tag Serial number Username Full name Email address Phone number Position Department Building Room
Peripherals	Peripheral type Customizable peripheral fields Bar code
Applications	Application name
Local User Accounts	Username
Application Usage	Application name
Fonts	Font name
Package Receipts	Package receipt name
Plug-ins	Plug-in name
Printers	Printer name
Services	Service name
Software Updates	Software update name Software update version

Note: Computers, peripherals, and applications are searchable by default. The other items are searchable if the JSS is configured to collect them as inventory. For more information, see Computer Inventory Collection Settings.

Search Syntax

The following table explains the syntax to use for refining a simple search:

Function	Usage	Example
Wildcard search	Use an asterisk (*) before or after any characters or search terms to return all results that include those characters or terms. Use an asterisk (*) without any other characters or terms to return all results for the item you are searching.	Enter "Adobe*" to return all results that begin with "Adobe". Enter "*.sh" to return all files with the ".sh" extension.
Include all search terms	Use a comma (,) between search terms to return results that include those search terms.	Enter "Microsoft, Adobe" to return all results that include "Microsoft" and "Adobe".
Exclude a search term	Use a hyphen (-) before a search term to exclude that term from all results.	Enter "Microsoft, -Word" to return all results for "Microsoft" except those that include "Word".
Return all results	Perform a search with no criteria in the search field to return all results for the item you are searching. This only works when searching for computers or peripherals.	--

Performing a Simple Computer Search

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Choose an item from the **Search** pop-up menu.
5. Enter one or more search terms in the field(s) provided.
   For information on the syntax to use to refine your search, see Search Syntax.

6. Press the Enter key.

   The list of search results is displayed.

   If you searched for an item other than computers or peripherals, you can view the computers associated with a result by clicking **Expand** ⊕ next to the result. You can also change the item on which the results are based by choosing an item from the pop-up menu at the top of the page.

Related Information

For related information, see the following sections in this guide:

- Viewing and Editing Inventory Information for a Single Computer

  Find out how to view and edit inventory information for a single computer.
- Computer Reports

  Find out how to export the data in your search results to different file formats.
- Performing Mass Actions for Computers

  Find out how to perform actions on the results of a computer search.
- Advanced Computer Searches

  Lean how to create and save an advanced computer search.
- Computer Inventory Display Settings

  Learn how to change the attribute fields displayed in the results of a simple computer search.

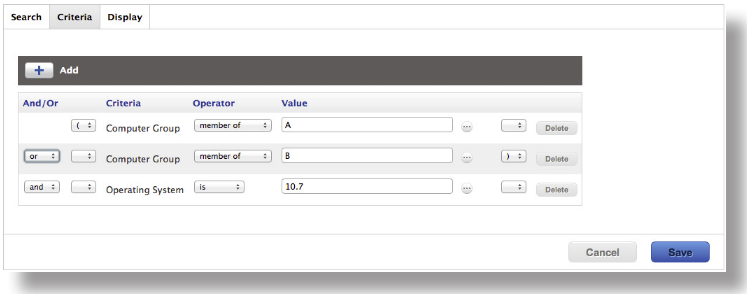
Advanced Computer Searches

Advanced computer searches allow you to use detailed search criteria to search the managed and unmanaged computers in the JAMF Software Server (JSS). These types of searches give you more control over your search by allowing you to do the following:

- Generate specific search results.
- Specify which attribute fields to display in the search results.
- Save the search.

Creating an Advanced Computer Search

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the Search pane to configure basic settings for the search.
   To save the search, select the **Save this Search** checkbox.
6. Click the **Criteria** tab and add criteria for the search:
   a. Click **Add** + .
   b. Click **Choose** for the criteria you want to add.
      To display additional criteria, click **Choose** for "Other Criteria".
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse** ⋯ .
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.



And/Or		Criteria	Operator	Value		
	(	Computer Group	member of	A		Delete
or		Computer Group	member of	B	)	Delete
and		Operating System	is	10.7		Delete

9. Click the **Display** tab and select the attribute fields you want to display in your search results.

10. Click **Save**.

    Operations in the search take place in the order they are listed (top to bottom).

    The results of a saved search are updated each time computers check in with the JSS and meet or fail to meet the specified search criteria.

    To view the search results, click **View**.

Cloning, Editing, or Deleting a Saved Advanced Computer Search

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Click the advanced computer search you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the search, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the search, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the search, click **Delete**. Then click **Delete** again to confirm.

Viewing Advanced Computer Search Results

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Click the advanced computer search you want to view the results for.
5. Click **View**.

   The list of search results is displayed.

Related Information

For related information, see the following sections in this guide:

- Computer Reports

  Find out how to export the data in your search results to different file formats.
- Performing Mass Actions for Computers

  Find out how to perform actions on the results of a computer search.
- Viewing and Editing Inventory Information for a Single Computer

  Find out how to view and edit inventory information for a single computer.
- Simple Computer Searches

  Learn how to quickly search the items in your inventory for a general range of results.

Computer Reports

The data displayed in smart or static group membership lists, computer search results, or lists of license usage matches can be exported from the JAMF Software Server (JSS) to the following file formats:

- Comma-separated values file (.csv)
- Tab delimited text file (.txt)
- XML file

You can change the way the data is organized by basing the export on any of the following inventory items:

- Computers
- Applications
- Fonts
- Plug-ins
- Packages installed by the Casper Suite
- Packages installed by Installer.app/Software Update
- Cached packages
- Local user accounts
- Mapped printers
- Available software updates
- Running services
- Computer groups
- Licensed software

The data is displayed in alphanumeric order by the selected inventory item.

Creating Computer Reports

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

   Note: You can only create a report from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Export**.
5. Follow the onscreen instructions to export the data.

   The report downloads immediately.

Performing Mass Actions for Computers

Mass actions allow you to perform potentially tedious tasks for multiple computers at the same time. You can use the JSS to perform the following mass actions:

- Edit the building or department.
- Edit the site.
- Edit the management account.
- Look up and populate purchasing information from Apple's Global Service Exchange (GSX).
- Send a mass email to users.
- Edit Autorun data.
- Delete Autorun data.
- Delete the computers from the JSS.

Mass actions can be performed on smart or static group membership lists, computer search results, or lists of license usage matches.

Mass Editing the Building or Department for Computers

Mass editing the building or department for computers allows you to add the computers to a building or department or change the building or department they belong to.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
    - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
    - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

    Note: You can only perform mass actions from a simple computer search if you searched by computers.

    - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Edit the Building and Department**.

    This option is only displayed if there are one or more buildings or departments in the JSS. (For more information, see Buildings and Departments.)
6. Follow the onscreen instructions to edit the building or department.

Mass Editing the Site for Computers

Mass editing the site for computers allows you to add the computers to a site or change the site they belong to.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

> ***Note:*** You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Edit the Site**.

   This option is only displayed if there are one or more sites in the JSS. (For more information, see Sites.)
6. Follow the onscreen instructions to edit the site.

Mass Editing the Management Account for Computers

Mass editing the management account for computers allows you to change the username and password for the computers' management accounts. This can be useful when the management account is from a directory service and has been changed.

Mass editing the management account updates the username and password in the JSS, not on the computers.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

> ***Note:*** You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)

4. At the bottom of the list, click **Action**.
5. Select **Edit the Management Account Information**.
6. Follow the onscreen instructions to edit the management account.

Mass Looking up and Populating Purchasing Information for Computers

You can mass look up purchasing information from Apple's Global Service Exchange (GSX) and populate the information in the JSS if desired.

This requires a GSX connection set up in the JSS. (For more information, see Integrating with GSX.)

Note: GSX may not always return complete purchasing information. Only the information found in GSX is returned.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

Note: You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Look up Purchasing Information from GSX**.
   This option is only displayed if there is a GSX connection set up in the JSS.
6. Follow the onscreen instructions to look up and populate the purchasing information.

Sending a Mass Email to Computer Users

You can send a mass email to users associated with the computers in the JSS. The email is sent to the email address associated with each computer.

This requires an SMTP server set up in the JSS. (For more information, see Integrating with an SMTP Server.)

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.

3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

     Note: You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Send Email**.

   This option is only displayed if there is an SMTP server set up in the JSS.
6. Follow the onscreen instructions to create and send the email.

Mass Editing Autorun Data

You can mass edit Autorun data for computers.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

Note: You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Edit Autorun Data**.
6. Follow the onscreen instructions to edit the Autorun data.

Mass Deleting Autorun Data

You can mass delete Autorun data for computers.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.

3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

> ***Note:*** You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Delete Autorun Data.**

   This option is only displayed if there is Autorun data in the JSS.
6. Follow the onscreen instructions to delete the Autorun data.

Mass Deleting Computers

You can mass delete computers from the JSS.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Do one of the following:
   - View computer group memberships. (For more information, see Smart Computer Groups or Static Computer Groups.)
   - View simple or advanced computer search results. (For more information, see Simple Computer Searches or Advanced Computer Searches.)

> ***Note:*** You can only perform mass actions from a simple computer search if you searched by computers.

   - View license usage matches. (For more information, see Viewing License Usage.)
4. At the bottom of the list, click **Action**.
5. Select **Delete Computers**.
6. Follow the onscreen instructions to delete the computers.

Related Information

For related information, see the following sections in this guide:

- Viewing and Editing Inventory Information for a Single Computer

  Find out how to edit the building, department, site, purchasing information, or management account for a single computer.

- Autorun Imaging

  Find out how to create, edit, or delete Autorun data for a single computer.

For related information, see the following Knowledge Base article:

Removing JAMF Software Components from Computers
Find out how to remove all Casper Suite-related components from computers that have been deleted from the JSS.

Viewing and Editing Inventory Information for a Single Computer

The JAMF Software Server (JSS) stores detailed inventory information for each computer. You can view and edit this information right from the JSS.

The following table describes the information that you can view and edit for each computer:

Category	Description	Editable Fields
General	View general information about the computer, including computer name, IP address, and management account. Disable management tasks for the computer.	Computer name Site Asset tag Bar code 1 Bar code 2 IP address Username and password for the management account
Hardware	View hardware information, including make, model, and MAC address(es).	UDID Primary MAC address Secondary MAC address
Operating System	View information about the operating system, including version number and build number.	--
User and Location	View information about the primary user and the computer's physical location. Look up and populate user information from an LDAP directory service. (This requires an LDAP server set up in the JSS. For more information, see Integrating with LDAP Directory Services.)	Username Full name Email address Phone number Department Building Room Position

Category	Description	Editable Fields
Purchasing	View purchasing information, including PO details, warranty information, and purchasing contact. Look up and populate purchasing information from Apple's Global Service Exchange (GSX). (This requires a GSX connection set up in the JSS. For more information see Integrating with GSX.)	Purchased or leased PO number PO date Vendor Warranty expiration AppleCare ID Lease expiration Purchase price Life expectancy Purchasing account Purchasing contact
Extension Attributes	View custom data collected using extension attributes.	Non-script extension attributes
Storage	View storage information, including model, serial number, drive capacity, and number of partitions. View information about each partition, including size, percent used, and the FileVault 2 encryption state.	--
Disk Encryption	View FileVault 2 information for the boot partition, including the encryption state, the disk encryption configuration used, and the FileVault 2 enabled users. View the FileVault 2 encryption state for any non-boot partitions.	--
Peripherals	View a list of peripherals associated with the computer. View information about a peripheral. Delete a peripheral.	--
Licensed Software	View a list of licensed software titles installed on the computer.	--
Applications	View a list of applications installed on the computer.	--
Fonts	View a list of fonts installed on the computer.	--
Plug-ins	View a list of plug-ins installed on the computer.	--
Profiles	View a list of profiles installed on the computer.	--

Category	Description	Editable Fields
Certificates	View a list of certificates installed on the computer.	--
Package Receipts	View a list of packages installed by Installer.app or Software Update. View a list of packages installed or cached by the Casper Suite.	--
Software Updates	View a list of software updates available for the computer.	--
Local User Accounts	View a list of local user accounts and information about them, including username, UID, home directory, and the Legacy FileVault or FileVault 2 enabled status.	--
Printers	View a list of printers mapped to the computer and information about those printers, including model, location, and URI.	--
Services	View a list of active services.	--
Attachments	View a list of files attached to the inventory record. Upload attachments. Delete attachments.	--

Viewing Inventory Information for a Single Computer

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view information for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

   The computer's inventory information is displayed.

5. Use the categories to view information for the computer.

Editing Inventory Information for a Single Computer

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to edit information for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item name to view the computers related to that item.

   The computer's inventory information is displayed.

5. Select the category that contains the information you want to edit and click **Edit**.

6. Make changes as needed.

   If you are editing user and location information or purchasing information, you can click **Search** 🔍 to look up and populate information from an LDAP directory service or Apple's Global Service Exchange (GSX).

   > ***Note:*** This button is only displayed if you have an LDAP server or a GSX connection set up in the JSS.

7. Click **Save**.

Viewing Management Information for a Single Computer

The JAMF Software Server (JSS) allows you to view the following management information for a single computer:

- Pending management commands
- Policies
- OS X configuration profiles
- Managed Preferences
- Restricted software
- FileVault 2 recovery key(s)
- Group memberships

Requirements

To view pending management commands for a computer, the computer and the JSS must meet the requirements for sending an OS X remote command or installing an OS X configuration profile. (For more information, see OS X Remote Commands or OS X Configuration Profiles.)

Viewing the Pending Management Commands for a Single Computer

When viewing management information for a single computer, you can view a list of pending management commands for the computer. The list includes all pending actions related to sending an OS X remote command and installing or removing an OS X configuration profile.

You can also cancel a pending management command.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.
   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view pending management commands for.
   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab.

   A list of pending management commands for the computer is displayed.

   > ***Note:*** You cannot view pending management commands if the MDM profile has been removed from the computer.

6. To cancel a pending management command, click **Cancel** for the command.

Viewing Policies for a Single Computer

When viewing management information for a single computer, you can view a list of policies that have the computer in the scope. You can also view a list of policies for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view policies for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab, and then click the **Policies** category.

   A list of policies for the computer is displayed.

6. To view policies for a specific user, enter the username in the **Username** field and click **Update**.

   A list of policies for the user is displayed.

Viewing Configuration Profiles for a Single Computer

When viewing management information for a single computer, you can view a list of OS X configuration profiles that have the computer in the scope. You can also view a list of configuration profiles for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view configuration profiles for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab, and then click the **Configuration Profiles** category.

   A list of configuration profiles for the computer is displayed.

6. To view configuration profiles for a specific user, enter the username in the **Username** field and click **Update**.

   A list of configuration profiles for the user is displayed.

Viewing Managed Preferences for a Single Computer

When viewing management information for a single computer, you can view a list of Managed Preference profiles that have the computer in the scope. You can also view a list of profiles for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view Managed Preferences for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab, and then click the **Managed Preferences** category.

   A list of Managed Preference profiles for the computer is displayed.

6. To view a list of Managed Preference profiles for a specific user, enter the username in the **Username** field and click **Update**.

   A list of Managed Preference profiles for the user is displayed.

Viewing Restricted Software for a Single Computer

When viewing management information for a single computer, you can view a list of restricted software that has the computer in the scope. You can also view a list of restricted software for a specific user on that computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view restricted software for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab, and then click the **Restricted Software** category.

   A list of restricted software for the computer is displayed.

6. To view restricted software for a specific user, enter the username in the **Username** field and click **Update**.

   A list of restricted software for the user is displayed.

Viewing the FileVault 2 Recovery Key for a Single Computer

When viewing management information for a single computer, you can view the File Vault 2 recovery key for the computer if FileVault 2 disk encryption has been activated using the Casper Suite. (For information on creating and deploying disk encryption configurations, see Managing Disk Encryption Configurations and Deploying Disk Encryption Configurations.)

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view the FileVault 2 recovery key for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab, and then click the **FileVault 2** category.
6. Click **Get FileVault 2 Recovery Key**.
   - If the key is an institutional recovery key, a **Download** link is displayed. Click the link to download the recovery key.
   - If the key is an individual recovery key, the recovery key is displayed on the pane.

Viewing Group Memberships for a Single Computer

When viewing management information for a single computer, you can view the smart and static group memberships for the computer.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view group memberships for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **Management** tab, and then click the **Computer Groups** category.
   A list of smart computer group memberships is displayed.
6. To view the static computer group memberships, click **Static Groups**.
   A list of static computer group memberships is displayed.

Related Information

For related information, see the following sections in this guide:

- Viewing Smart Computer Group Memberships
  Find out how to view all group memberships for a smart group.
- Viewing Static Computer Group Memberships
  Find out how to view all group memberships for a static group.

Viewing the History for a Single Computer

The JAMF Software Server (JSS) allows you to view the history for a single computer. The information you can view includes:

- Application Usage logs
- Computer Usage logs
- Policy logs
- Casper Remote logs
- Screen sharing logs
- Casper Imaging logs
- Management history (completed, pending, and failed management commands)
- Hardware/software history
- User and location history

You can also flush policy logs for a single computer.

Viewing Application Usage Logs for a Single Computer

The Application Usage logs for a single computer allow you to view a pie chart that shows the amount of time each application was in the foreground during a specified date range.

Note: You can only view Application Usage logs for a computer if the Computer Inventory Collection settings are configured to collect Application Usage information. For more information, see Computer Inventory Collection Settings.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view Application Usage logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab.

   Application Usage logs for the computer are displayed.
6. To view Application Usage logs for a different date range, specify the starting and ending dates using the **Date Range** pop-up menus. Then click **Update**.

Viewing Computer Usage Logs for a Single Computer

The Computer Usage logs for a single computer allow you to view the following information:

- Startup dates/times
- Login and logout dates/times
- Usernames used to log in and out of the computer

Note: You can only view Computer Usage logs for a computer if a startup script or login/logout hooks are configured to log Computer Usage information. (For more information, see Startup Script and Login and Logout Hooks.)

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view Computer Usage logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab, and then click the **Computer Usage Logs** category.

   Computer Usage logs for the computer are displayed.

Viewing and Flushing Policy Logs for a Single Computer

The policy logs for a single computer include a list of the policies that have run on the computer and the following information for each policy:

- The date/time that the policy ran on the computer
- The status of the policy
- The actions logged for the policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view policy logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab, and then click the **Policy Logs** category.

   Policy logs for the computer are displayed.

6. To view the actions logged for a policy, click **Show** for the policy.

   To hide the information when you are done viewing it, click **Hide**.

7. To flush a policy log, click **Flush** for the policy.

8. To flush all policies for the computer, click **Flush All** at the top of the pane.

Viewing Casper Remote Logs for a Single Computer

The Casper Remote logs for a single computer allow you to view the following information:

- The date/time that the Casper Remote event took place on the computer
- The status of the Casper Remote event
- The actions logged for the Casper Remote event

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view Casper Remote logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **History** tab, and then click the **Casper Remote Logs** category.

   Casper Remote logs for the computer are displayed.

6. To view the actions logged for a Casper Remote event, click **Show** for the event.

   To hide the information when you are done viewing it, click **Hide**.

Viewing Screen Sharing Logs for a Single Computer

The screen sharing logs for a single computer allow you to view the following information:

- The date/time that the screen sharing session took place
- The status of the screen sharing session
- Details of the screen sharing session

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view screen sharing logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **History** tab, and then click the **Screen Sharing Logs** category.

   Screen sharing logs for the computer are displayed.

Viewing Casper Imaging Logs for a Single Computer

The Casper Imaging logs for a single computer allow you to view the following information:

- The date/time that the computer was imaged
- The status of the imaging event
- The actions that took place during the imaging event

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view screen sharing logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **History** tab, and then click the **Casper Imaging Logs** category.

   Casper Imaging logs for the computer are displayed.

6. To view the actions logged for a Casper Imaging event, click **Show** for the event.

   To hide the information when you are done viewing it, click **Hide**.

Viewing Management History for a Single Computer

The management history for a single computer allows you to view lists of completed, pending, and failed management commands for the computer. The lists include all actions related to sending an OS X remote command and installing or removing an OS X configuration profile.

You can also cancel a pending management command.

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view group memberships for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **History** tab, and then click the **Management History** category.

   A list of completed management commands for the computer is displayed.

6. To view pending management commands, click **Pending Commands**.

   You can cancel a pending management command by clicking **Cancel** for the command.

7. To view failed management commands, click **Failed Commands**.

Viewing Hardware/Software History for a Single Computer

The hardware/software history for a single computer allows you to view a list of inventory reports submitted for the computer during a specified date range. Each inventory report includes hardware information for the computer, such as the operating system, make, model, and serial number, and information about any software changes that occurred since the previous inventory report.

Inventory report listings that show a change in a computer's hardware are displayed in red.

Note: You can only view software history for a computer if the Computer Inventory Collection settings are configured to collect applications, fonts, or plug-ins. For more information, see Computer Inventory Collection Settings.

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

2. Click **Computers** at the top of the page.

3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer you want to view hardware/software history for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **History** tab, and then click the **Hardware/Software History** category.

   The hardware/software history for the computer is displayed.

6. To view hardware/software history for a different date range, specify the starting and ending dates using the **Date Range** pop-up menus on the pane. Then click **Update**.

Viewing User and Location History for a Single Computer

The user and location history for a single computer allows you to view a list of the user and location information associated with the computer over time. A record of the current information is added to the list whenever changes are made to the User and Location category in the computer's inventory information.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view user and location history for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab, and then click the **User and Location History** category.

   The user and location history for the computer is displayed.

Related Information

For related information, see the following section in this guide:

Flushing Logs
Find out how to schedule automatic log flushing or manually flush logs.

Deleting a Single Computer from the JSS

You can remove a computer from your inventory by deleting it from the JAMF Software Server (JSS).

The files and folders installed during enrollment are not removed from the computer when it is deleted from the JSS. For instructions on how to remove these components, see the Removing JAMF Software Components from Computers Knowledge Base article.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.

   On a smartphone, this option is in the pop-up menu.
4. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
5. Click the computer you want to delete.

   If you performed a simple search for an item other than computers, such as computer applications, you must click **Expand** ⊕ next to an item name to view the computers related to that item.
6. Click **Delete**, and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Mass Deleting Computers
Find out how to mass delete computers from the JSS.

Computer Groups

About Computer Groups

Computer groups allow you to organize computers that share similar attributes. You can use these groups as a basis for performing advanced inventory searches, configuring the scope of remote management tasks, and viewing Application Usage logs.

There are two kinds of computer groups: smart computer groups and static computer groups. Smart computer groups are based on criteria and have dynamic memberships. Static computer groups have fixed memberships that you manually assign.

Related Information

For related information, see the following sections in this guide:

- Smart Computer Groups

  Learn how to create computer groups that are based on criteria and have dynamic memberships.
- Static Computer Groups

  Learn how to create computer groups that have fixed memberships.

Smart Computer Groups

Smart computer groups give you a way to organize managed computers based on one or more attributes, such as building, model, and operating system. These groups have dynamic memberships that are updated each time computers check in with the JAMF Software Server (JSS).

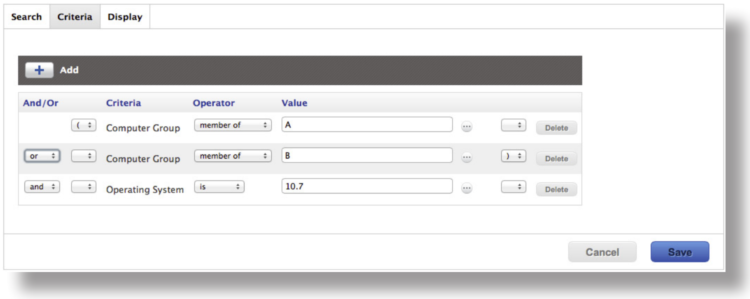
If there is an SMTP server set up in the JSS, you can enable email notifications for the group. This allows email notifications to be sent to JSS users each time the group membership changes. (For information on setting up an SMTP server and enabling email notifications for JSS user accounts, see Integrating with an SMTP Server and Email Notifications.)

After creating a smart computer group, you can view its memberships.

Creating a Smart Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the Computer Group pane to configure basic settings for the group.
   To enable email notifications, select the **Send email notification on membership change** checkbox.
6. Click the **Criteria** tab and add criteria to the group:
   a. Click **Add** + .
   b. Click **Choose** for the criteria you want to add.
      To display additional criteria, click **Choose** for "Other Criteria".
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse** ⋯ .
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.

8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.



And/Or		Criteria	Operator	Value	
	(	Computer Group	member of	A	
or		Computer Group	member of	B	)
and		Operating System	is	10.7	

9. Click **Save**.

Operations in the group take place in the order they are listed (top to bottom).

Group memberships are updated each time computers check in with the JSS and meet or fail to meet the specified criteria.

To view the group memberships, click **View**.

Cloning, Editing, or Deleting a Smart Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the smart computer group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the group, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the group, click **Delete.** Then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers the next time they check in with the JSS.

Viewing Smart Computer Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Smart Computer Groups**.
   On a smartphone, this option is in the pop-up menu.

4. Click the smart computer group you want to view memberships for.

5. Click **View**.

   A list of group memberships is displayed.

Related Information

For related information, see the following sections in this guide:

- Computer Reports
  Find out how to export the data in group membership lists to different file formats.
- Performing Mass Actions for Computers
  Find out how to perform mass actions on group memberships.
- Scope
  Learn how to configure scope based on computer groups.

Static Computer Groups

Static computer groups give you a way to organize computers by assigning them to a group. These groups have fixed memberships that must be changed manually.

After creating a static computer group, you can view its memberships.

Creating a Static Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Static Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the Computer Group pane to configure basic settings for the group.
6. Click the **Assignments** tab and select the checkbox for each computer you want to add.
7. Click **Save**.

Computers become members of the group the next time they check in with the JSS.

To view the group memberships, click **View**.

Cloning, Editing, or Deleting a Static Computer Group

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Static Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the group, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the group, click **Delete.** Then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers the next time they check in with the JSS.

Viewing Static Computer Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Static Computer Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the computer group you want to view memberships for.
5. Click **View**.

A list of group memberships is displayed.

Related Information

For related information, see the following sections in this guide:

- Computer Reports
  Find out how to export the data in group membership lists to different file formats.
- Performing Mass Actions for Computers
  Find out how to perform mass actions on group memberships.
- Scope
  Learn how to configure scope based on computer groups.

Policies

About Policies

Policies allow you to remotely perform common management tasks on managed computers. For example, you can run scripts, manage accounts, and distribute software using a policy.

While Casper Remote allows you to perform management tasks immediately, policies allow you to automate these tasks so that they run on a schedule. When you create a policy, you specify the tasks you want to automate, when the policy should run (called "trigger"), how often it should run (called "execution frequency"), and the users and computers for which it should run (called "scope").

You can also make policies available in Self Service for users to run on their computers.

Related Information

For related information, see the following sections in this guide:

- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.
- Policy Payload Reference

  Learn about each payload in the policy interface.
- Self Service Policies

  Find out how to make policies available in the Self Service.

Managing Policies

When you create a policy, you use a payload-based interface to configure settings for the policy and add tasks to it. For more information on the settings you can configure, see the following section in this guide:

Policy Payload Reference

After you create a policy, you can view the plan, status, and logs for the policy. You can also flush policy logs.

Creating a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Use the rest of the payloads to configure the tasks you want to perform.

   For an overview of each payload, see Policy Payload Reference.
7. Click the **Scope** tab and configure the scope of the policy.

   For more information, see Scope.
8. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

   For more information, see Self Service Policies.
9. (Optional) Click the **User Interaction** tab and enter messages to display to users or allow users to defer the policy.

   For more information, see User Interaction.
10. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Cloning, Editing, or Deleting a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click the policy you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the policy, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the policy, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the policy, click **Delete** and then click **Delete** again to confirm.

   The clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS.

Viewing the Plan for a Policy

The plan for a policy includes the following information:

- An indicator light that shows whether the policy is enabled
- The execution frequency for the policy
- The trigger(s) for the policy
- The scope of the policy
- The site that the policy belongs to
- A list of actions for the policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
   A list of policies and their plans are displayed.
4. To view the actions for a policy, click **Expand** ⊕ for the policy.

Viewing the Status of a Policy

For each policy, you can view a pie chart that shows the number of computers for which the policy has completed, failed, and is still remaining.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Grid View** ⊞ at the top of the list.

Viewing and Flushing Logs for a Single Policy

The logs for a single policy include a list of computers that have run the policy and the following information for each computer:

- The date/time that the policy ran on the computer
- The status of the policy
- The actions logged for the policy

Flushing logs for a policy with an execution frequency of "Once per computer" or "Once per user"

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click the policy you want to view logs for.
5. Click **Logs**.
6. To view the actions logged for a computer, click **Show** for the computer.
   To hide the information when you are done viewing it, click **Hide**.
7. To flush a policy log for a single computer, click **Flush** for the computer.
8. To flush all logs for the policy, click **Flush All** at the top of the pane.

Related Information

For related information, see the following sections in this guide:

- Viewing and Flushing Policy Logs for a Single Computer

  Find out how to view and flush policy logs for a single computer.
- Flushing Logs

  Find out how to flush all policy logs.

Policy Payload Reference

When creating or editing a policy, you use a payload-based interface to configure settings for the policy and add tasks to it. This section provides an overview of each payload.

General Payload

This payload allows you to do the following:

- Enable or disable the policy. (For example, if you need to take the policy out of production temporarily, you may want to disable it.)
- Add the policy to a site. (For more information, see Sites.)
- Add the policy to a category. (For more information, see Categories.)
- Choose one or more events to use to initiate the policy (called "trigger").
- Choose how often the policy should run (called "execution frequency").
- Make the policy available offline. (This only works with the "Ongoing" execution frequency.)
- Specify the drive on which to run the policy.
- Specify server-side and client-side limitations for the policy. (For example, you can specify an expiration date/time for the policy, or ensure that the policy does not run on weekends.)

Packages Payload

This payload allows you to perform the following software distribution tasks:

- Install packages.
- Cache packages.
- Install cached packages.

Note: To install all cached packages, use the Maintenance payload. For more information, see the following section in this guide:

Maintenance Payload

- Uninstall packages.

This payload also allows you to do the following when installing packages:

- Specify the distribution point computers should download the packages from.
- Add the packages to the Autorun data of each computer in the scope.

For complete instructions on creating a policy to perform software distribution tasks, see one of the following sections in this guide:

- Installing Packages
- Caching Packages
- Installing Cached Packages
- Uninstalling Packages

Software Updates Payload

This payload allows you to run Apple's Software Update and choose the software update server that you want computers to install updates from.

For complete instructions on creating a policy to run Software Update, see the following section in this guide:

Running Software Update

Scripts Payload

This payload allows you to run scripts and choose when they run in relation to other tasks in the policy. You can also enter values for script parameters.

For complete instructions on running scripts using a policy, see the following section in this guide:

Running Scripts

Printers Payload

This payload allows you to map and unmap printers. You can also make a printer the default.

For complete instructions on administering printers using a policy, see the following section in this guide:

Administering Printers

Disk Encryption Payload

This payload allows you to enable FileVault 2 on computers with OS X v10.8 or later by distributing disk encryption configurations.

For complete instructions on enabling FileVault 2, see the following section in this guide:

Deploying Disk Encryption Configurations

This payload also allows you to issue a new FileVault 2 recovery key for computers with OS X v10.9 or later.

For complete instructions on issuing a new recovery key, see the following section in this guide:

Issuing a New FileVault 2 Recovery Key

Dock Items Payload

This payload allows you to add and remove Dock items. When you add Dock items, you can also choose to add them to the beginning or end of the Dock.

For complete instructions on administering Dock items, see the following section in this guide:

Administering Dock Items

Local Accounts Payload

This payload allows you to create and delete local accounts, and reset local account passwords. When you create an account, you can do the following:

- Specify a location for the home directory.
- Configure the account picture.
- Allow the user to administer the computer.
- Enable the account for FileVault 2 on computers with OS X v10.9 or later.

This payload also allows you to disable an existing local account for FileVault 2 on computers with OS X v10.9 or later.

For complete instructions on administering local accounts, see the following section in this guide:

Administering Local Accounts

Management Account Payload

This payload allows you to reset the management account password. You can choose to specify the new password or randomly generate it.

This payload also allows you to enable or disable the management account for FileVault 2 on computers with OS X v10.9 or later.

For complete instructions on administering the management account, see the following section in this guide:

Administering the Management Account

Directory Bindings Payload

This payload allows you to bind computers to a directory service.

For complete instructions on binding to a directory service, see the following section in this guide:

Binding to Directory Services

EFI Password Payload

This payload allows you to set or remove an Open Firmware or EFI password.

For complete instructions on administering Open Firmware and EFI passwords, see the following section in this guide:

Administering Open Firmware/EFI Passwords

Restart Options Payload

This payload allows you to restart computers after the policy runs. It also allows you to do the following:

- Specify the disk to restart computers from, such as a NetBoot image.
- Specify criteria for the restart depending on whether or not a user is logged in.
- Configure a restart delay.

Note: You can also display a message to users before a policy restarts computers. For more information, see the following section in this guide:

User Interaction

For complete instructions on booting computers to a NetBoot image, see the following section in this guide:

Booting Computers to NetBoot Images

Maintenance Payload

This payload allows you to perform the following maintenance tasks:

- Update inventory.
- Reset computer names.
- Install all cached packages.
- Fix disk permissions.
- Fix ByHost files.
- Flush caches.
- Verify the startup disk.

For complete instructions on installing all cached packages, see the following section in this guide:

Installing Cached Packages

Files and Processes Payload

This payload allows you to search computers for specific files and processes, and use policy logs to log when they are found. You can kill processes that are found and delete files that are found when searching by path.

This payload also allows you to execute commands.

User Interaction

User Interaction allows you to display custom messages to users about the policies that run on their computers. You can also use it to allow users to defer policies.

Note: User Interaction messages and deferrals cannot be used with Self Service policies since users have control over when the policy starts.

Messages

You can display User Interaction messages to users at the following times:

- Before a policy runs
- After a policy runs
- Before a policy restarts computers

This allows you to communicate with users about the policies that run on their computers. For example, you can let users know that software is about to be installed or that a new printer is available.

In OS X v10.8 and later, most User Interaction messages are displayed in the OS X Notification Center in a category called "Management". Otherwise, messages are displayed using the JAMF Helper utility.

Deferral

You can allow users to defer a policy, and you can specify a date and time at which to prohibit further deferral (called the "deferral limit"). This allows you to give users more control over when the policy runs while ensuring that the policy eventually runs.

Before a policy runs on a computer, the user is prompted to choose to have the policy run immediately or to defer the policy for one of the following amounts of time:

- 1 hour
- 2 hours
- 4 hours
- 1 day
- The amount of time until the deferral limit is reached

If the user chooses to defer the policy, they are prompted with the same message after the chosen amount of time. When the deferral limit is reached, a message is displayed to notify the user, and the policy runs immediately.

Configuring User Interaction for a Policy

1. Log in to the JSS with a web browser.
2. Create or edit a policy.
   For more information, see Managing Policies.
3. Click the **User Interaction** tab.
4. Configure the settings on the pane.
5. When you are done configuring the policy, click **Save**.

Self Service

About Self Service

The Self Service application allows users to browse and run policies, access webpages, and utilize plug-ins developed with the Self Service API. Users can point-and-click their way through Self Service using an intuitive interface similar to iTunes.

The JAMF Software Server (JSS) allows you to manage every aspect of Self Service, including its installation, authentication, and the items available to users.

You can make any policy available in Self Service and customize how it is displayed to users. This includes displaying an icon and description, featuring the policy on the main page, and displaying it in relevant categories. You can also specify which computers display the policy in Self Service and which users can access it.

In addition, you can make plug-ins available in Self Service to extend the functionality of the application. There are two types of plug-ins you can make available: URL plug-ins and Self Service Plug-in bundles. URL plug-ins give users easy access to webpages right from the application. Self Service Plug-in bundles are custom plug-ins developed with the Self Service API.

Related Information

For related information, see the following sections in this guide:

- Installing Self Service

  Find out how to install Self Service on managed computers.
- User Authentication Settings for Self Service

  Find out how to require users to log in to Self Service and authenticate locally before running Self Service policies.
- Self Service Policies

  Find out how to make policies available in Self Service.
- Self Service Plug-ins

  Find out how to add plug-ins to Self Service.
- Self Service User Experience

  Learn how users run policies and use plug-ins in Self Service.

Installing Self Service

There are two ways to install Self Service on managed computers. You can install Self Service automatically on all managed computers using the Self Service settings in the JAMF Software Server (JSS), or you can install Self Service using a policy. Installing Self Service using a policy gives you more control over the installation.

Installing Self Service Automatically

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Self Service** .
5. Click **Edit**.
6. Select the **Install Automatically** checkbox.
7. (Optional) Configure the installation location for Self Service.
8. Click **Save**.

Self Service is installed on all managed computers the next time they check in with the JSS. It is also installed on computers as they are newly enrolled.

Installing Self Service Using a Policy

This method involves the following steps:

1. Download a copy of Self Service from the JSS.
2. Package Self Service using Composer or a third-party package building tool.
3. Deploy Self Service using a policy.

For complete instructions on installing Self Service using this method, see the following Knowledge Base article:

Installing Self Service Using a Policy

User Authentication Settings for Self Service

The User Authentication settings for Self Service allow you to configure requirements for logging in to Self Service and for authenticating locally before running Self Service policies.

Requirements

To require or allow users to log in to Self Service, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

Configuring the User Authentication Settings for Self Service

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Self Service** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

The changes are applied the next time computers check in with the JSS.

Self Service Policies

You can make any policy available in Self Service, but it is up to you to determine which policies are appropriate.

When you make a policy available in Self Service, you can specify which computers display it in Self Service and which users can access it (called "scope").

You can also customize how Self Service policies are displayed to users by doing the following:

- Entering a description
- Uploading an icon
- Featuring the policy on the main page
- Displaying or featuring the policy in one or more categories

Creating a Self Service Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, see General Payload
6. Use the rest of the payloads to configure the tasks you want to perform.
   For an overview of each payload, see Policy Payload Reference.
7. Click the **Scope** tab and configure the scope of the policy.
   For more information, see Scope.
8. Click the **Self Service** tab.
9. Select **Make the policy available in Self Service**.
10. Configure how the policy is displayed in Self Service using the settings on the pane.
11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.
    For more information, see User Interaction.
12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Related Information

For related information, see the following sections in this guide:

- User Authentication Settings for Self Service

  Find out how to require users authenticate locally before running Self Service policies.

- Running Self Service Policies

  Learn how users run the policies available in Self Service.

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.

Self Service Plug-ins

There are two types of plug-ins that you can make available in Self Service: URL plug-ins and Self Service Plug-in bundles. URL plug-ins give users easy access to webpages right from the application. Self Service Plug-in bundles are custom plug-ins developed with the Self Service API.

When you make a URL plug-in available in Self Service, you can customize how the plug-in is displayed to users. This includes uploading an icon for the plug-in, and specifying whether the plug-in opens in Self Service or in a web browser.

By default, Self Service plug-ins are available on all managed computers and to all users.

Adding a Self Service Plug-in

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management - Management Framework" section, click **Self Service Plug-ins** .
5. Click **New** + .
6. Enter a display name and description, and choose a priority for the plug-in.
7. Choose "Self Service Plug-in Bundle" or "URL Plug-in" from the **Plug-in Type** pop-up menu.
8. Configure the plug-in using the options on the pane.
9. Click **Save**.

The plug-in is available in Self Service the next time computers check in with the JSS.

Cloning, Editing, or Deleting a Self Service Plug-in

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Self Service Plug-ins** .
5. Click the plug-in you want to clone, edit, or delete.

6. Do one of the following:
   - To clone the plug-in, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the plug-in, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the plug-in, click **Delete** and then click **Delete** again to confirm.

   The changes are applied the next time computers check in with the JSS.

Related Information

For more information on the Self Service API, download the Casper Suite SDK from:

http://www.jamfsoftware.com/developer-resources/

For related information, see the following section in this guide:

Using Self Service Plug-ins
Learn how users use the plug-ins available in Self Service.

For related information, see the following Knowledge Base article:

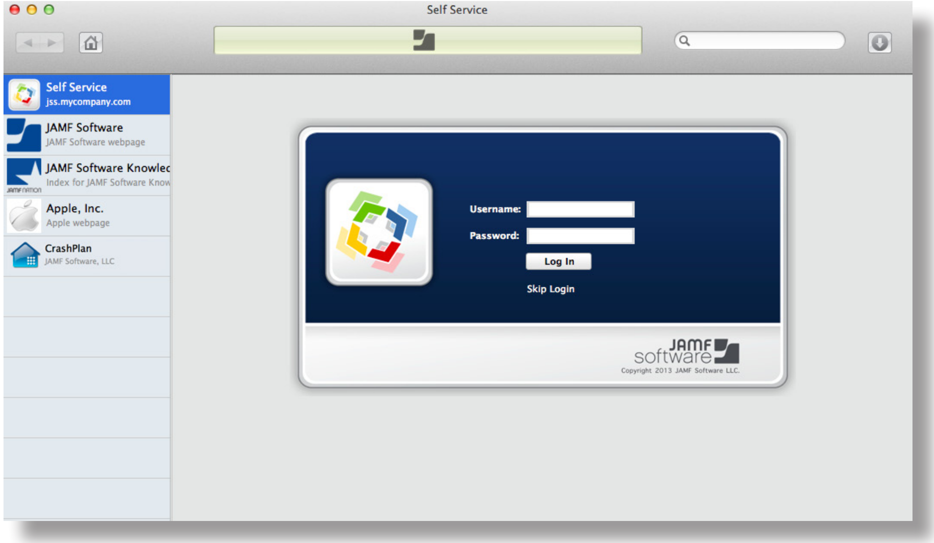
Scope of Self Service Plug-ins
Find out how to distribute a Self Service plug-in using a policy so you can control which users have access to the plug-in.

Self Service User Experience

This section provides an overview of what users do to run policies and use plug-ins available in Self Service.

Logging in to Self Service

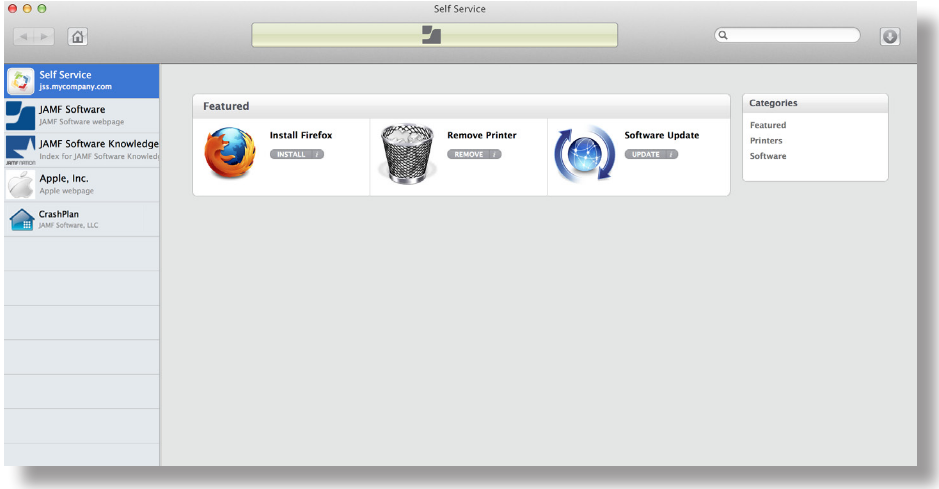
After opening Self Service, users may need to log in using their LDAP directory accounts. The login pane is only displayed if the User Authentication settings for Self Service are configured to require or allow login. (For more information, see User Authentication Settings for Self Service.)



Running Self Service Policies

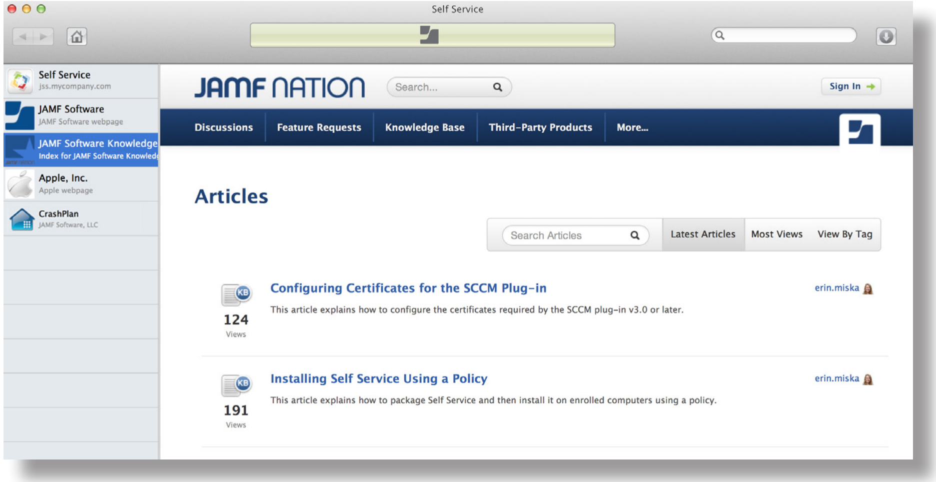
Users can browse policies from the "Featured" section or the list of categories on the main page. Policies are only displayed in the "Featured" section if you configured the policy to do so. (For more information, see Self Service Policies.)

To run a policy, users click the button next to it. If User Authentication settings for Self Service are configured to require user authentication, users are prompted to enter their local credentials before running the policy. (For more information, see User Authentication Settings for Self Service.)



Using Self Service Plug-ins

Self Service plug-ins are displayed in the sidebar. Users click a plug-in to access a webpage or utilize a plug-in developed with the Self Service API.



Configuring Certificates for the SCCM Plug-in

erin.miska

This article explains how to configure the certificates required by the SCCM plug-in v3.0 or later.

124 Views

Installing Self Service Using a Policy

erin.miska

This article explains how to package Self Service and then install it on enrolled computers using a policy.

191 Views

Related Information

For related information, see the following sections in this guide:

- Self Service Policies

  Find out how to make policies available in Self Service.

- Self Service Plug-ins

  Find out how to add plug-ins to Self Service.

Software Distribution

Managing Packages

Packages in the following formats can be administered using the Casper Suite:

- DMG
- PKG
- MPKG

Note: There are special instructions for managing OS X Installers, and Adobe Updaters and Installers for CS3 or CS4. For more information, see Managing OS X Installers or Administering Adobe CS3 and CS4.

Before you can deploy a package, it must exist on the distribution point you plan to deploy it from and in the JAMF Software Server (JSS). There are three ways to achieve this:

- **Add the package to Casper Admin**—This method adds the package to the master distribution point and the JSS. You can then add the package to other distribution points via replication.
- **Upload the package directly to the JSS**—This method is only available if your master distribution point is the cloud distribution point or a JDS instance. It adds the package to the master distribution point and the JSS. You can then add the package to other distribution points via replication.
- **Manually**—This method is only available if your master distribution point is a file share distribution point. It involves manually copying the package to the distribution point and then entering information about the package in the JSS.

Each of these methods also involves configuring settings for the package. When you configure settings for a package, you can do the following:

- Add the package to a category. (For more information, see Categories.)
- Choose a priority for deploying or uninstalling the package.
- Fill user templates with the contents of the home directory in the package's Users folder.
- Fill existing user home directories with the contents of the home directory in the package's Users folder.
- Allow the package to be uninstalled.
- Specify whether computers must be restarted after installing the package.
- Choose whether the package must be installed on the boot drive after imaging.
- Specify operating system and architecture type requirements for deploying the package.
- Only allow the package to be installed if it is available in Software Update.

You can also index packages. Indexing creates a log of all the files contained within a package. This allows you to uninstall the package and view the contents of the package from the JSS. Packages can only be indexed using Casper Admin.

When you add, edit, or delete a package in Casper Admin, the changes are reflected in the JSS and vice versa.

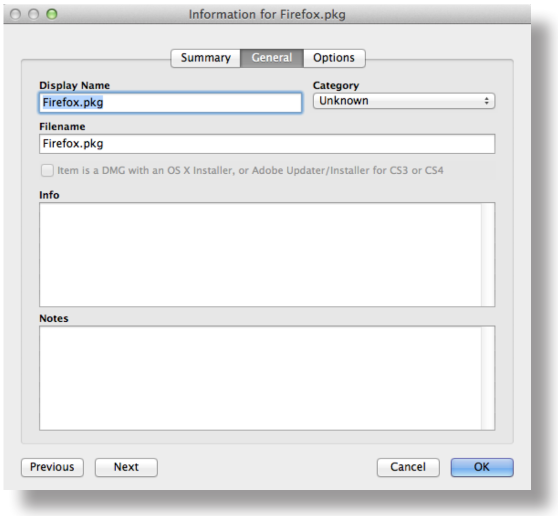
Requirements

To manage packages, you need a distribution point set up in the JSS. (For more information, see About Distribution Points.)

Adding a Package to Casper Admin

Adding a package to Casper Admin adds the package to the master distribution point and the JSS.

1. Open Casper Admin and authenticate to the JSS.
2. Drag the package to the main repository in Casper Admin.
   The package is displayed in blue text in the Unknown category until you add it to a category.
3. Double-click the package in the main repository.
4. Click the **General** tab and configure basic settings for the package, including the display name and category.


Information for Firefox.pkg

Display Name: Firefox.pkg

Category: Unknown

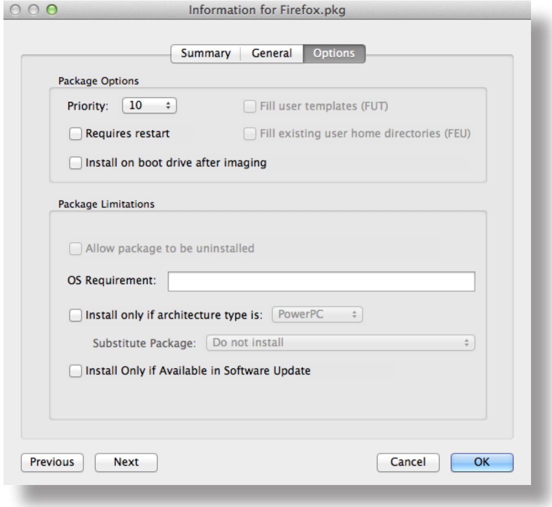
Filename: Firefox.pkg

□ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

Info

Notes

5. Click the **Options** tab and configure additional settings for the package, including the priority, and operating system and architecture type requirements.



Package Options

Priority: 10

□ Fill user templates (FUT)

□ Requires restart

□ Fill existing user home directories (FEU)

□ Install on boot drive after imaging

Package Limitations

□ Allow package to be uninstalled

OS Requirement:

□ Install only if architecture type is: PowerPC

Substitute Package: Do not install

□ Install Only if Available in Software Update

6. Click **OK**.

Uploading a Package to the JSS

If your master distribution point is the cloud distribution or a JDS instance, you can upload the package directly to the JSS. This adds the package to the master distribution point and the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Packages** 📦 .
5. Click **New** + .
6. Use the General pane to configure basic settings for the package, including the display name and category.

   > ***Note:*** If you do not add the package to a category, Casper Admin displays the package in blue text in the Unknown category.
7. Click **Upload Package** and upload the package.
8. Click the **Options** tab and configure additional settings for the package, including the priority.
9. (Optional) Click the **Limitations** tab and configure limitations for the package, including operating system and architecture type requirements.
10. Click **Save**.

Manually Adding a Package to a Distribution Point and the JSS

If your master distribution point is a file share distribution point, you can manually copy a package to the distribution point and then enter information about the package in the JSS.

1. Copy the package to the Packages folder at the root of the file share on the distribution point.
2. Log in to the JSS with a web browser.
3. In the top-right corner of the page, click **Settings** ⚙ .
4. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
5. In the "Computer Management" section, click **Packages** .
6. Click **New** + .
7. Use the General pane to configure basic settings for the package, including the display name, category, and filename.

   > ***Note:*** If you do not add the package to a category, Casper Admin displays the package in blue text in the Unknown category.
8. Click the **Options** tab and additional settings for the package, including the priority.
9. (Optional) Click the **Limitations** tab and configure limitations for the package, including operating system and architecture type requirements.
10. Click **Save**.

Editing or Deleting a Package Using Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the package you want to edit or delete.
3. Do one of the following:
   - To edit the package, double-click it and make changes as needed. Then click **OK**.
   - To delete the package, click **Delete** 🚫 and then click **Delete** again to confirm.

The edit or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.

Editing or Deleting a Package Using the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Packages** .
5. Click the package you want to edit or delete.
6. Do one of the following:
   - To edit the package, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the package, click **Delete** and then click **Delete** again to confirm.

The edit or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.

Indexing a Package

Indexing a package creates a log of all the files contained within the package. This allows you to uninstall the package and view the contents of the package from the JSS.

Packages can be indexed using Casper Admin only. The time it takes to index a package depends on the amount of data in the package.

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the package you want to index and click **Index** at the bottom of the pane.
3. If prompted, authenticate locally.

When the indexing process is complete, Casper Admin defaults back to the main repository.

Viewing the Contents of an Indexed Package

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Packages** .

5. Click the package you want to view the contents of.

6. Click **Contents**.

   A table that contains the package contents is displayed.

Related Information

For related information, see the following sections in this guide:

- Installing Packages
  Find out how to install packages using a policy or Casper Remote.
- Caching Packages
  Find out how to cache packages using a policy or Casper Remote.
- Installing Cached Packages
  Find out how to install packages that were cached using the Casper Suite.
- Uninstalling Packages
  Find out how to uninstall packages that were installed using the Casper Suite.

Managing OS X Installers

Adding an OS X Installer to Casper Admin is the first step to installing a clean copy of OS X on computers.

If the OS X Installer is for OS X v10.6 or earlier, you can also create a custom OS X installation from the installer. This allows you to change the default software and language settings in OS X.

Requirements

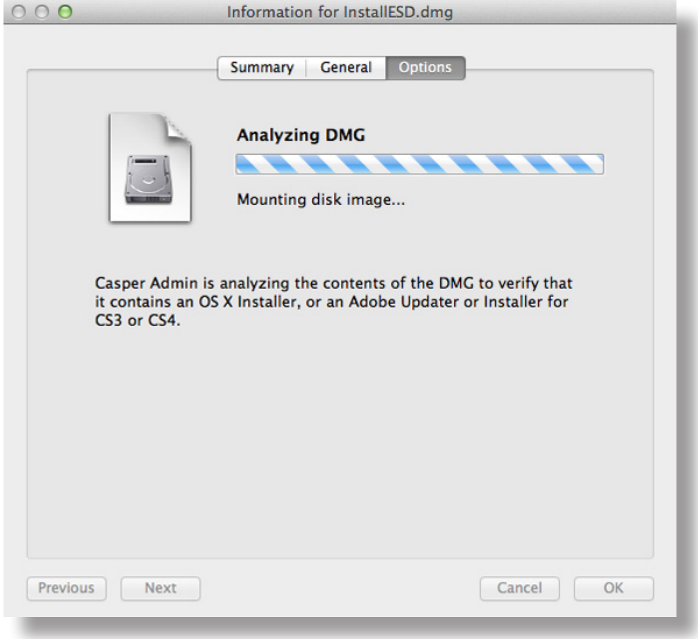
To manage OS X Installers, you need a distribution point set up in the JAMF Software Server (JSS). (For more information, see About Distribution Points.)

To add an OS X Installer to Casper Admin, the OS X Installer must be a .app file from the Mac App Store or a DMG.

Adding a .app File for OS X to Casper Admin

Adding a .app file for OS X to Casper Admin adds it to the master distribution point and the JSS.

1. Open Casper Admin and authenticate to the JSS.
2. Drag the .app file to the main repository in Casper Admin.
   Casper Admin extracts the `InstallESD.dmg` file and then analyzes its contents.

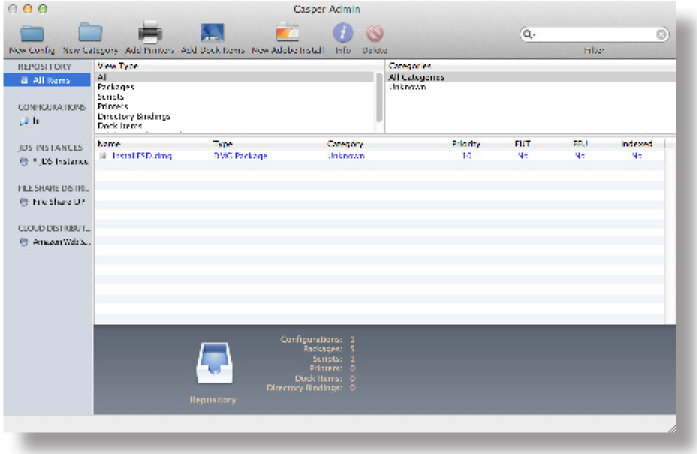


Analyzing DMG

Mounting disk image...

Casper Admin is analyzing the contents of the DMG to verify that it contains an OS X Installer, or an Adobe Updater or Installer for CS3 or CS4.

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

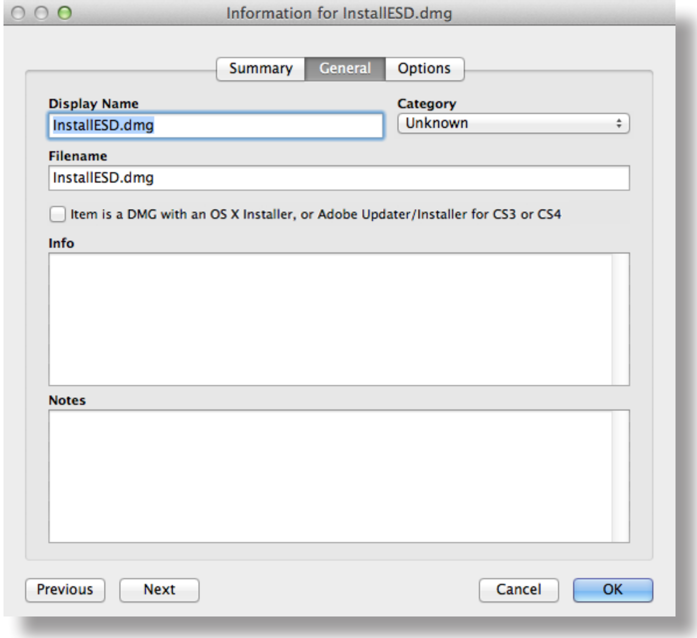


Name	Type	Category	Priority	FUT	FEU	Indexed
InstallESD.dmg	DMG Package	Unknown	10	No	No	No

Configurations: 1
Packages: 5
Scripts: 1
Printers: 0
Dock Items: 0
Directory Bindings: 0

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

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



Display Name: InstallESD.dmg

Category: Unknown

Filename: InstallESD.dmg

☐ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

Info

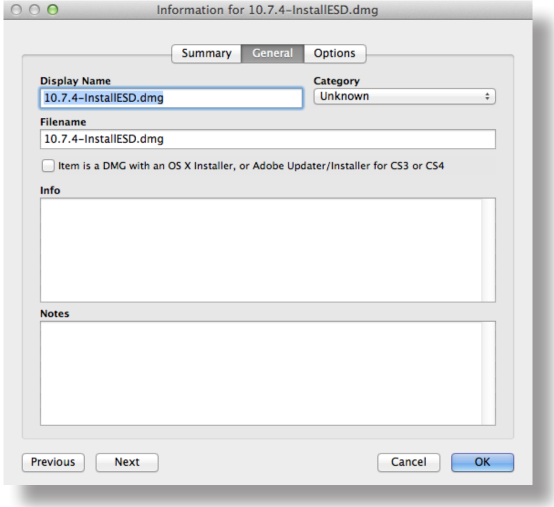
Notes

5. Click **OK**.

Adding a DMG of an OS X Installer to Casper Admin

Adding a DMG of an OS X Installer to Casper Admin adds it to the master distribution point and the JSS.

1. Open Casper Admin and authenticate to the JSS.
2. Drag the DMG to the main repository in Casper Admin.
   The DMG is displayed in blue text in the Unknown category until you add it to a category.
3. Double-click the DMG in the main repository.
4. Click the **General** tab and configure basic settings for the DMG, including the display name and category.
   Be sure to select the **Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4** checkbox.



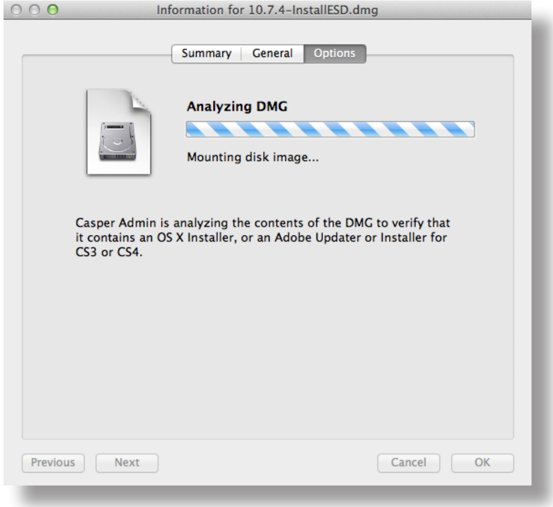
Display Name: 10.7.4-InstallESD.dmg

Category: Unknown

Filename: 10.7.4-InstallESD.dmg

□ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

5. When prompted, click **OK** to continue.
   Casper Admin analyzes the contents of the DMG.

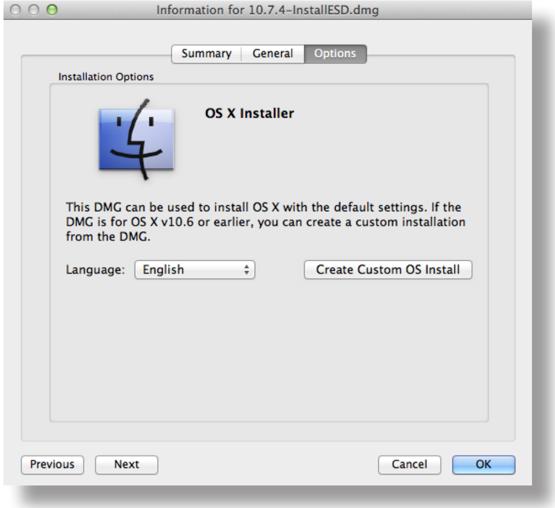


Analyzing DMG

Mounting disk image...

Casper Admin is analyzing the contents of the DMG to verify that it contains an OS X Installer, or an Adobe Updater or Installer for CS3 or CS4.

6. When the Options pane appears, choose a default language for the installation from the **Language** pop-up menu.



This DMG can be used to install OS X with the default settings. If the DMG is for OS X v10.6 or earlier, you can create a custom installation from the DMG.

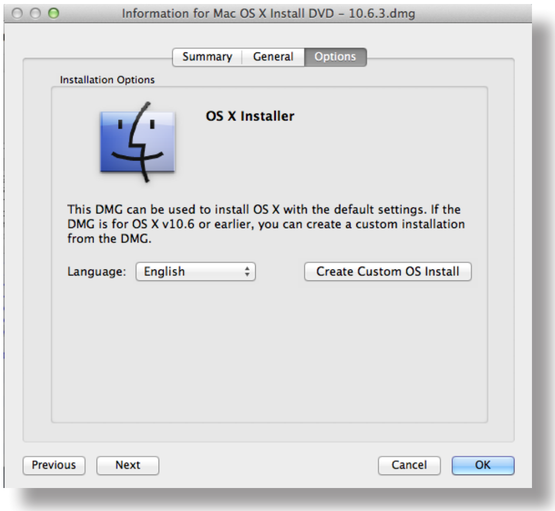
Language: English

7. Click **OK**.

Creating a Custom OS X Installation

If the DMG is for OS X v10.6 or earlier, you can create a custom OS X installation from the DMG. This allows you to change the default software and language settings in OS X.

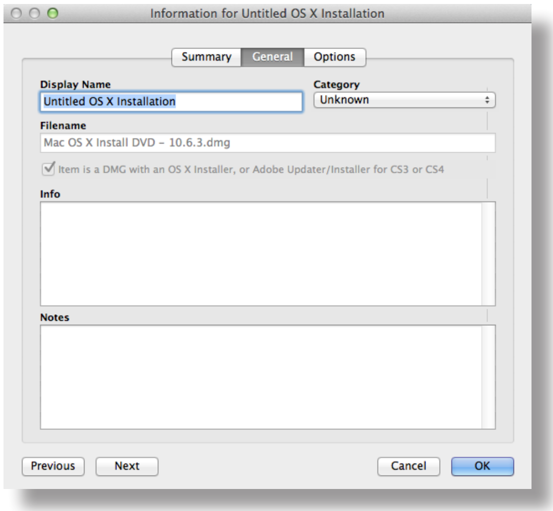
1. Open Casper Admin and authenticate to the JSS.
2. Double-click the DMG of the OS X Installer that you want to base your custom installation on.
3. Click the **Options** tab and click **Create Custom OS Install**.



This DMG can be used to install OS X with the default settings. If the DMG is for OS X v10.6 or earlier, you can create a custom installation from the DMG.

Language: English

4. On the General pane, configure basic settings for the installation, including the display name and category.



Display Name: Untitled OS X Installation

Category: Unknown

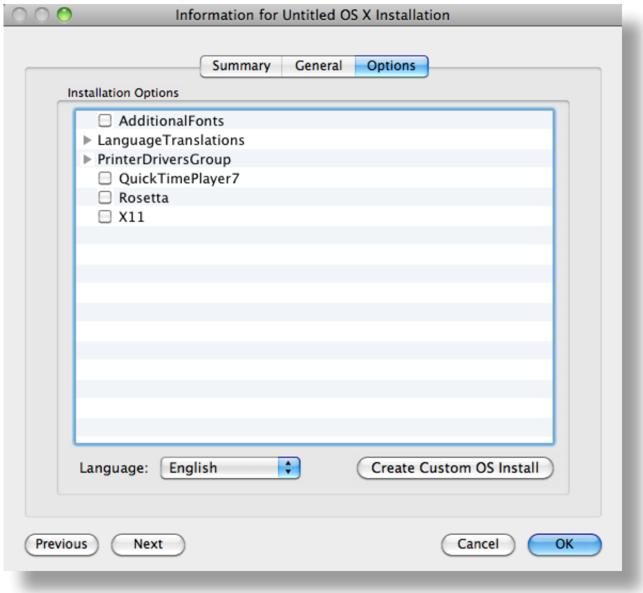
Filename: Mac OS X Install DVD – 10.6.3.dmg

☑ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

Info

Notes

5. Click the **Options** tab and configure additional settings for the installation.



Installation Options

- ☐ AdditionalFonts
- ▶ LanguageTranslations
- ▶ PrinterDriversGroup
- ☐ QuickTimePlayer7
- ☐ Rosetta
- ☐ X11

Language: English

6. Click **OK**.

Related Information

For related information, see the following technical paper:

Deploying OS X v10.7 or Later with the Casper Suite
Get step-by-step instructions for deploying OS X v10.7 or later.

Administering Adobe CS3 and CS4

Deploying Adobe CS3 or CS4 involves the following steps:

1. Use Disk Utility to create a DMG of the installer DVD.
2. Add the DMG to Casper Admin.
   For more information, see Adding a DMG of an Adobe CS3/CS4 Updater or Installer to Casper Admin.
3. Create an Adobe installation from the DMG.
   For more information, see Creating a CS3/CS4 Adobe Installation.
4. Install the Adobe installation using a policy or Casper Remote.
   For more information, see Installing Packages.

Updating Adobe CS3 or CS4 involves the following steps:

1. Obtain or create a DMG of the appropriate Adobe Updater.
   The Adobe Updater must support silent installation.

Note: Most Adobe updates are available in the DMG format at Adobe's website.

2. Add the DMG to Casper Admin.
   For more information, see Adding a DMG of an Adobe CS3/CS4 Updater or Installer to Casper Admin.
3. Install the DMG using a policy or Casper Remote.
   For more information, see Installing Packages.

Requirements

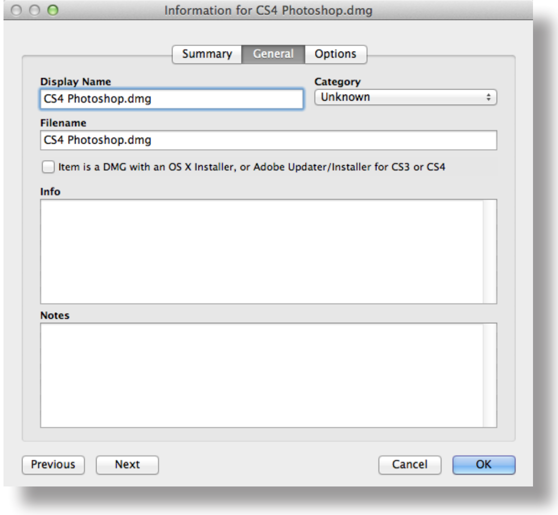
To manage Adobe CS3/CS4 Updaters or Installers using Casper Admin, you need a distribution point set up in the JSS. (For more information, see About Distribution Points.)

Adding a DMG of an Adobe CS3/CS4 Updater or Installer to Casper Admin

Adding a package to Casper Admin adds the package to the master distribution point and the JSS.

1. Open Casper Admin and authenticate to the JSS.
2. Drag the DMG to the main repository in Casper Admin.
   The DMG is displayed in blue text in the Unknown category until you add it to a category.
3. Double-click the DMG in the main repository.

4. Click the **General** tab and configure basic settings for the DMG, including the display name and category. Be sure to select the **Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4** checkbox.



Display Name: CS4 Photoshop.dmg

Category: Unknown

Filename: CS4 Photoshop.dmg

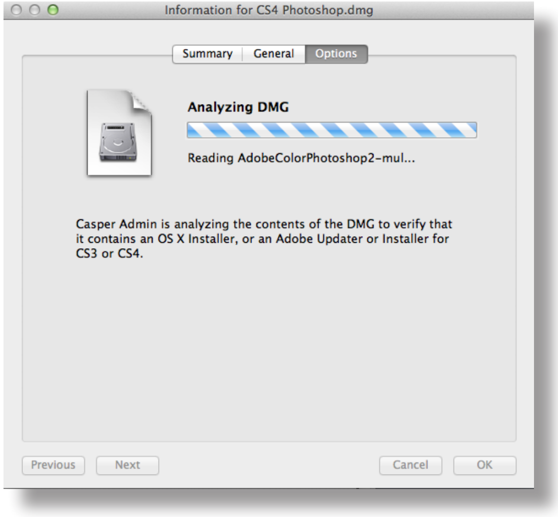
□ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

Info

Notes

5. When prompted, click **OK** to continue.

Casper Admin analyzes the contents of the DMG.

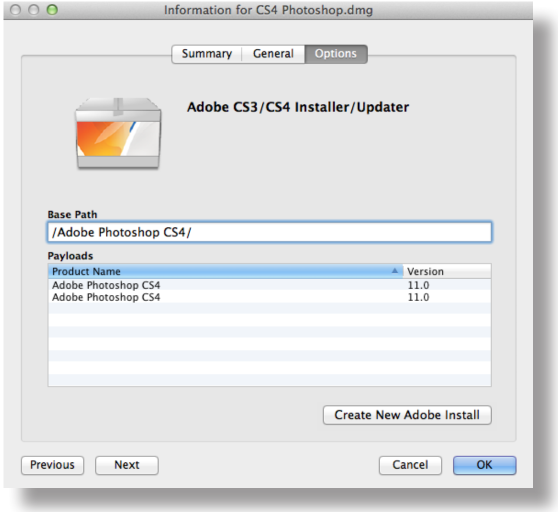


Analyzing DMG

Reading AdobeColorPhotoshop2-mul...

Casper Admin is analyzing the contents of the DMG to verify that it contains an OS X Installer, or an Adobe Updater or Installer for CS3 or CS4.

6. When the Options pane appears, click **OK**.



Adobe CS3/CS4 Installer/Updater

Base Path

/Adobe Photoshop CS4/

Payloads

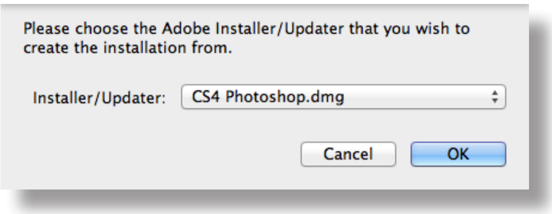
Product Name	Version
Adobe Photoshop CS4	11.0
Adobe Photoshop CS4	11.0

Creating a CS3/CS4 Adobe Installation

After you add a DMG of an Adobe Installer to Casper Admin, you can create one or more Adobe installations. This allows you to do the following:

- Choose a priority for the deploying or uninstalling CS3/CS4 during imaging.
- Specify an installation language.
- Enter a serial number for the installation.
- Suppress the Dock item during installation.
- Ignore conflicting processes.
- Suppress the EULA, registration, and updates.
- Allow the package to be uninstalled.

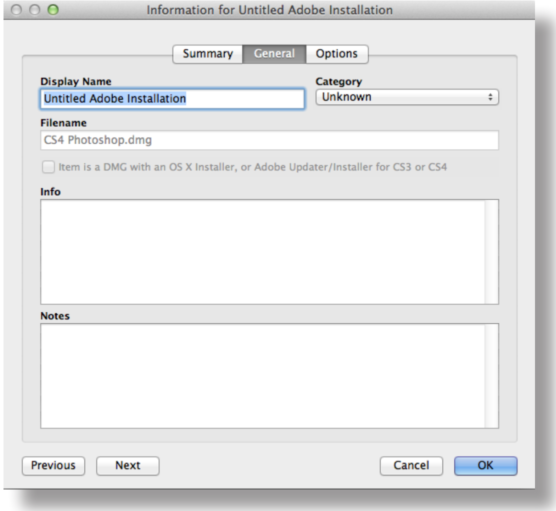
1. Open Casper Admin and authenticate to the JSS.
2. Click **New Adobe Install** .
3. If you have more than one DMG of Adobe Installers, choose the one on which you want to base your installation from the **Installer/Updater** pop-up menu.



Please choose the Adobe Installer/Updater that you wish to create the installation from.

Installer/Updater: CS4 Photoshop.dmg

4. On the General pane, configure basic settings for the installation, including the display name and category.



Information for Untitled Adobe Installation

Summary | General | Options

Display Name: Untitled Adobe Installation

Category: Unknown

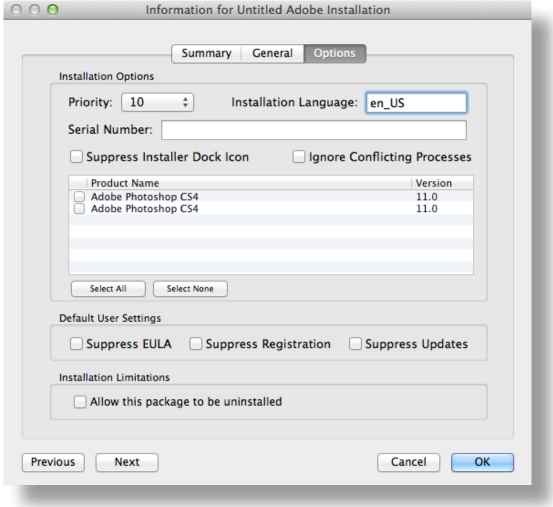
Filename: CS4 Photoshop.dmg

□ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

Info

Notes

5. Click the **Options** tab and configure additional settings for the installation, including the priority and installation language.



Information for Untitled Adobe Installation

Summary | General | Options

Installation Options

Priority: 10

Installation Language: en_US

Serial Number:

□ Suppress Installer Dock Icon □ Ignore Conflicting Processes

Product Name	Version
□ Adobe Photoshop CS4	11.0
□ Adobe Photoshop CS4	11.0

Default User Settings

□ Suppress EULA □ Suppress Registration □ Suppress Updates

Installation Limitations

□ Allow this package to be uninstalled

6. Click **OK**.

Installing Packages

When you install a package, you can do the following:

- Fill user templates.
- Fill existing user home directories.
- Add the package to Autorun data.
- Specify a distribution point for computers to download the package from.

There are two ways to install a package on computers: using a policy or using Casper Remote.

Note: You can also install packages during imaging. For more information, see Configurations.

Requirements

To install a package on computers, the package must exist on the distribution point you plan to deploy it from and in the JSS. (For more information, see Managing Packages.)

Installing a Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Packages payload and click **Configure**.
7. Click **Add** for the package you want to install.
8. Choose "Install" from the **Action** pop-up menu.
9. Configure the settings for the package.

   To add the package to each computer's Autorun data, select the **Update Autorun data** checkbox. For more information, see Autorun Imaging.
10. Specify a distribution point for computers to download the package from.
11. Use the Restart Options payload to configure settings for restarting computers.

    For more information, see Restart Options Payload.

12. Click the **Scope** tab and configure the scope of the policy.
    For more information, see Scope.
13. (Optional) Click the **Self Service** tab and make the policy available in Self Service.
    For more information, see Self Service Policies.
14. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.
    For more information, see User Interaction.
15. Click **Save**.

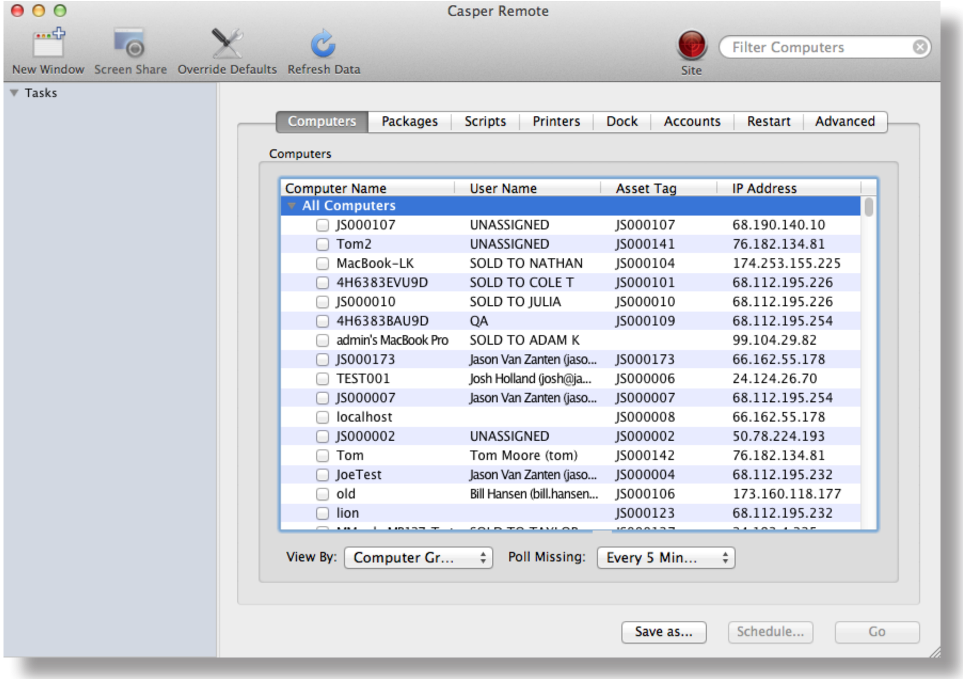
The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Installing a Package Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** ● and choose a site.
   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to install the package.



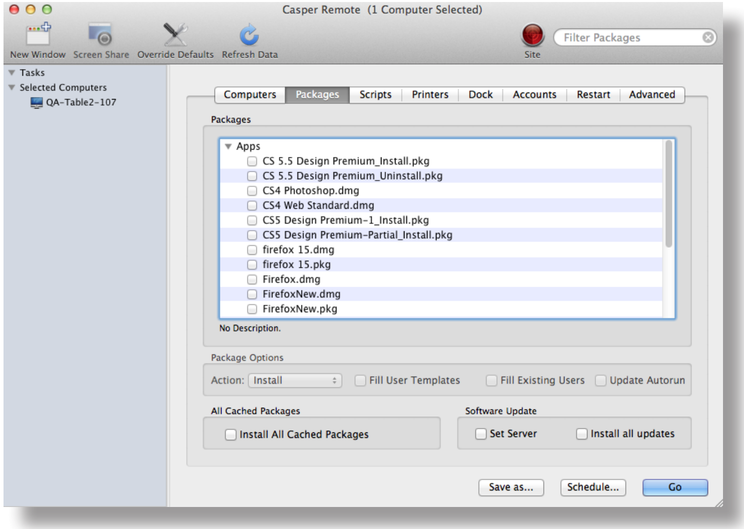
Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...

Poll Missing: Every 5 Min...

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the package you want to install.



Tasks
Selected Computers
QA-Table2-107

Packages

Apps
- ☐ CS 5.5 Design Premium_Install.pkg
- ☐ CS 5.5 Design Premium_Uninstall.pkg
- ☐ CS4 Photoshop.dmg
- ☐ CS4 Web Standard.dmg
- ☐ CS5 Design Premium-1_Install.pkg
- ☐ CS5 Design Premium-Partial_Install.pkg
- ☐ firefox 15.dmg
- ☐ firefox 15.pkg
- ☐ Firefox.dmg
- ☐ FirefoxNew.dmg
- ☐ FirefoxNew.pkg

No Description.

Package Options

Action: Install ☐ Fill User Templates ☐ Fill Existing Users ☐ Update Autorun

All Cached Packages

☐ Install All Cached Packages

Software Update

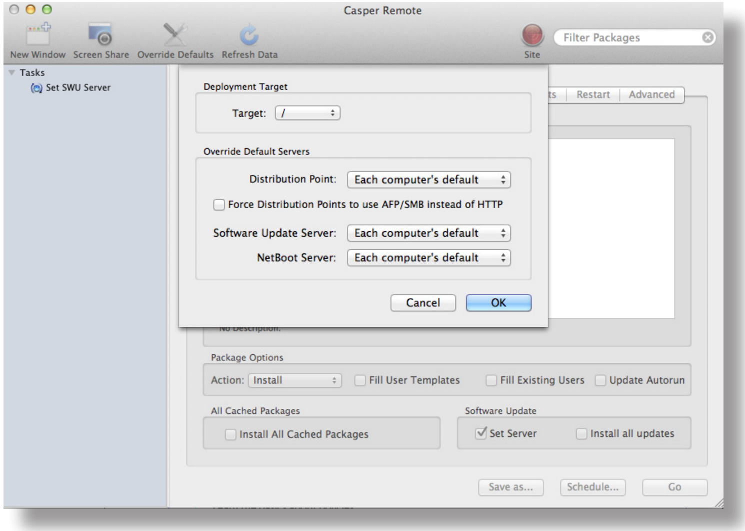
☐ Set Server ☐ Install all updates

6. Choose "Install" from the **Action** pop-up menu.

7. Configure the settings for the package.

   To add the package to each computer's Autorun data, select the **Update Autorun data** checkbox. For more information, see Autorun Imaging.

8. If you want to change the distribution point that computers download packages from, click **Override Defaults** and choose a distribution point.



Tasks
Set SWU Server

Deployment Target

Target: /

Override Default Servers

Distribution Point: Each computer's default

☐ Force Distribution Points to use AFP/SMB instead of HTTP

Software Update Server: Each computer's default

NetBoot Server: Each computer's default

Package Options

Action: Install ☐ Fill User Templates ☐ Fill Existing Users ☐ Update Autorun

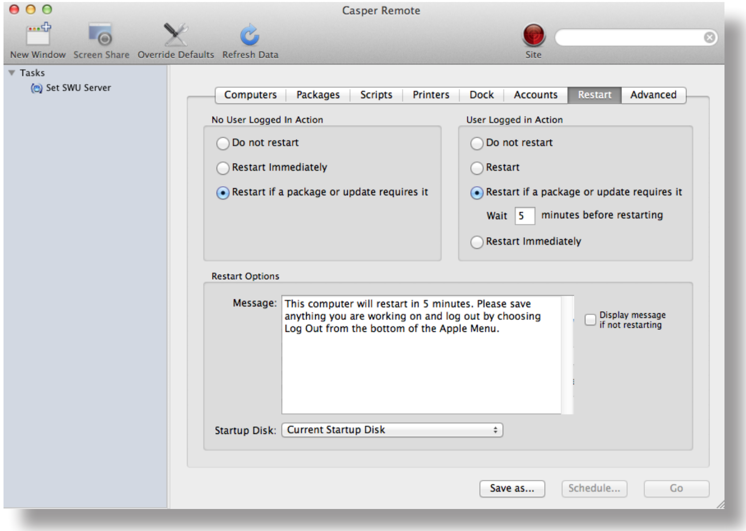
All Cached Packages

☐ Install All Cached Packages

Software Update

☑ Set Server ☐ Install all updates

9. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart
○ Restart Immediately
● Restart if a package or update requires it

User Logged in Action

○ Do not restart
○ Restart
● Restart if a package or update requires it
Wait 5 minutes before restarting
○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

10. Do one of the following:

- To immediately perform the tasks on the specified computers, click **Go**.
- To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies
  Learn the basics about policies.
- Managing Policies
  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.

Caching Packages

Caching packages allows you to download them on computers without installing them right away.

When you cache a package, you can specify a distribution point for computers to download the package from.

There are two ways to cache packages on computers: using a policy or using Casper Remote.

Requirements

To cache a package on computers, the package must exist on the distribution point you plan to deploy it from and in the JSS. (For more information, see Managing Packages.)

Caching a Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, see General Payload.
6. Select the Packages payload and click **Configure**.
7. Click **Add** for the package you want to cache.
8. Choose "Cache" from the **Action** pop-up menu.
9. Configure the settings for the package.
   To add the package to each computer's Autorun data, select the **Add to Autorun data** checkbox. For more information, see Autorun Imaging.
10. Specify a server for computers to download the package from.
11. Use the Restart Options payload to configure settings for restarting computers.
    For more information, see Restart Options Payload.
12. Click the **Scope** tab and configure the scope of the policy.
    For more information, see Scope.

13. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

14. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

15. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

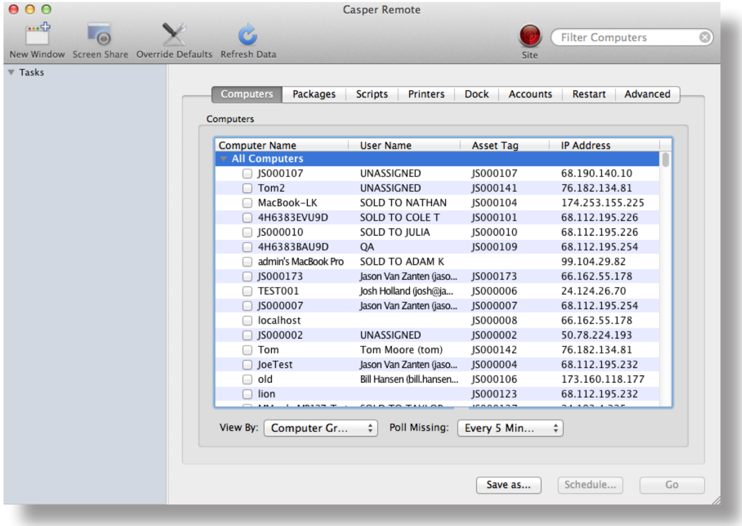
Caching a Package Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** and choose a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to cache the package.



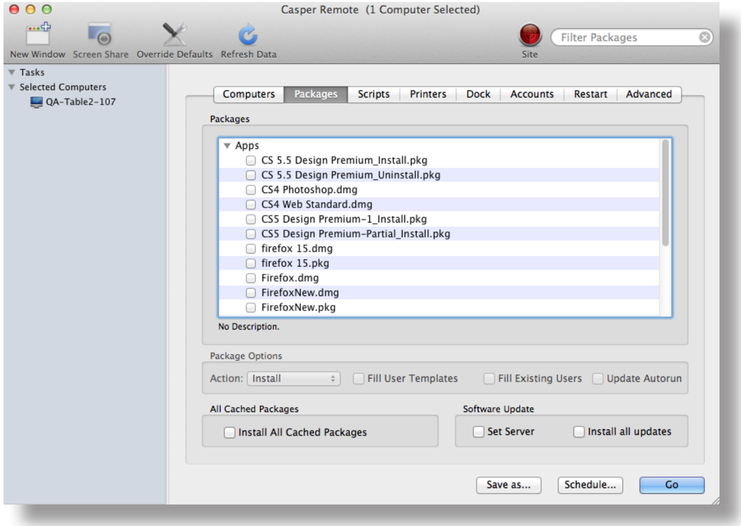
Computers

Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr... Poll Missing: Every 5 Min...

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the package you want to cache.



Packages

- Apps
  - □ CS 5.5 Design Premium_Install.pkg
  - □ CS 5.5 Design Premium_Uninstall.pkg
  - □ CS4 Photoshop.dmg
  - □ CS4 Web Standard.dmg
  - □ CS5 Design Premium-1_Install.pkg
  - □ CS5 Design Premium-Partial_Install.pkg
  - □ firefox 15.dmg
  - □ firefox 15.pkg
  - □ Firefox.dmg
  - □ FirefoxNew.dmg
  - □ FirefoxNew.pkg

No Description.

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

All Cached Packages

□ Install All Cached Packages

Software Update

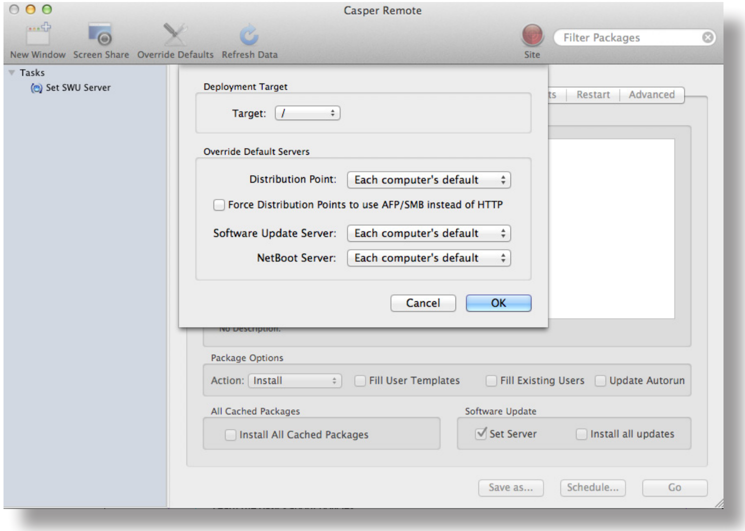
□ Set Server □ Install all updates

6. Choose "Cache" from the **Action** pop-up menu.

7. Configure the settings for the package.

   To add the package to each computer's Autorun data, select the **Update Autorun data** checkbox. For more information, see Autorun Imaging.

8. If you want to change the distribution point that computers download packages from, click **Override Defaults** ✂ and choose a distribution point.



Deployment Target

Target: /

Override Default Servers

Distribution Point: Each computer's default

□ Force Distribution Points to use AFP/SMB instead of HTTP

Software Update Server: Each computer's default

NetBoot Server: Each computer's default

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

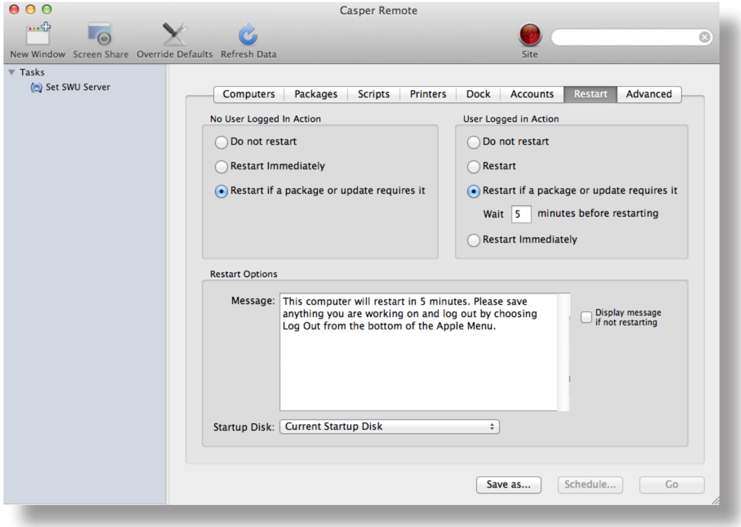
All Cached Packages

□ Install All Cached Packages

Software Update

☑ Set Server □ Install all updates

9. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

10. Do one of the following:

- To immediately perform the tasks on the specified computers, click **Go**.
- To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- Smart Computer Groups

  You can create smart computer groups based on cached packages.
- About Policies

  Learn the basics about policies.
- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.
- Installing Cached Packages

  Find out how to install a cached package using a policy or Casper Remote.

Installing Cached Packages

You can choose to install one or more specific cached packages, or all cached packages.

When you install one or more specific cached packages, you can do the following:

- Fill user templates.
- Fill existing user home directories.
- Add the package to Autorun data.

There are two ways to install packages that were cached using the Casper Suite: using a policy or using Casper Remote.

Requirements

To install a specific cached package,the package must exist on the distribution point you plan to deploy it from and in the JSS. (For more information, see Managing Packages.)

Installing a Cached Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, see General Payload.
6. Select the Packages payload.
7. Click **Configure**.
8. Click **Add** for the cached package you want to install.
9. Choose "Install Cached" from the **Action** pop-up menu.
10. Configure the settings for the package.
    To add the package to each computer's Autorun data, select the **Update Autorun data** checkbox. For more information on Autorun data and Autorun Imaging, see Autorun Imaging.
11. (Optional) Use the Restart Options payload to change the settings for restarting computers.
    For more information, see Restart Options Payload.

12. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.

13. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

14. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

15. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Installing a Cached Package Using Casper Remote

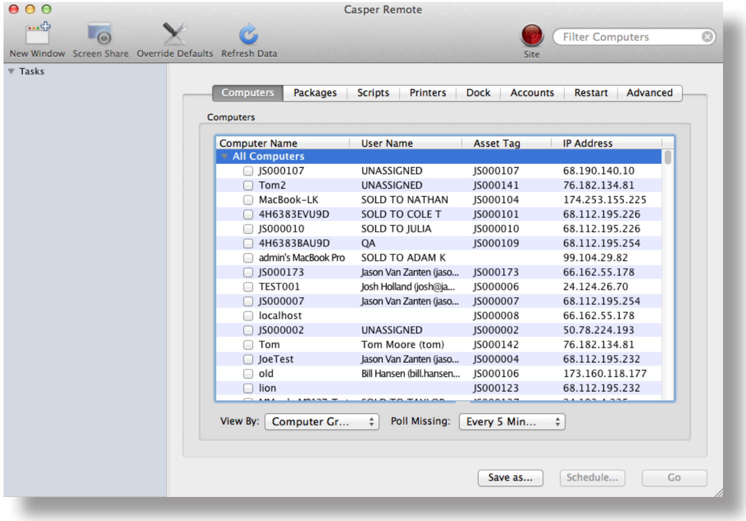
1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** and choose a site.

   This determines which items are available in Casper Remote.

   > ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to install the cached package.



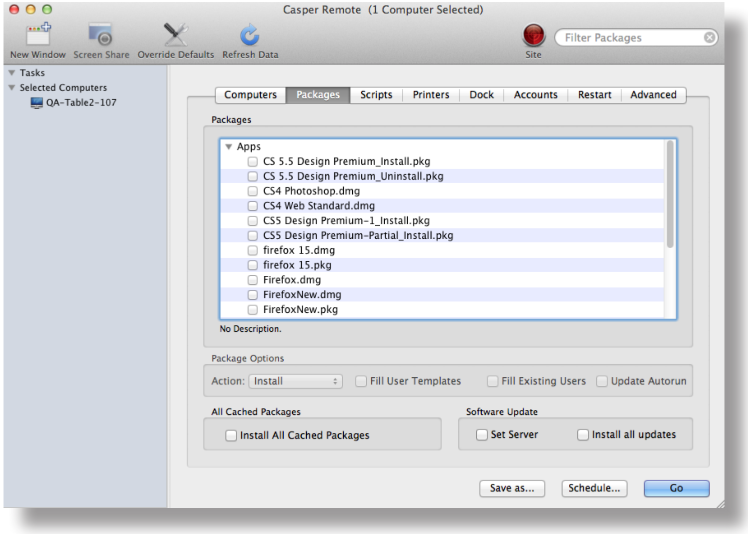
Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...

Poll Missing: Every 5 Min...

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the cached package you want to install.



Packages

- Apps
  - □ CS 5.5 Design Premium_Install.pkg
  - □ CS 5.5 Design Premium_Uninstall.pkg
  - □ CS4 Photoshop.dmg
  - □ CS4 Web Standard.dmg
  - □ CS5 Design Premium-1_Install.pkg
  - □ CS5 Design Premium-Partial_Install.pkg
  - □ firefox 15.dmg
  - □ firefox 15.pkg
  - □ Firefox.dmg
  - □ FirefoxNew.dmg
  - □ FirefoxNew.pkg

No Description.

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

All Cached Packages

□ Install All Cached Packages

Software Update

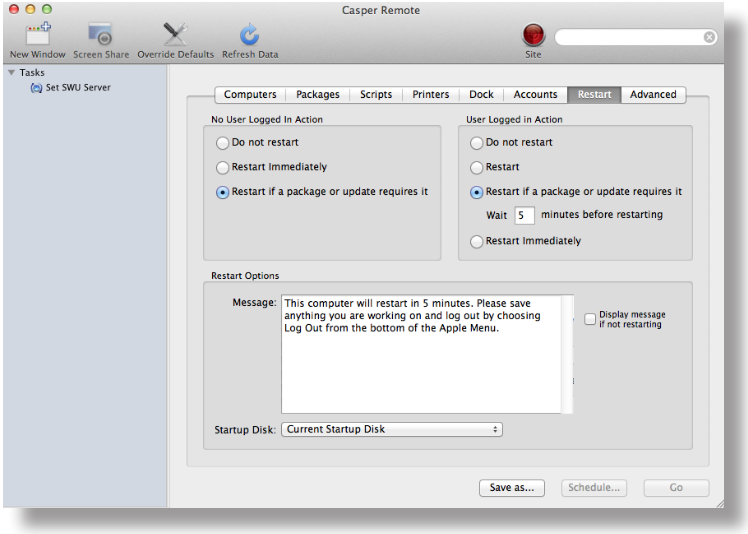
□ Set Server □ Install all updates

6. Choose "Install Cached" from the **Action** pop-up menu.

7. Configure the settings for the package.

   To add the package to each computer's Autorun data, select the **Update Autorun data** checkbox. For more information, see Autorun Imaging.

8. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart
○ Restart Immediately
● Restart if a package or update requires it

User Logged in Action

○ Do not restart
○ Restart
● Restart if a package or update requires it
Wait 5 minutes before restarting
○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

9. Do one of the following:
   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Installing All Cached Packages Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Maintenance payload and click **Configure**.
7. Select **Install Cached Packages**.
8. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
9. Click the **Scope** tab and configure the scope of the policy.

   For more information, see Scope.
10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.
11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.
12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

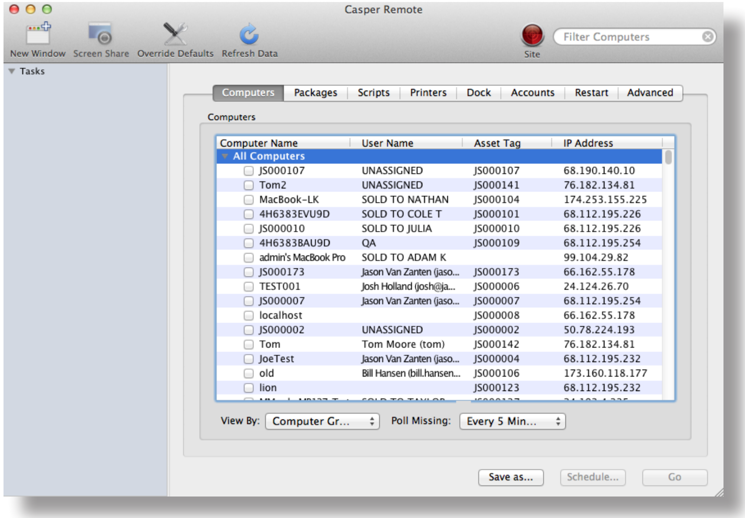
Installing All Cached Packages Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** ● and choose a site.

   This determines which items are available in Casper Remote.

   Note: This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to install all cached packages.



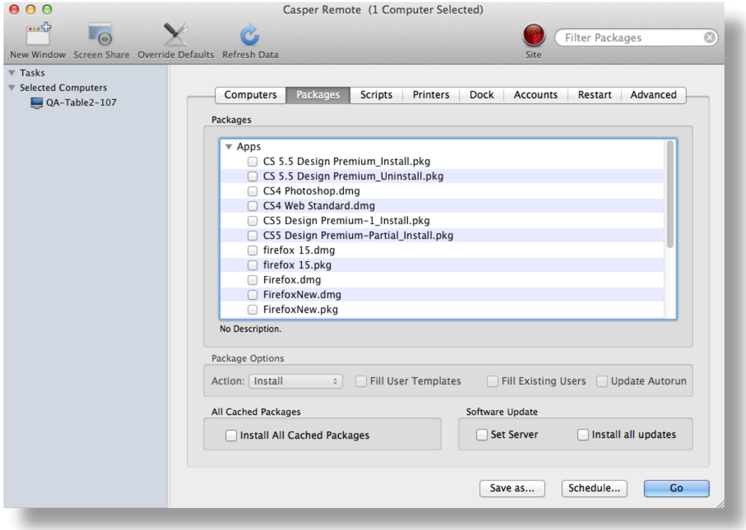
Computer Name	User Name	Asset Tag	IP Address
▾ All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...

Poll Missing: Every 5 Min...

4. Click the **Packages** tab.

5. Select the **Install All Cached Packages** checkbox.



▾ Apps
- □ CS 5.5 Design Premium_Install.pkg
- □ CS 5.5 Design Premium_Uninstall.pkg
- □ CS4 Photoshop.dmg
- □ CS4 Web Standard.dmg
- □ CS5 Design Premium-1_Install.pkg
- □ CS5 Design Premium-Partial_Install.pkg
- □ firefox 15.dmg
- □ firefox 15.pkg
- □ Firefox.dmg
- □ FirefoxNew.dmg
- □ FirefoxNew.pkg

No Description.

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

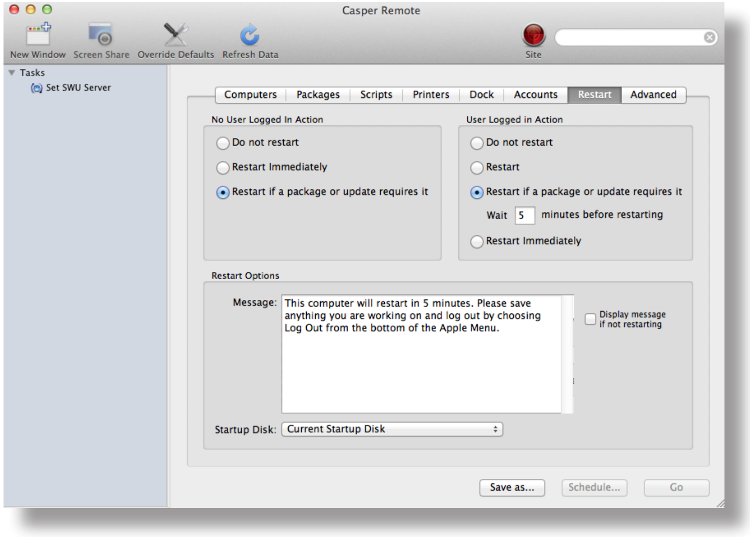
All Cached Packages

□ Install All Cached Packages

Software Update

□ Set Server □ Install all updates

6. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

7. Do one of the following:

- To immediately perform the tasks on the specified computers, click **Go**.
- To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.

Uninstalling Packages

There are two ways to uninstall packages that were installed using the Casper Suite: using a policy or using Casper Remote.

When you uninstall a package, you can remove the package from Autorun data.

Requirements

To uninstall a package from computers, you need:

- The package indexed in Casper Admin (For more information, see Managing Packages.)
- The package configured so that it can be uninstalled (For more information, see Managing Packages.)

> ***Note:*** If the package is an Adobe CS3/CS4 installation, it does not need to be indexed or configured so that it can be uninstalled.

Uninstalling a Package Using a Policy

1. Log in to the JSS with a web browser.
2. Click the **Computers** tab at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Packages payload and click **Configure**.
7. Click **Add** for the package you want to uninstall.
8. Choose “Uninstall” from the **Action** pop-up menu.
9. Configure the settings for the package.

   To remove the package from each computer's Autorun data, select the **Update Autorun data** checkbox. For more information on Autorun data and Autorun Imaging, see Autorun Imaging.
10. Use the Restart Options payload to configure settings for restarting computers.

    For more information, see Restart Options Payload.
11. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.

12. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

13. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

14. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

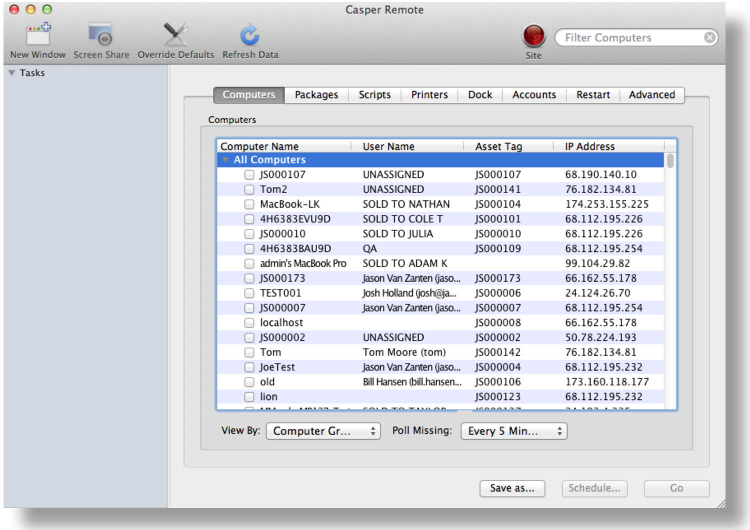
Uninstalling a Package Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** and choose a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer from which you want to uninstall the package.

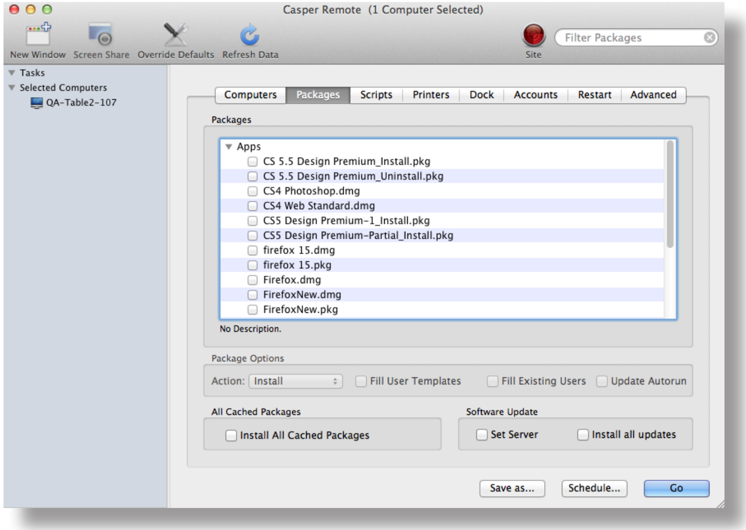


Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr... Poll Missing: Every 5 Min...

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the package you want to uninstall.



Packages

- Apps
  - □ CS 5.5 Design Premium_Install.pkg
  - □ CS 5.5 Design Premium_Uninstall.pkg
  - □ CS4 Photoshop.dmg
  - □ CS4 Web Standard.dmg
  - □ CS5 Design Premium-1_Install.pkg
  - □ CS5 Design Premium-Partial_Install.pkg
  - □ firefox 15.dmg
  - □ firefox 15.pkg
  - □ Firefox.dmg
  - □ FirefoxNew.dmg
  - □ FirefoxNew.pkg

No Description.

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

All Cached Packages

□ Install All Cached Packages

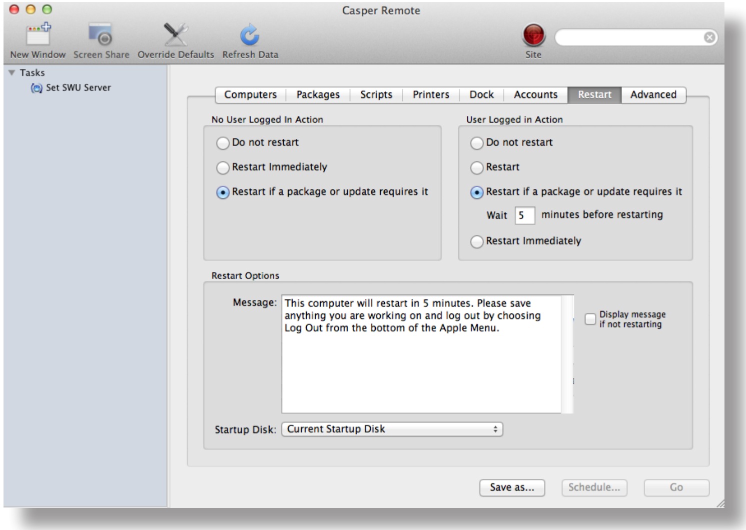
Software Update

□ Set Server □ Install all updates

6. Choose "Uninstall" from the **Action** pop-up menu.

7. Configure the settings for the package.

8. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart
○ Restart Immediately
● Restart if a package or update requires it

User Logged in Action

○ Do not restart
○ Restart
● Restart if a package or update requires it
Wait 5 minutes before restarting
○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

9. Do one of the following:
   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.

Patch Management

Running Software Update

When you run Software Update on computers, you can choose whether updates are installed from Apple's Software Update server or an internal software update server.

There are two ways to run Software Update on computers: using a policy or using Casper Remote.

Requirements

To have computers install updates from an internal software update server, the software update server must be in the JSS. (For more information, see Software Update Servers.)

Running Software Update Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, see General Payload.
6. Select the Software Updates payload and click **Configure**.
7. Specify a server for computers to install software updates from.
8. Use the Restart Options payload to configure settings for restarting computers.
   For more information, see Restart Options Payload.
9. Click the **Scope** tab and configure the scope of the policy.
   For more information, see Scope.

10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

12. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Running Software Update Using Casper Remote

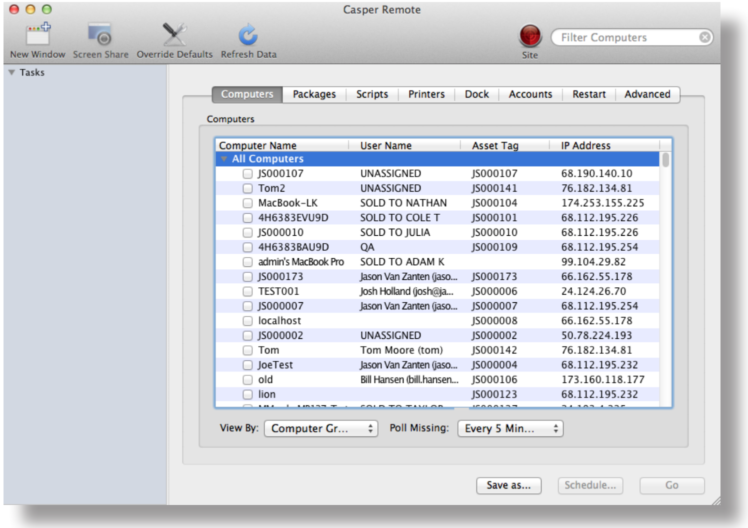
1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** and choose a site.

   This determines which items are available in Casper Remote.

   > ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to run Software Update.



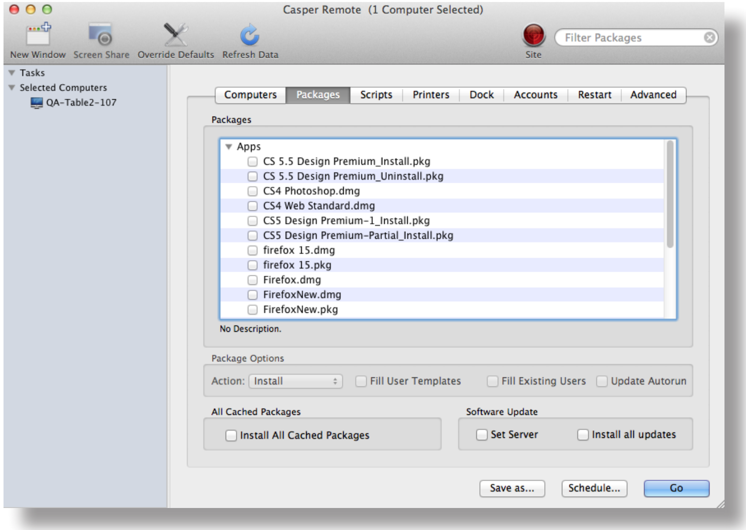
Computers

Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...   Poll Missing: Every 5 Min...

4. Click the **Packages** tab.

5. Select the **Install all updates** checkbox.



Packages

- Apps
  - □ CS 5.5 Design Premium_Install.pkg
  - □ CS 5.5 Design Premium_Uninstall.pkg
  - □ CS4 Photoshop.dmg
  - □ CS4 Web Standard.dmg
  - □ CS5 Design Premium-1_Install.pkg
  - □ CS5 Design Premium-Partial_Install.pkg
  - □ firefox 15.dmg
  - □ firefox 15.pkg
  - □ Firefox.dmg
  - □ FirefoxNew.dmg
  - □ FirefoxNew.pkg

No Description.

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

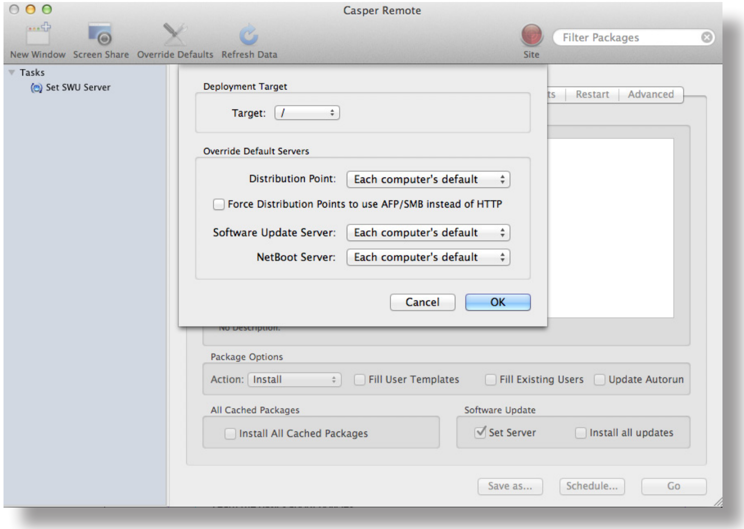
All Cached Packages

□ Install All Cached Packages

Software Update

□ Set Server □ Install all updates

6. If you want to change the software update server that computers download software updates from, click **Override Defaults** and choose a software update server.



Deployment Target

Target: /

Override Default Servers

Distribution Point: Each computer's default

□ Force Distribution Points to use AFP/SMB instead of HTTP

Software Update Server: Each computer's default

NetBoot Server: Each computer's default

Package Options

Action: Install □ Fill User Templates □ Fill Existing Users □ Update Autorun

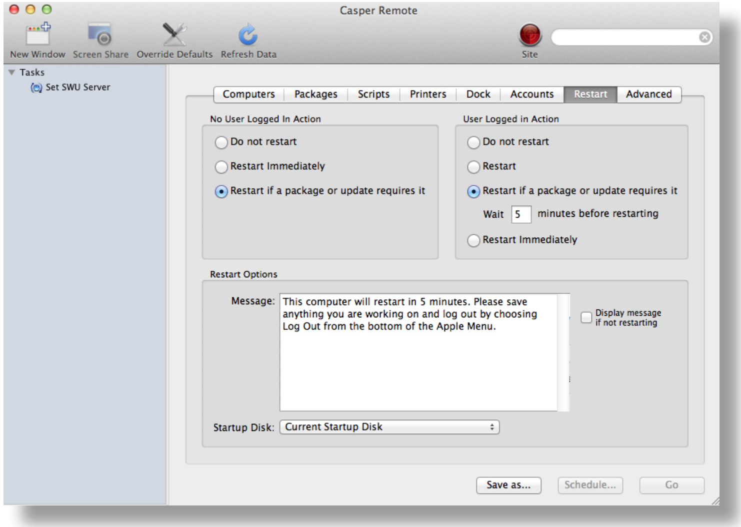
All Cached Packages

□ Install All Cached Packages

Software Update

☑ Set Server □ Install all updates

7. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

8. Do one of the following:
   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.
- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.

Remote Control

Screen Sharing

Screen sharing allows you to remotely view and control the screen of another computer. You can allow the end user to see the screen sharing session, or you can hide the screen sharing session so that the user is not interrupted.

How Screen Sharing Works

When a screen sharing session is initiated from Casper Remote, the following steps are performed to start the screen sharing session:

1. Casper Remote creates an SSH connection to the target computer.
2. Casper Remote checks the target computer for the most current version of the jamf binary.

   If the jamf binary is out of date or missing, Casper Remote installs the most current version over SCP or HTTP, depending on the way the Casper Remote preferences are configured.
3. Casper Remote checks the target 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 or overwrites the file.
4. The jamf binary checks if the JSS user who initiated the screen sharing session has the "Screen Share with Remote Computers" and "Screen Share with Remote Computers without Asking" privilege.
5. If the JSS user does not have the "Screen Share with Remote Computers without Asking" privilege, the end user is prompted to allow the screen sharing session to take place.
6. The JSS logs the connection.
7. On the target computer, Casper Remote starts the Screen Sharing service that is built into OS X.
8. On the target computer, Casper Remote creates a temporary account with limited privileges and uses it for the screen sharing session.

When the Screen Sharing window is closed, Casper Remote deletes the temporary account, stops the Screen Sharing service, and logs out of the SSH connection. If the SSH connection is terminated unexpectedly, a launch daemon deletes the temporary account and stops the Screen Sharing service within 60 seconds of the SSH connection being terminated.

Requirements

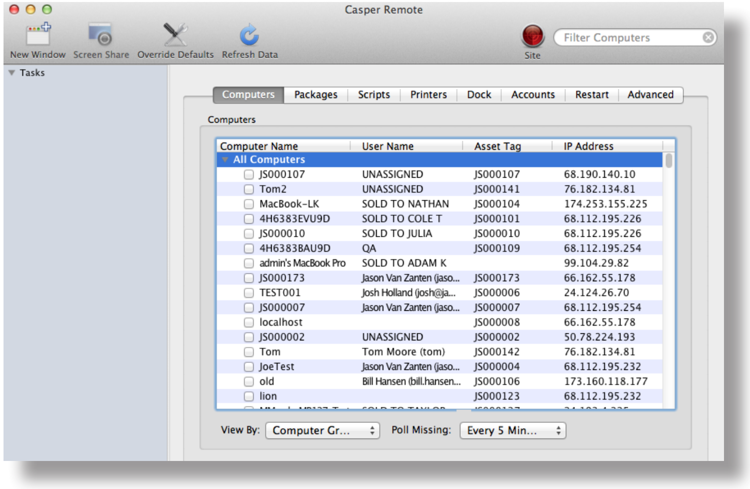
To share the screen of another computer, SSH (Remote Login) must be enabled on the target computer.

Sharing the Screen of Another Computer

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** and choose a site.
   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the computer that you want to screen share with.



Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232
[illegible]	[illegible]	[illegible]	[illegible]

View By: Computer Gr... Poll Missing: Every 5 Min...

4. Click **Screen Share** .
5. When prompted, choose a screen sharing option:
   - To allow the end user to see the screen sharing session, choose "Share Display" (OS X v10.8 and 10.9) or "Ask to share the display" (OS X v10.7).
   - To hide the screen sharing session, choose "Log In" (OS X v10.8 and 10.9) or "Connect to a virtual display" (OS X v10.7).

If you do not have the "Screen Share Remote Computers Without Asking" privilege, the end user is prompted to allow the screen sharing session to take place.

Settings and Security Management

Managed Preferences

Managed Preferences are manifest files that define preferences for computers and users. You can use the JAMF Software Server (JSS) to create Managed Preference profiles, which contain groups of Managed Preferences. You can also specify the users and computers for which a profile should be applied (called "scope").

The JSS comes with manifest files for many common Managed Preferences so that you can easily add them to profiles. You can also add custom Managed Preferences by creating them manually or uploading a manifest file.

Levels for Managed Preferences

When you add a Managed Preference to a profile, you must specify a level at which to apply the preference. The level determines how and when the preference is applied. The levels available for each Managed Preference depend on the application or utility for which you are defining the preference.

If you have applied Managed Preferences using Apple's Workgroup Manager, the level names in the JSS may be unfamiliar to you. The following table shows each level, its Workgroup Manager equivalent, when and how it is applied, and whether it is available for some or all Managed Preferences.

JSS Levels	Workgroup Manager Levels	Applied at	Available for
User-level enforced	Always	Login with a login hook	Some Managed Preferences
User-level at every login	Often	Login with a login hook	All Managed Preferences
User-level at next login only	Once	Login with a login hook	All Managed Preferences
Computer-level enforced	Always (Applied to a computer object)	Reboot with a startup script	Some Managed Preferences
Unmanaged	Unset	Login or reboot	All Managed Preferences

Compatibility with Third-Party Providers

In OS X v10.6 and v10.7, you can use more than one provider to apply Managed Preferences. In some cases, Managed Preferences applied using the JSS can interfere with or be interfered with by Managed Preferences from a third-party provider.

The following table shows the compatibility of Managed Preferences applied using the JSS and tested third-party providers.

Third-Party Provider	Local Home Directory	Network Home Directory	Mobile Home Directory
OS X Directory Utility–Active Directory	Compatible	Compatible	Compatible
OS X Directory Utility–Open Directory	Compatible	Compatible	Compatible
PowerBroker Identity Services (formerly called "Likewise")	Compatible	N/A	Incompatible
ADmitMac	Compatible	Compatible	Incompatible
Centrify	Compatible	N/A	Incompatible

Requirements

To apply user-level Managed Preferences, they must be enabled in the Login/Logout Hooks settings in the JSS. (For more information, see Login and Logout Hooks.)

To apply computer-level Managed Preferences, they must be enabled in the Startup Script settings in the JSS. (For more information, see Startup Script.)

Creating a Managed Preference Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Managed Preferences**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the profile.
6. Use the rest of the payloads to configure the Managed Preferences you want to apply.

7. (Optional) Manually create a custom Managed Preference:
   a. Select the Custom payload.
   b. Click **Add** ⊕ for **Manual Setting**.
   c. Configure the Managed Preference using the options on the pane.

8. (Optional) Upload a manifest file:
   a. Select the Custom payload.
   b. Click **Add** ⊕ for **Upload Manifest**.
   c. Upload the manifest file.

9. Click the **Scope** tab and configure the scope of the profile.
   For more information, see Scope.

10. Click **Save**.

The profile is applied the next time computers in the scope check in with the JSS.

Cloning, Editing, or Deleting a Managed Preference Profile

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

2. Click **Computers** at the top of the page.

3. Click **Managed Preferences**.
   On a smartphone, this option is in the pop-up menu.

4. Click the Managed Preference profile you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the profile, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the profile, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the profile, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS.

Related Information

For related information, see the following section in this guide.

Viewing Managed Preferences for a Single Computer
Find out how to view managed preferences for a single computer or user.

OS X Configuration Profiles

OS X configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for computers and users.

You can use the JAMF Software Server (JSS) to manually create an OS X configuration profile or upload a configuration profile that was created using Apple's Profile Manager.

Before creating a configuration profile, you should have basic knowledge of configuration profile payloads and settings, and how they affect computers. For detailed information about each payload and setting, see Apple's Profile Manager documentation at:

https://help.apple.com/profilemanager/mac

Some configuration profile settings are unique to the JSS. For more information on these settings, see the following Knowledge Base article:

Configuration Profiles Reference

When you create an OS X configuration profile, you must specify the level at which to apply the profile—computer level or user level. Each level has a unique set of payloads and a few that are common to both. You can also specify the computers and users to which the profile should be applied (called "scope").

Payload Variables for OS X Configuration Profiles

There are several payload variables that you can use to populate settings in an OS X configuration profile with attribute values stored in the JSS. This allows you to create payloads containing information about each computer and user to which you are distributing the profile.

To use a payload variable, enter the variable into any text field when creating a configuration profile in the JSS. When the profile is installed on a computer, the variable is replaced with the value of the corresponding attribute in the JSS.

Variable	Computer Information
$COMPUTERNAME	Computer Name
$UDID	UDID
$SERIALNUMBER	Serial Number
$USERNAME	Username associated with the computer in the JSS (computer-level profiles only) Username of the user logging in to the computer (user-level profiles only)

Variable	Computer Information
`$FULLNAME` or `$REALNAME`	Full Name
`$EMAIL`	Email Address
`$PHONE`	Phone Number
`$ROOM`	Room
`$POSITION`	Position
`$MACADDRESS`	MAC Address
`$EXTENSIONATTRIBUTE_<#>`	Value for any LDAP attribute

Note: An `$EXTENSIONATTRIBUTE_<#>` variable is generated each time you create an extension attribute with the "LDAP Attribute Mapping" input type. For more information, see Computer Extension Attribute Input Types.

Requirements

To install an OS X configuration profile, you need:

- Computers with OS X v10.7 or later
- The **Enable certificate-based authentication** and **Enable push notifications** settings configured in the JSS. (For more information, see Security Settings.)
- (User-level profiles only) Computers that are bound to a directory service (For more information, see Binding to Directory Services.)
- (User-level profiles only) Login hooks configured in your environment (For information on creating login hooks with the Casper Suite, see Login and Logout Hooks.)

Manually Creating an OS X Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings, including the level at which to apply the profile.

   Only payloads and settings that apply to the selected level are displayed for the profile.
6. Use the rest of the payloads to configure the settings you want to apply.
7. Click the **Scope** tab and configure the scope of the profile.

   For more information, see Scope.

8. Click **Save**.

   Computer-level profiles are installed the next time computers in the scope check in with the JSS. User-level profiles are installed the next time users in the scope log in to their computers.

Uploading an OS X Configuration Profile

You can create an OS X configuration profile by uploading a profile that was created using Apple's Profile Manager.

> ***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 still applied to computers and users.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Upload** ↑ and upload the configuration profile (.mobileconfig).
5. Use the General payload to change or configure basic settings for the profile.
6. Use the rest of the payloads to configure or edit settings as needed.
7. Click the **Scope** tab and configure the scope of the profile.
   For more information, see Scope.
8. Click **Save**.

   Computer-level profiles are installed the next time computers in the scope check in with the JSS. User-level profiles are installed the next time users in the scope log in to their computers.

Cloning, Editing, or Deleting an OS X Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click the configuration profile you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the profile, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the profile, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the profile, click **Delete** and then click **Delete** again to confirm.

For computer-level profiles, the clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS. For user-level profiles, the clone, edit, or delete action is applied the next time users in the scope log in to their computers.

Downloading an OS X Configuration Profile

If you want to view the contents of an OS X configuration profile for troubleshooting purposes, you can download the profile (.mobileconfig) from the JSS.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click the configuration profile you want to download.
5. Click **Download**.

The profile downloads immediately.

Related Information

For related information, see the following sections in this guide:

- Viewing the Pending Management Commands for a Single Computer
  Find out how to view and cancel pending OS X configuration profile installations and removals for a single computer.
- Viewing Management History for a Single Computer
  Find out how to view all completed, pending, and failed OS X configuration profile installations and removals for a single computer.
- Viewing Configuration Profiles for a Single Computer
  Find out how to view the OS X configuration profiles in the scope for a single computer.

OS X Remote Commands

The OS X remote commands available in the JAMF Software Server (JSS) allow you to remotely perform the following tasks on a computer:

- Manage security by locking or wiping the computer.
- Remove the MDM profile.
- Send a blank push notification.

You can send an OS X remote command to a single computer.

The following table describes the OS X remote commands that you can send from the JSS.

OS X Remote Command	Description
Lock Computer	Logs the user out of the computer, restarts the computer, and then locks the computer To unlock the computer, the user must enter the passcode that you specified when you sent the Lock Computer command.
Remove MDM Profile	Removes the MDM profile from the computer, along with any configuration profiles that were distributed with the Casper Suite If the MDM profile is removed, you can no longer send remote commands or distribute configuration profiles to the computer. ***Note:*** Removing the MDM profile from a computer does not remove the computer from the JSS or change its inventory information.
Wipe Computer	Permanently erases all data on the computer ***Note:*** Wiping a computer does not remove the computer from the JSS or change its inventory information. To restore the computer to the original factory settings, the user must enter the passcode that you specified when you sent the Wipe Computer command, and then reinstall the operating system. For detailed information on OS X Recovery, see the following Apple Knowledge Base article: https://support.apple.com/kb/HT4718
Send Blank Push	Sends a blank push notification, prompting the computer to check in with Apple Push Notification service (APNs)

Requirements

To manage OS X remote commands, you need:

- Computers with OS X v10.7 or later and a Recovery Partition
- A push certificate in the JSS (For more information, see Push Certificates.)
- The **Enable certificate-based authentication** and **Enable push notifications** settings configured in the JSS (For more information, see Security Settings.)

Sending an OS X Remote Command

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to send the OS X remote command to.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **Management** tab, and then click the button for the remote command that you want to send.
   - If you are sending a Lock Computer command, type a password that the user must enter to unlock the computer.
   - If you are sending a Wipe Computer command, type a password that the user must enter to restore the computer.

The remote command runs on the computer the next time the computer checks in with the JSS.

Viewing the Status of OS X Remote Commands

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view OS X remote commands for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab.
6. Use the Management History pane to view completed, pending, or failed commands.

Canceling an OS X Remote Command

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.

4. Click the computer for which you want to cancel an OS X remote command.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.

5. Click the **History** tab, and then click **Pending Commands**.

6. Find the command you want to cancel, and click **Cancel** across from it.

Managing Scripts

The way you manage scripts depends on the way scripts are stored in your environment. There are two ways scripts can be stored:

- **As data in the jamfsoftware database**—Before you can run a script in this type of environment, the script must exist in the database. There are two ways to achieve this:
  - Add the script to Casper Admin
  - Add the script to the JSS using the script editor
- **As files on your distribution point(s)**—Before you can run a script in this type of environment, the script must exist on the distribution point you plan to deploy it from and in the JSS. You can add the script to the master distribution point by adding it to Casper Admin. Then you can add the script to other distribution points via replication.

Note: For more information on migrating the scripts on your master distribution point, see the following Knowledge Base article:

Migrating Packages and Scripts

Each of these methods also involves configuring settings for the script. When you configure settings for a script, you can do the following:

- Add the script to a category. (For more information, see Categories.)
- Choose a priority for running the script during imaging.
- Enter parameter labels.
- Specify operating system requirements for running the script.

When you add, edit, or delete a script in Casper Admin, the changes are reflected in the JSS and vice versa.

Requirements

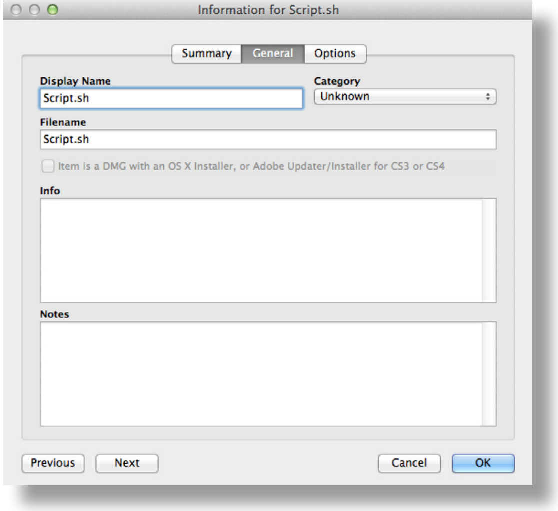
To add a script to Casper Admin, the script file must be non-compiled and in one of the following formats:

- Perl (.pl)
- Bash (.sh)
- Shell (.sh)
- Non-compiled AppleScript (.applescript)
- C Shell (.csh)
- Zsh (.zsh)
- Korn Shell (.ksh)
- Tool Command Language (.tcl)
- Hypertext Preprocessor (.php)
- Ruby (.rb)
- Python (.py)

Adding a Script to Casper Admin

Adding a script to Casper Admin adds the script to the jamfsoftware database or the master distribution point, and to the JSS.

1. Open Casper Admin and authenticate to the JSS.
2. Drag the script to the main repository in Casper Admin.
   The script is displayed in blue text in the Unknown category until you add it to a category.
3. Double-click the script in the main repository.
4. Click the **General** tab and configure basic settings for the script, including the display name and category.



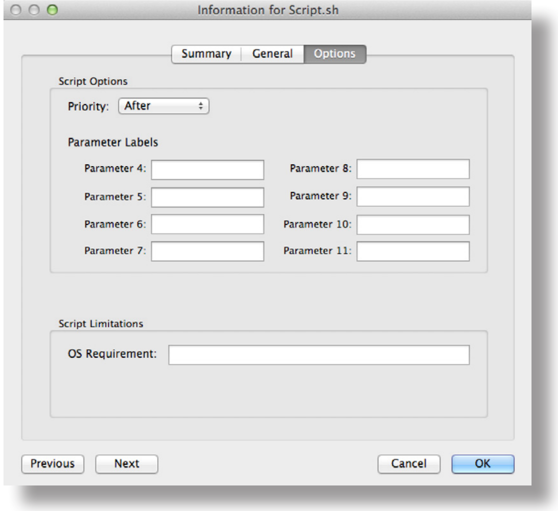
Display Name: Script.sh

Category: Unknown

Filename: Script.sh

□ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

5. Click the **Options** tab and configure additional settings for the script, including the priority and parameter labels.



Priority: After

6. Click **OK**.

Adding a Script to the JSS

If your environment is one in which scripts are stored in the jamfsoftware database, you can add a script to the JSS using the script editor.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Scripts** .
5. Click **New** + .
6. Use the General pane to configure basic settings for the script, including the display name and category.

   Note: If you do not add the script to a category, Casper Admin displays the script in blue text in the Unknown category.

7. Click the **Script** tab and enter the script contents in the script editor.
8. Click the **Options** tab and configure additional settings for the script, including the priority.
9. (Optional) Click the **Limitations** tab and configure operating system requirements for the script.
10. Click **Save**.

Editing or Deleting a Script Using Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the script you want to edit or delete.
3. Do one of the following:
   - To edit the script, double-click it and make changes as needed. Then click **OK**.
   - To delete the script, click **Delete** 🚫 and then click **Delete** again to confirm.

   If the script is stored in the jamfsoftware database, the edit or delete action is applied immediately.

   If the script is stored on your distribution point(s), the edit or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.

Cloning, Editing, Deleting a Script Using the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Scripts** >_ .
5. Click the script you want to edit or delete.
6. Do one of the following:
   - To clone the script, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the script, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the script, click **Delete** and then click **Delete** again to confirm.

If the script is stored in the jamfsoftware database, the clone, edit, or delete action is applied immediately.

If the script is stored on your distribution point(s), the clone, edit, or delete action is applied immediately on the master distribution point. The action is applied to your other distribution points when replication occurs.

Related Information

For related information, see the following section in this guide:

Running Scripts
Find out how to run scripts using a policy or Casper Remote.

Running Scripts

When you run a script, you can choose a priority for running the script. You can also enter parameter values for the script.

There are two ways to run scripts on computers: using a policy or using Casper Remote.

Requirements

To run a script on computers, the script must exist on the distribution point you plan to deploy it from and in the JSS, or in the jamfsoftware database. (For more information, see Managing Scripts.)

Running a Script Using a Policy

1. Log in to the JSS with a web browser.
2. Click the **Computers** tab at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, see General Payload.
6. Select the Scripts payload and click **Configure**.
7. Click **Add** for the script you want to run.
8. Configure the settings for the script.
9. Use the Restart Options payload to configure settings for restarting computers.
   For more information, see Restart Options Payload.
10. Click the **Scope** tab and configure the scope of the policy.
    For more information, see Scope.
11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.
    For more information, see Self Service Policies.
12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.
    For more information, see User Interaction.

13. Click **Save**.

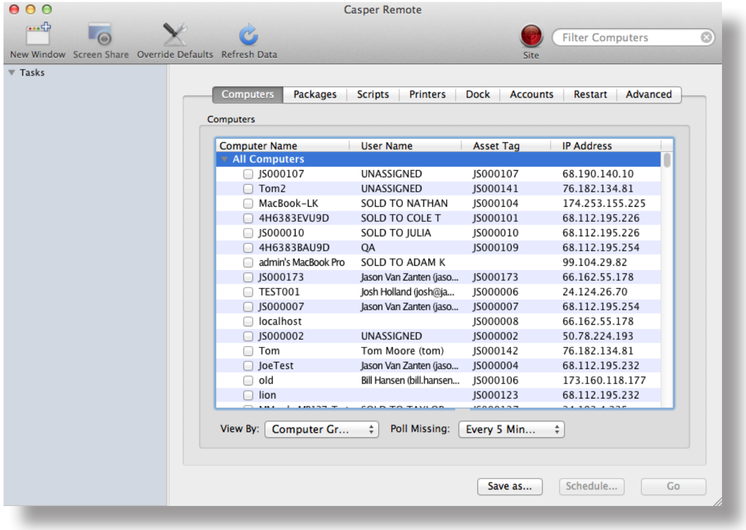
    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Running a Script Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** ● and choose a site.
   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

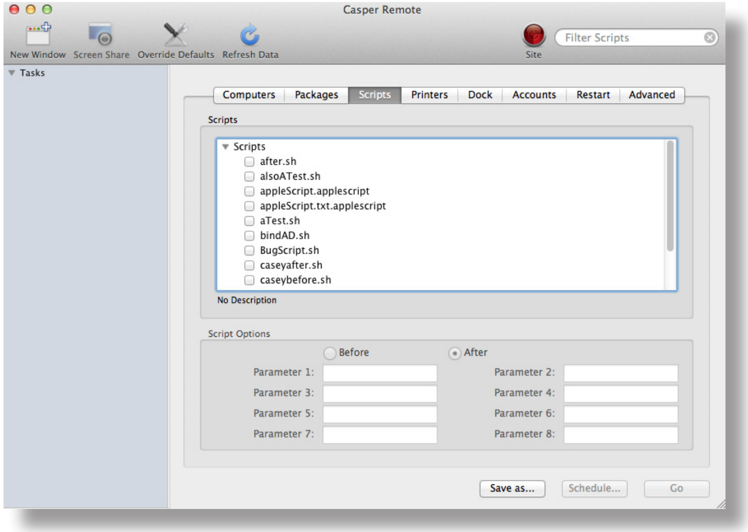
3. In the list of computers, select the checkbox for each computer on which you want to run the script.



Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

4. Click the **Scripts** tab.

5. In the list of scripts, select the checkbox for the script you want to run.



Scripts

- Scripts
  - ☐ after.sh
  - ☐ alsoATest.sh
  - ☐ appleScript.applescript
  - ☐ appleScript.txt.applescript
  - ☐ aTest.sh
  - ☐ bindAD.sh
  - ☐ BugScript.sh
  - ☐ caseyafter.sh
  - ☐ caseybefore.sh

No Description

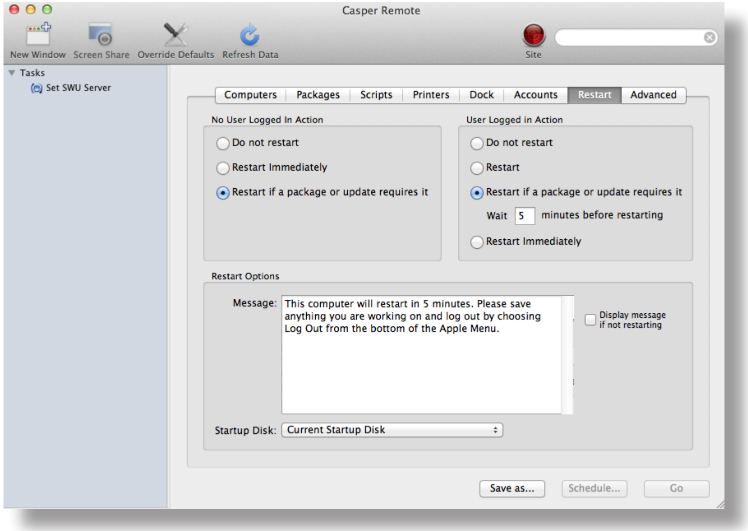
Script Options

○ Before ● After

Parameter 1: Parameter 2:
Parameter 3: Parameter 4:
Parameter 5: Parameter 6:
Parameter 7: Parameter 8:

6. Configure the settings for the script.

7. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart
○ Restart Immediately
● Restart if a package or update requires it

User Logged in Action

○ Do not restart
○ Restart
● Restart if a package or update requires it
Wait 5 minutes before restarting
○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

☐ Display message if not restarting

Startup Disk: Current Startup Disk

8. Do one of the following:
   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.
- Managing Policies

  Find out how to create policies, view the plan and status for a policy, and view and flush policy logs.

Managing Printers

Adding printers to Casper Admin or the JAMF Software Server (JSS) is the first step to administering printers on computers.

When you add a printer to Casper Admin, you choose from a list of printers that are on the computer running Casper Admin. When you add a printer to the JSS, you manually specify information about the printer, such as the CUPS name and device URI.

When you add, edit, or delete a printer in Casper Admin, the changes are reflected in the JSS and vice versa.

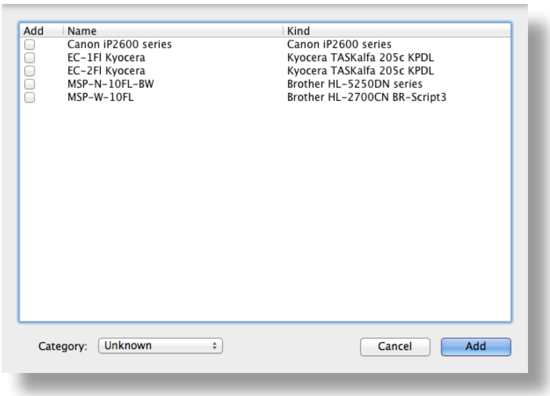
When you configure a printer, you can do the following:

- Add the printer to a category.
- Choose whether or not the printer is set as the default when mapped during imaging.
- Specify an operating system requirement for mapping the printer.

Adding a Printer to Casper Admin

Several settings in Casper Admin have tool tips. To read more about a specific setting, hover your mouse over it until a tool tip is displayed.

1. Open Casper Admin and authenticate to the JSS.
2. Click **Add Printers** 🖨.
3. If prompted, authenticate locally.
4. Select the checkbox next to each printer you want to add.

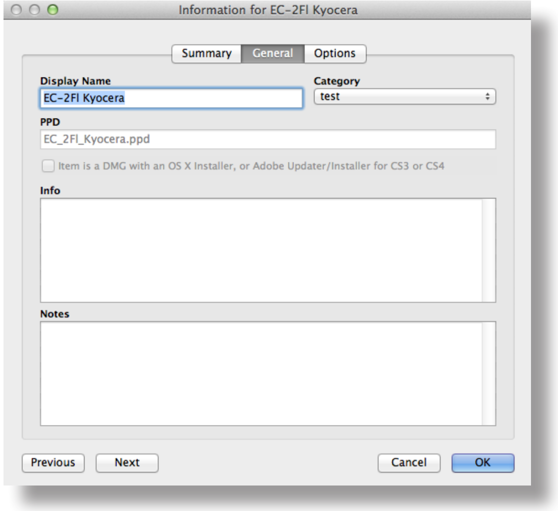


Add	Name	Kind
☐	Canon iP2600 series	Canon iP2600 series
☐	EC-1Fl Kyocera	Kyocera TASKalfa 205c KPDL
☐	EC-2Fl Kyocera	Kyocera TASKalfa 205c KPDL
☐	MSP-N-10FL-BW	Brother HL-5250DN series
☐	MSP-W-10FL	Brother HL-2700CN BR-Script3

Category: Unknown

5. (Optional) Choose a category to add printer(s) to.
6. Click **Add**.
7. Select the printer in the main repository and double-click it.

8. Click the **General** tab and configure basic settings for the printer, including the display name and category.


Information for EC-2FI Kyocera

Display Name: EC-2FI Kyocera

Category: test

PPD: EC_2FI_Kyocera.ppd

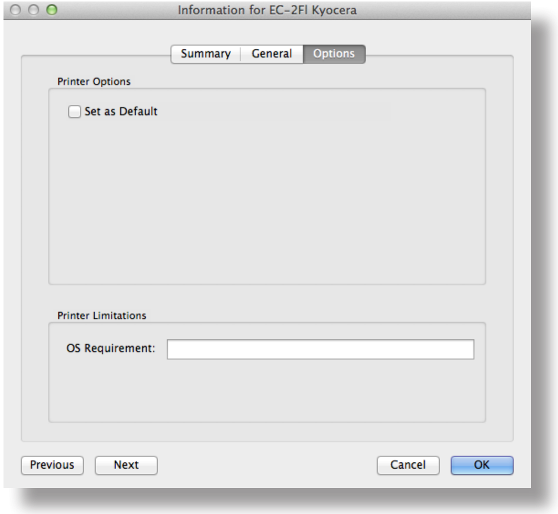
□ Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4

Info

Notes

9. Click the **Options** tab.

10. Choose whether or not the printer is set as the default when mapped during imaging, and configure the operating system requirement.


Information for EC-2FI Kyocera

Printer Options

□ Set as Default

Printer Limitations

OS Requirement:

11. Click **OK**.

Adding a Printer to the JSS

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

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.

4. In the "Computer Management" section, click **Printers** 🖨 .

5. Click **New** + .

6. Use the General pane to configure basic settings for the printer, including the display name and category.

7. Click the **Definition** tab and specify information about the printer, including the CUPS name and device URI.

8. (Optional) Click the **Limitations** tab and specify an operating system requirement.

9. Click **Save**.

Editing or Deleting a Printer in Casper Admin

Several settings in Casper Admin have tool tips. To read more about a specific setting, hover your mouse over it until a tool tip is displayed.

1. Open Casper Admin and authenticate to the JSS.

2. In the main repository, select the printer you want to edit or delete.

3. Do one of the following:
   - To edit the printer, double-click it and make changes as needed. Then click **OK**.
   - To delete the printer, click **Delete** 🚫 and then click **Delete** again to confirm.

Cloning, Editing, or Deleting a Printer in the JSS

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

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.

4. In the "Computer Management" section, click **Printers** 🖨 .

5. Click the printer you want to clone, edit, or delete.

6. Do one of the following:
   - To clone the printer, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the printer, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the printer, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Administering Printers
Find out how to map and unmap printers using a policy or Casper Remote.

Administering Printers

There are two ways to map or unmap printers on computers: using a policy or using Casper Remote.

Note: You can also map printers during imaging. For more information, see Configurations.

When you map a printer, you can choose whether or not to make the printer the default.

Requirements

To map or unmap a printer, the printer must be added to Casper Admin or the JSS. (For more information, see Managing Printers.)

Mapping or Unmapping a Printer Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Printers payload and click **Configure**.
7. Click **Add** across from the printer you want to map or unmap.
8. Choose "Map" or "Unmap" from the **Action** pop-up menu.
9. (Optional) If you are mapping the printer, make it the default printer by selecting the **Set as Default** checkbox.
10. Use the Restart Options payload to configure settings for restarting computers.

    For more information, see Restart Options Payload.
11. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.
12. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

13. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

14. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

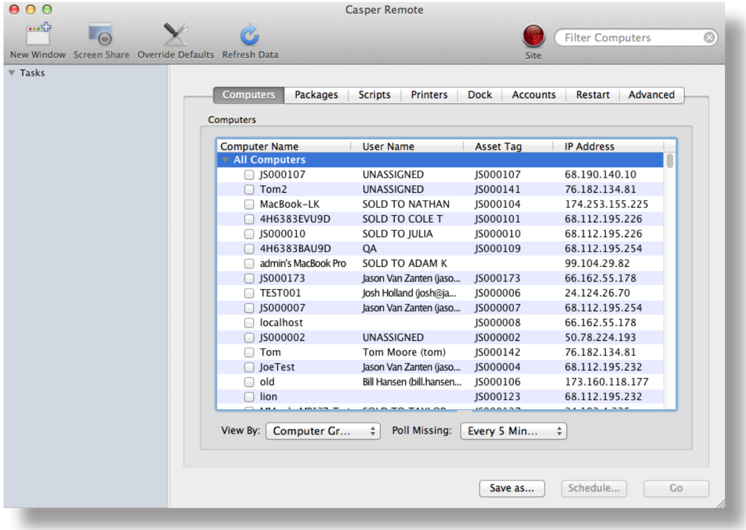
Mapping or Unmapping a Printer Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** and choose a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to map or unmap the printer.

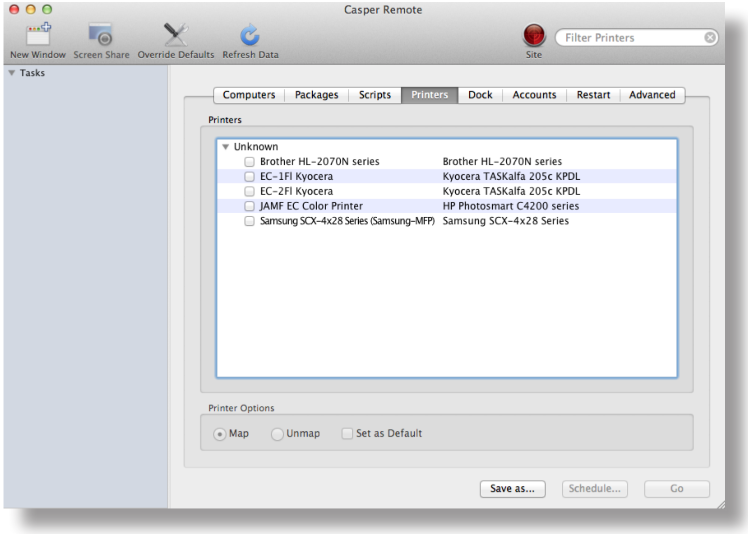


Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...   Poll Missing: Every 5 Min...

4. Click the **Printers** tab.

5. In the list of printers, select the checkbox for the printer you want to map or unmap.



Printers

▼ Unknown

□ Brother HL-2070N series	Brother HL-2070N series
□ EC-1Fl Kyocera	Kyocera TASKalfa 205c KPDL
□ EC-2Fl Kyocera	Kyocera TASKalfa 205c KPDL
□ JAMF EC Color Printer	HP Photosmart C4200 series
□ Samsung SCX-4x28 Series (Samsung-MFP)	Samsung SCX-4x28 Series

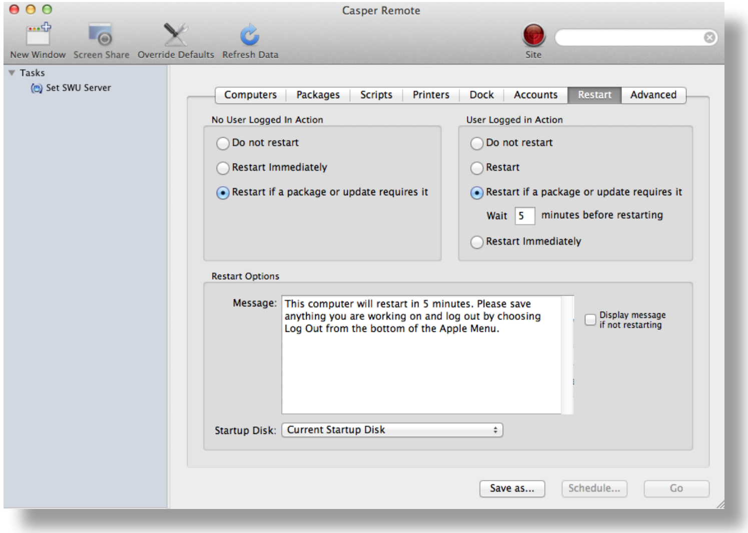
Printer Options

● Map ○ Unmap □ Set as Default

6. Select the **Map** or **Unmap** option.

7. (Optional) Make the printer the default by selecting the **Set as Default** checkbox.

8. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

9. Do one of the following:

- To immediately perform the tasks on the specified computers, click **Go**.
- To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- Smart Computer Groups

  You can create smart computer groups based on mapped printers.

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create policies, view the plan and status of a policy, and view and flush policy logs.

Managing Dock Items

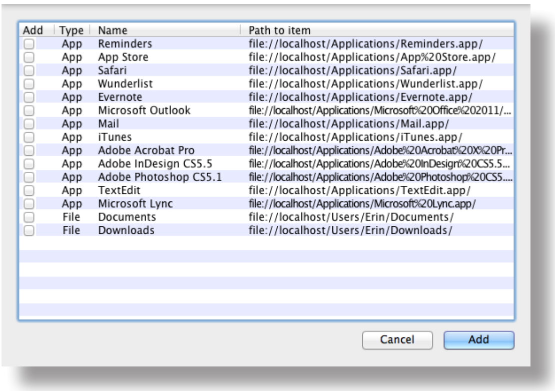
Adding Dock items to Casper Admin or the JAMF Software Server (JSS) is the first step to administering Dock items on computers.

When you add a Dock item to Casper Admin, you choose from a list of Dock items that are on the computer running Casper Admin. When you add a Dock item to the JSS, you manually specify information about the Dock item.

When you add, edit, or delete a Dock item in Casper Admin, the changes are reflected in the JSS and vice versa.

Adding a Dock Item to Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. Click **Add Dock Items** .
3. Select the checkbox next to each Dock item you want to add.



Add	Type	Name	Path to item
□	App	Reminders	file://localhost/Applications/Reminders.app/
□	App	App Store	file://localhost/Applications/App%20Store.app/
□	App	Safari	file://localhost/Applications/Safari.app/
□	App	Wunderlist	file://localhost/Applications/Wunderlist.app/
□	App	Evernote	file://localhost/Applications/Evernote.app/
□	App	Microsoft Outlook	file://localhost/Applications/Microsoft%20Office%202011/...
□	App	Mail	file://localhost/Applications/Mail.app/
□	App	iTunes	file://localhost/Applications/iTunes.app/
□	App	Adobe Acrobat Pro	file://localhost/Applications/Adobe%20Acrobat%20X%20Pr...
□	App	Adobe InDesign CS5.5	file://localhost/Applications/Adobe%20InDesign%20CS5.5...
□	App	Adobe Photoshop CS5.1	file://localhost/Applications/Adobe%20Photoshop%20CS5....
□	App	TextEdit	file://localhost/Applications/TextEdit.app/
□	App	Microsoft Lync	file://localhost/Applications/Microsoft%20Lync.app/
□	File	Documents	file://localhost/Users/Erin/Documents/
□	File	Downloads	file://localhost/Users/Erin/Downloads/

4. Click **Add**.

Adding a Dock Item to the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Dock Items** .
5. Click **New** + .

6. Configure the Dock item using the settings on the pane.
7. Click **Save**.

Deleting a Dock Item in Casper Admin

1. Open Casper Admin and authenticate to the JSS.
2. In the main repository, select the Dock item you want to delete.
3. Click **Delete** 🚫 and then click **Delete** again to confirm.

Cloning, Editing, or Deleting a Dock Item in the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Dock Items** 🖥 .
5. Click the Dock item you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the Dock item, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the Dock item, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the Dock item, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Administering Dock Items
Find out how to add and remove Dock items using a policy or Casper Remote.

Administering Dock Items

There are two ways to add or remove Dock items on computers: using a policy or using Casper Remote.

When you add a Dock item on computers, you can choose whether to add it to the beginning or the end of the Dock.

Requirements

To add or remove a Dock item on computers, the Dock item must be added to Casper Admin or the JSS. (For more information, see Managing Dock Items.)

Adding or Removing a Dock Item Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Dock Items payload and click **Configure**.
7. Click **Add** for the Dock item you want to add or remove.
8. Choose "Add to Beginning of Dock", "Add to End of Dock", or "Remove from Dock" from the **Action** pop-up menu.
9. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
10. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.
11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.
12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

13. Click **Save**.

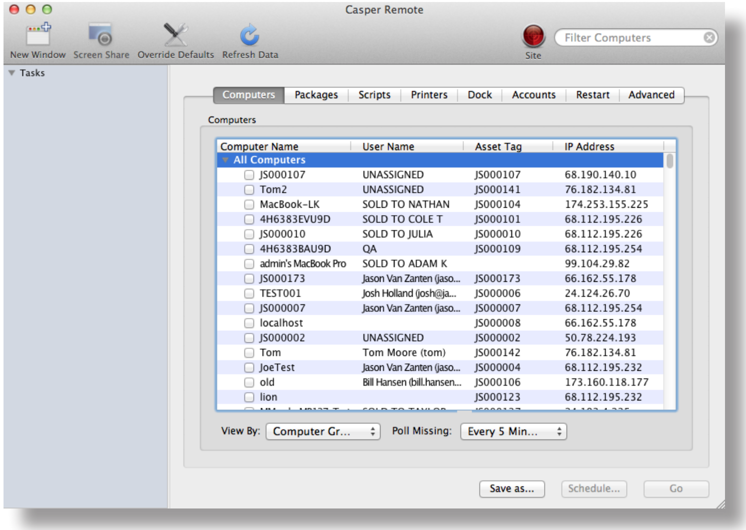
The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Adding or Removing a Dock Item Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** ● and choose a site.
   This determines which items are available in Casper Remote.

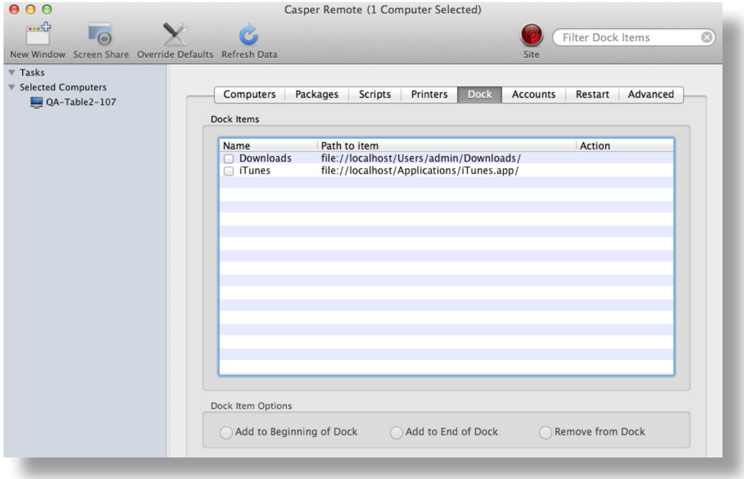
> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to add or remove the Dock item.



Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

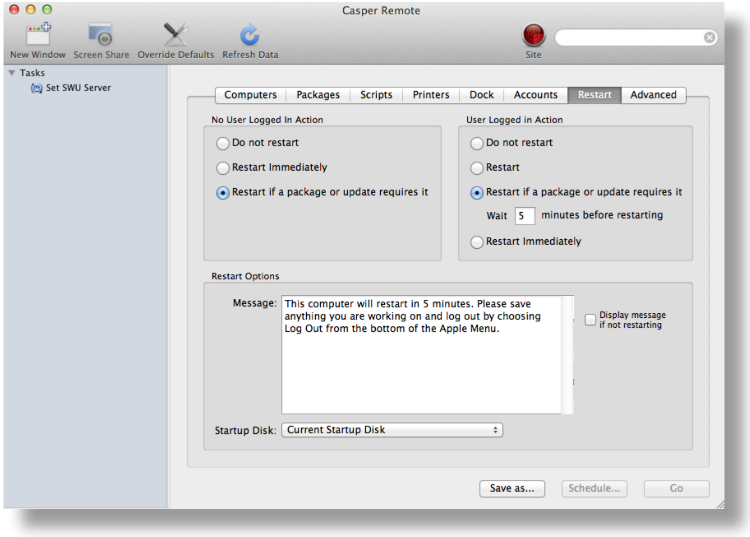
4. Click the **Dock** tab.
5. In the list of Dock items, select the checkbox for the Dock item you want to add or remove.



Name	Path to item	Action
□ Downloads	file://localhost/Users/admin/Downloads/	
□ iTunes	file://localhost/Applications/iTunes.app/	

6. Select the **Add to Beginning of Dock**, **Add to End of Dock**, or **Remove from Dock** option.

7. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

8. Do one of the following:

   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create policies, view the plan and status of a policy, and view and flush policy logs.

Administering Local Accounts

You can perform the following local account administration tasks using a policy or Casper Remote:

- Create a new account.
- Delete an existing account.
- Reset the password for an existing account.
- (Policy only) Disable an existing account for FileVault 2 on computers with OS X v10.9 or later.

When you create a new account, you can do the following:

- Specify the password and password hint.
- Specify a location for the home directory.
- Configure the account picture.
- Give the user administrator privileges to the computer.
- (Policy only) Enable the account for FileVault 2 on computers with OS X v10.9 or later.

When you delete an existing account, you can permanently delete the home directory or specify an archive location.

Requirements

To disable an existing account for FileVault 2, the computer must be running OS X v10.9 or later. To enable a new account for FileVault 2, the computer must be running OS X v10.9 or later and have an individual recovery key.

Administering Local Accounts Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, see General Payload.
6. Select the Local Accounts payload and click **Configure**.
7. Choose an action from the **Action** pop-up menu.
8. Configure the action using the options on the pane.

9. Use the Restart Options payload to configure settings for restarting computers.
   For more information, see Restart Options Payload.

10. Click the **Scope** tab and configure the scope of the policy.
    For more information, see Scope.

11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.
    For more information, see Self Service Policies.

12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.
    For more information, see User Interaction.

13. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

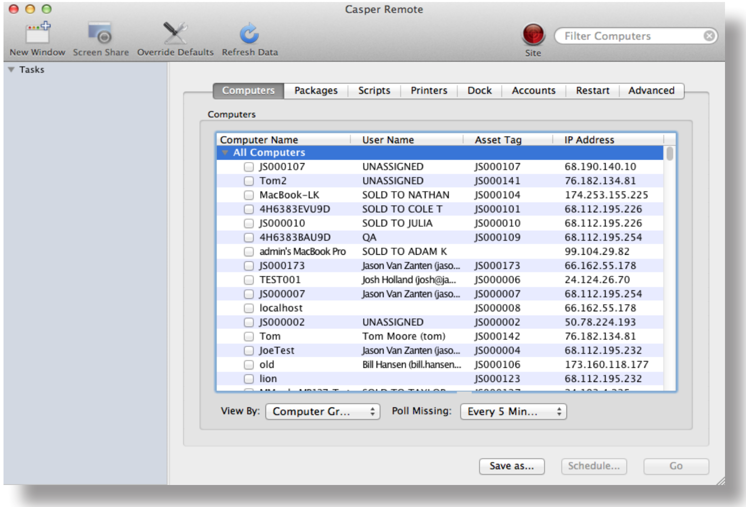
Administering Local Accounts Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** ● and choose a site.
   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to administer local accounts.

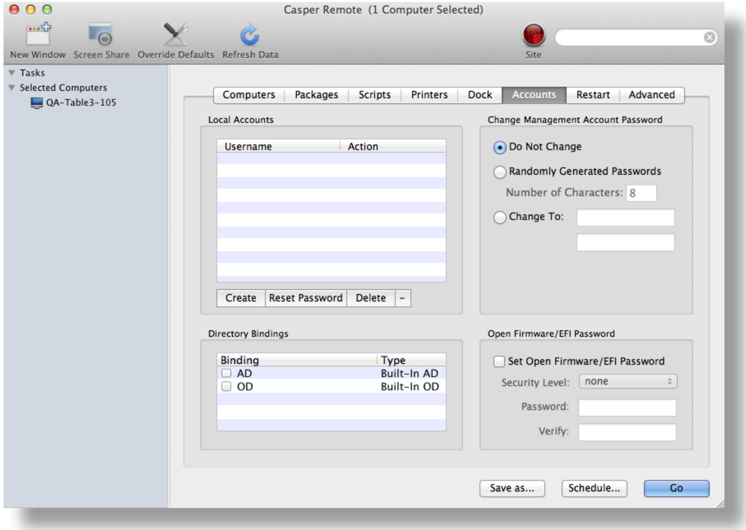


Computer Name	User Name	Asset Tag	IP Address
▼ All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr... Poll Missing: Every 5 Min...

4. Click the **Accounts** tab.

5. Click **Create**, **Reset Password**, or **Delete**.



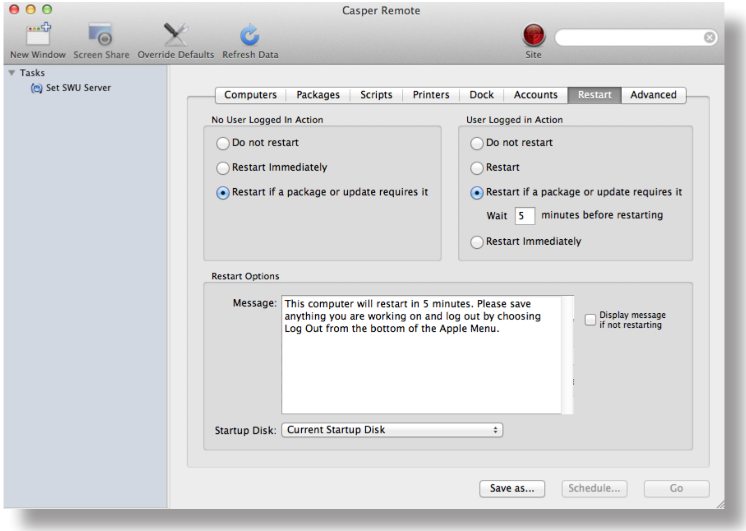
Change Management Account Password:
● Do Not Change
○ Randomly Generated Passwords
Number of Characters: 8
○ Change To:

Binding	Type
□ AD	Built-In AD
□ OD	Built-In OD

□ Set Open Firmware/EFI Password
Security Level: none
Password:
Verify:

6. Configure the action using the options in the window that appears.

7. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action:
○ Do not restart
○ Restart Immediately
● Restart if a package or update requires it

User Logged in Action:
○ Do not restart
○ Restart
● Restart if a package or update requires it
Wait 5 minutes before restarting
○ Restart Immediately

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

8. Do one of the following:

- To immediately perform the tasks on the specified computers, click **Go**.
- To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- Smart Computer Groups

  You can create smart computer groups based on local user accounts.

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

- Administering the Management Account

  Find out how to reset the management account password, and enable or disable the management account for FileVault 2.

Administering the Management Account

You can reset the management account password using a policy or Casper Remote. You can also enable or disable the management account for FileVault 2 on computers with OS X v10.9 or later using a policy.

Resetting the Management Account Password Using a Policy

1. Log in to the JSS with a web browser.
2. Click the **Computers** tab at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Management Account payload and click **Configure**.
7. Choose "Specify new password" or "Randomly generate new passwords" from the **Action** pop-up menu.
8. Configure the action using the options on the pane.
9. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
10. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.
11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.
12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.
13. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

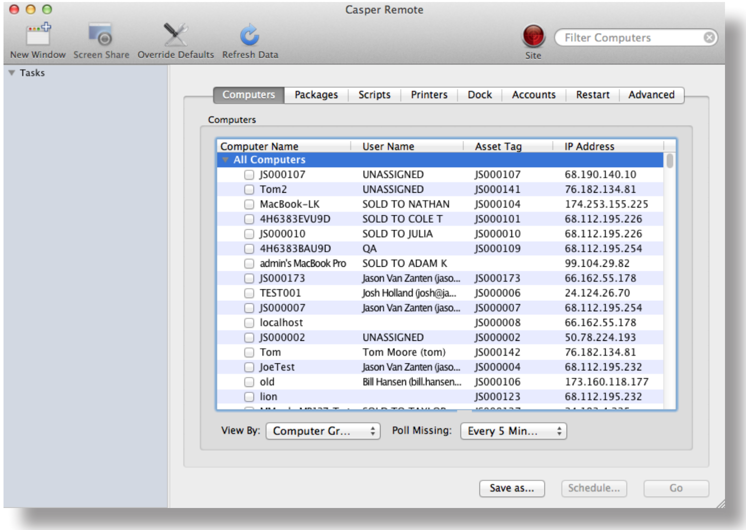
Resetting the Management Account Password Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** ● and select a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to administer local accounts.



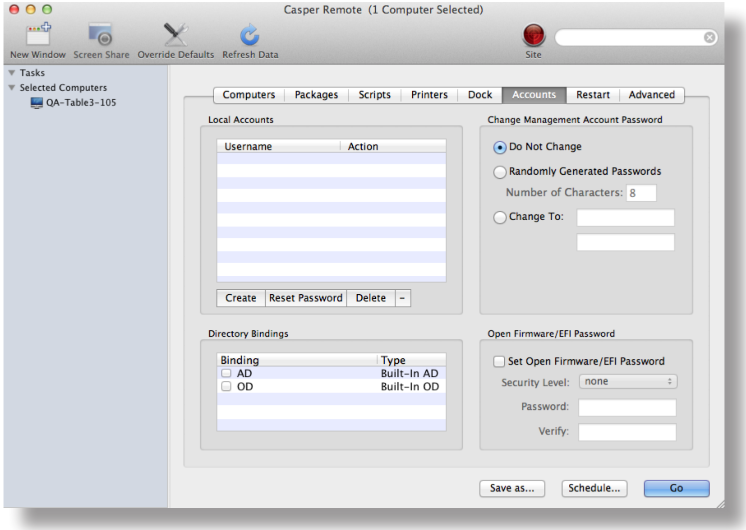
Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr... Poll Missing: Every 5 Min...

4. Click the **Accounts** tab.

5. Do one of the following:

   - To randomly generate new passwords, select **Randomly Generated Passwords** and enter the number of characters required.
   - To specify a new password, select **Change To** and enter the new password.



Change Management Account Password

● Do Not Change

○ Randomly Generated Passwords

Number of Characters: 8

○ Change To:

Directory Bindings

Binding	Type
□ AD	Built-In AD
□ OD	Built-In OD

Open Firmware/EFI Password

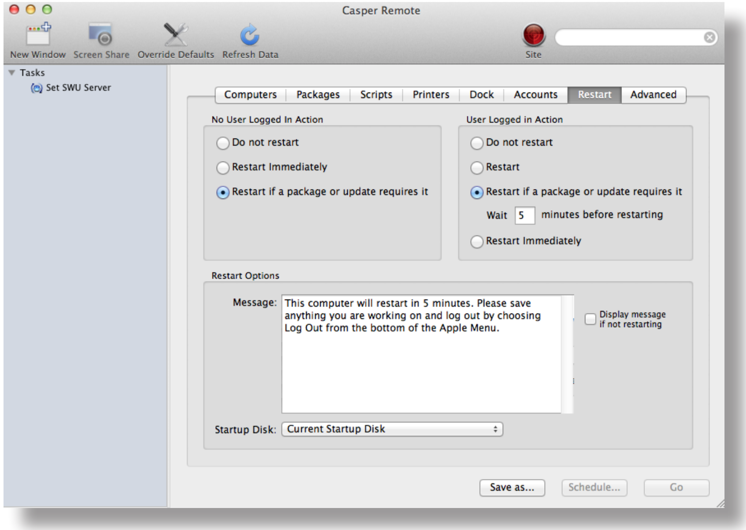
□ Set Open Firmware/EFI Password

Security Level: none

Password:

Verify:

6. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

7. Do one of the following:

   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Enabling or Disabling the Management Account for FileVault 2

You can enable or disable the management account for FileVault 2 on computers with OS X v10.9 or later. To enable the account for FileVault 2, the computer must have an individual recovery key.

1. Log in to the JSS with a web browser.
2. Click the **Computers** tab at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Management Account payload and click **Configure**.
7. Choose "Enable User for FileVault 2" or "Disable User for FileVault 2" from the **Action** pop-up menu.
8. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
9. Click the **Scope** tab and configure the scope of the policy.

   For more information, see Scope.
10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.
11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.
12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.
- Managing Policies

  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

Managing Directory Bindings

Adding a directory binding to the JAMF Software Server (JSS) is the first step to binding computers to a directory service.

You can add the following types of directory bindings to the JSS:

- OS X Directory Utility–Active Directory
- OS X Directory Utility–Open Directory
- PowerBroker Identity Services (formerly called "Likewise")
- ADmitMac
- Centrify

Adding a Directory Binding

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Directory Bindings** .
5. Click **New** + .
6. Choose the type of directory binding you want to add and click **Next**.
7. Configure the directory binding using the tabs and options provided.
   The tabs and options provided match the ones in the third-party directory service software.
8. Click **Save**.

Cloning, Editing, or Deleting a Directory Binding

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Computer Management**.
   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Directory Bindings** .
5. Click the directory binding you want to clone, edit, or delete.

6. Do one of the following:
   - To clone the directory binding, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the directory binding, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the directory binding, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Binding to Directory Services
Find out how to bind computers to a directory service using a policy or Casper Remote.

Binding to Directory Services

You can bind computers to a directory service using a policy or Casper Remote.

Note: You can also bind to directory services during imaging. For more information, see Configurations.

Requirements

To bind computers to a directory service, you need a directory binding in the JSS. (For more information, see Managing Directory Bindings.)

Binding to a Directory Service Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Directory Bindings payload and click **Configure**.
7. Click **Add** for the directory service you want to bind to.
8. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
9. Click the **Scope** tab and configure the scope of the policy.

   For more information, see Scope.
10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.
11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.
12. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

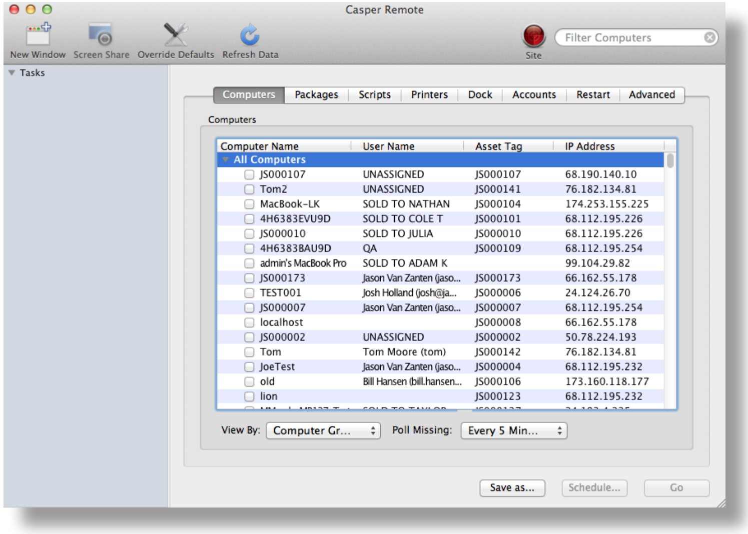
Binding to a Directory Service Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** ● and choose a site.
   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer you want to bind to the directory service.



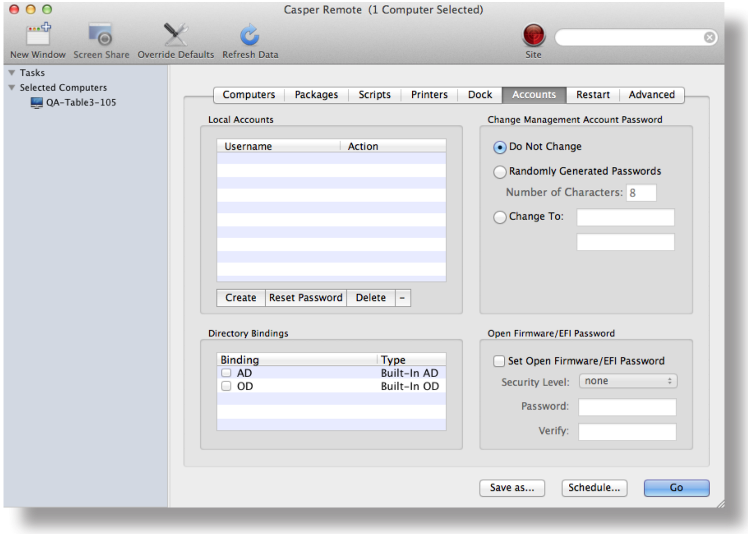
Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...

Poll Missing: Every 5 Min...

4. Click the **Accounts** tab.

5. In the list of directory bindings, select the checkbox for the directory service that you want to bind to.



● Do Not Change

○ Randomly Generated Passwords

Number of Characters: 8

○ Change To:

Binding	Type
□ AD	Built-In AD
□ OD	Built-In OD

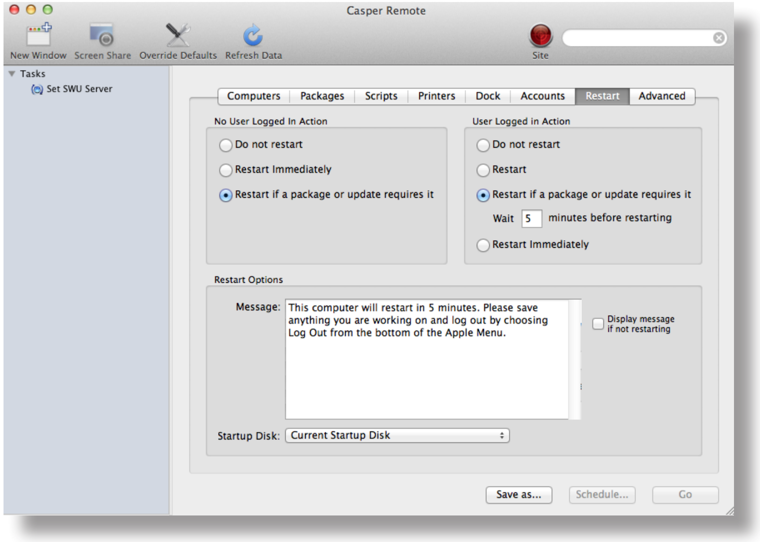
□ Set Open Firmware/EFI Password

Security Level: none

Password:

Verify:

6. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

7. Do one of the following:

- To immediately perform the tasks on the specified computers, click **Go**.
- To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide.

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

Managing Disk Encryption Configurations

Creating a disk encryption configuration in the JAMF Software Server (JSS) is the first step to activating FileVault 2 on computers with OS X v10.8 or later.

When you create a disk encryption configuration, you specify the following information:

- The type of recovery key to use for recovering encrypted data. There are three recovery key options you can choose from:
  - **Individual** (also known as "Personal")—Uses a unique alphanumeric recovery key for each computer. The individual recovery key is generated on the computer and sent back to the JSS for storage when the encryption takes place.
  - **Institutional**—Uses a shared recovery key. This requires you to create the recovery key with Keychain Access and upload it to the JSS for storage.
  - **Individual and Institutional**—Uses both types of recovery keys.
- The user for which to enable FileVault 2
  - **Management Account**—Makes the management account on the computer the enabled FileVault 2 user.
  - **Current or Next User**—Makes the user that is logged in to 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.

> ***Note:*** If you make the management account the enabled FileVault 2 user on computers with OS x v10.9 or later, you will be able to issue a new recovery key to those computers later if necessary. (For more information, see Issuing a New FileVault 2 Recovery Key.)

Requirements

To use either the "Institutional" recovery key or the "Individual and Institutional" recovery key options in the disk encryption configuration, you must first create and export a recovery key using Keychain Access. (For more information, see the Creating and Exporting an Institutional Recovery Key Knowledge Base article.)

Creating a Disk Encryption Configuration

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Disk Encryption Configurations** .

5. Click **New** + .
6. Configure the disk encryption configuration using the fields and options on the pane.
7. Click **Save**.

Cloning, Editing, or Deleting a Disk Encryption Configuration

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Disk Encryption Configurations** .
5. Click the disk encryption configuration you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the configuration, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the configuration, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the configuration, click **Delete**, and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

Deploying Disk Encryption Configurations
Find out how to activate FileVault 2 by deploying a disk encryption configuration using a policy or Casper Remote.

Deploying Disk Encryption Configurations

Deploying disk encryption configurations allows you to activate FileVault 2 on computers with OS X v10.8 or later. There are two ways to deploy a disk encryption configuration: using a policy or using Casper Remote.

The event that activates FileVault 2 depends on the enabled FileVault 2 user specified in the disk encryption configuration. If the enabled user is "Management Account," FileVault 2 is activated on a computer the next time the computer restarts. If the enabled user is "Current or Next User", FileVault 2 is activated on a computer the next time the current user logs out or the computer restarts.

Requirements

To activate FileVault 2 on a computer, the computer must be running OS X v10.8 or later and have a "Recovery HD" partition.

Deploying a Disk Encryption Configuration Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Disk Encryption payload and click **Configure**.
7. Choose the disk encryption configuration you want to deploy from the **Disk Encryption Configuration** pop-up menu.

   > ***Note:*** Options are only displayed in the **Disk Encryption Configuration** pop-up menu if one or more configurations are configured in the JSS. For more information, see Managing Disk Encryption Configurations.
8. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
9. Click the **Scope** tab and configure the scope of the policy.

   For more information, see Scope.
10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

12. Click **Save**.

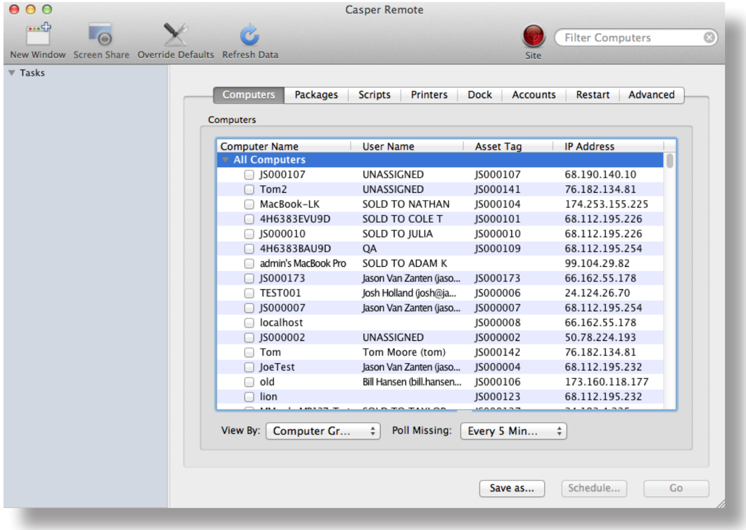
Deploying a Disk Encryption Configuration Using Casper Remote

1. Open Casper Remote and authenticate to the JSS.
2. Click **Site** ● and choose a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer to which you want to deploy the disk encryption configuration.

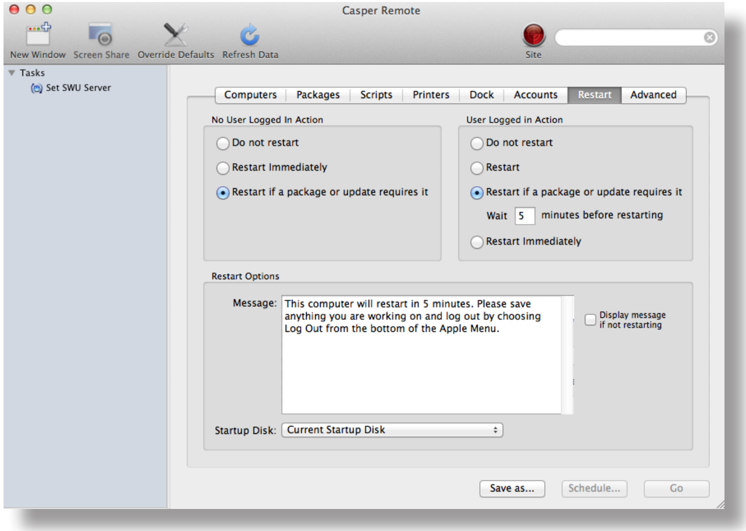


Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...

Poll Missing: Every 5 Min...

4. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

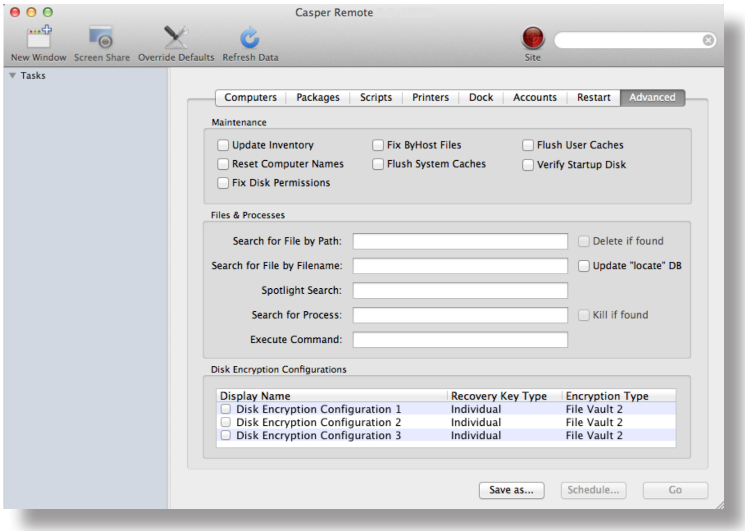
□ Display message if not restarting

Startup Disk: Current Startup Disk

5. Click the **Advanced** tab.

6. In the list of disk encryption configurations, select the checkbox next to the configuration you want to deploy.

> ***Note:*** Disk encryption configurations are only displayed in the list if one or more disk encryption configurations are configured in the JSS. For more information, see Managing Disk Encryption Configurations.



Maintenance

□ Update Inventory
□ Reset Computer Names
□ Fix Disk Permissions
□ Fix ByHost Files
□ Flush System Caches
□ Flush User Caches
□ Verify Startup Disk

Files & Processes

Search for File by Path: □ Delete if found
Search for File by Filename: □ Update "locate" DB
Spotlight Search:
Search for Process: □ Kill if found
Execute Command:

Disk Encryption Configurations

Display Name	Recovery Key Type	Encryption Type
□ Disk Encryption Configuration 1	Individual	File Vault 2
□ Disk Encryption Configuration 2	Individual	File Vault 2
□ Disk Encryption Configuration 3	Individual	File Vault 2

7. Do one of the following:
   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- Viewing the FileVault 2 Recovery Key for a Single Computer
  Find out how to view the FileVault 2 recovery key(s) for a single computer.
- Smart Computer Groups
  You can create smart computer groups based on criteria for FileVault 2.
- About Policies
  Learn the basics about policies.
- Managing Policies
  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

For related information, see the following Knowledge Base article:

Smart Group and Advanced Search Criteria for FileVault 2 and Legacy FileVault
Learn about the smart computer group and advanced computer search criteria available for FileVault 2.

Issuing a New FileVault 2 Recovery Key

You can issue a new FileVault 2 recovery key to computers with OS X v10.9 or later that have FileVault 2 activated. This allows you to do the following:

- Update the recovery key on computers on a regular schedule, without needing to decrypt and then re-encrypt the computers.
- Replace an individual recovery key that has been reported as invalid and does not match the recovery key stored in the JAMF Software Server (JSS).

Note: You can create a smart group to verify the recovery key on computers on a regular basis. For information on FileVault 2 smart group criteria, see the following Knowledge Base article:

Smart Group and Advanced Search Criteria for FileVault 2 and Legacy FileVault

You can issue a new FileVault 2 recovery key to computers using a policy.

Requirements

To issue a new individual recovery key to a computer, the computer must have:

- OS X v10.9 or later
- A "Recovery HD" partition
- FileVault 2 activated
- One of the following two conditions met:
  - The management account configured as the enabled FileVault 2 user
  - An existing, valid individual recovery key that matches the key stored in the JSS

To issue a new institutional recovery key to a computer, the computer must have:

- OS X v10.9 or later
- A "Recovery HD" partition
- FileVault 2 activated
- The management account configured as the enabled FileVault 2 user

Issuing a New FileVault 2 Recovery Key

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

5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.

6. Select the Disk Encryption payload and click **Configure**.

7. Choose "Issue New Recovery Key" from the **Action** pop-up menu.

8. Select the type of recovery key you want to issue:

   - **Individual**—A new individual recovery key is generated on each computer and then submitted to the JSS for storage.
   - **Institutional**—A new institutional recovery key is deployed to computers and stored in the JSS.

     To issue a new institutional recovery key, you must choose the disk encryption configuration that contains the institutional recovery key you want to use.
   - **Individual and Institutional**—Issues both types of recovery keys to computers.

9. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.

10. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.

11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

13. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- Viewing the FileVault 2 Recovery Key for a Single Computer

  Find out how to view the FileVault 2 recovery key(s) for a single computer.
- Smart Computer Groups

  You can create smart computer groups based on criteria for FileVault 2.
- About Policies

  Learn the basics about policies.
- Managing Policies

  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

For related information, see the following Knowledge Base article:

Smart Group and Advanced Search Criteria for FileVault 2 and Legacy FileVault
Learn about the smart computer group and advanced computer search criteria available for FileVault 2.

Administering Open Firmware/EFI Passwords

You can administer Open Firmware or EFI passwords to ensure the security of managed computers.

There are two ways to set and remove an Open Firmware/EFI password: using a policy or using Casper Remote.

Requirements

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 more information, see the Setting EFI Passwords on Mac Computers (Models Late 2010 or Later Knowledge Base article.)

Setting or Removing an Open Firmware/EFI Password Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the EFI Password payload and click **Configure**.
7. Do one of the following:
   - To set an Open Firmware/EFI password, choose "Command" from the pop-up menu and enter and verify the password.
   - To remove an Open Firmware/EFI password, choose "None" from the pop-up menu.
8. Use the Restart Options payload to configure settings for restarting computers.

   For more information, see Restart Options Payload.
9. Click the **Scope** tab and configure the scope of the policy.

   For more information, see Scope.

10. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.

11. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.

12. Click **Save**.

    The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Setting or Removing an Open Firmware/EFI Password Using Casper Remote

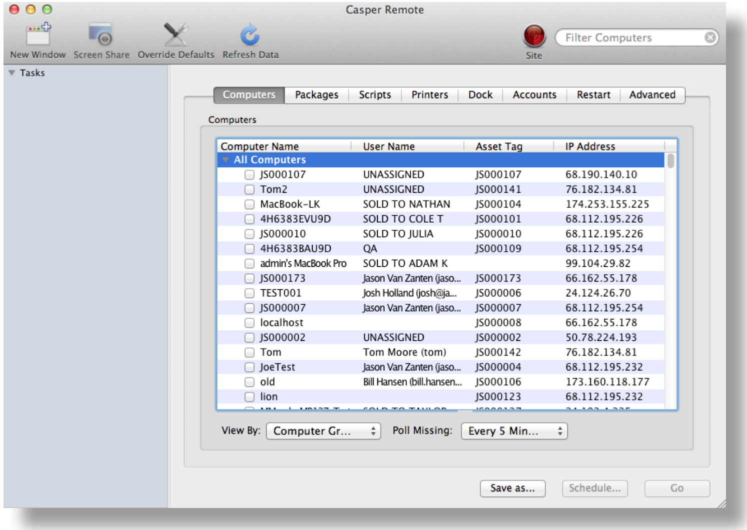
1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** ● and choose a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer on which you want to set or remove an Open Firmware/EFI password.



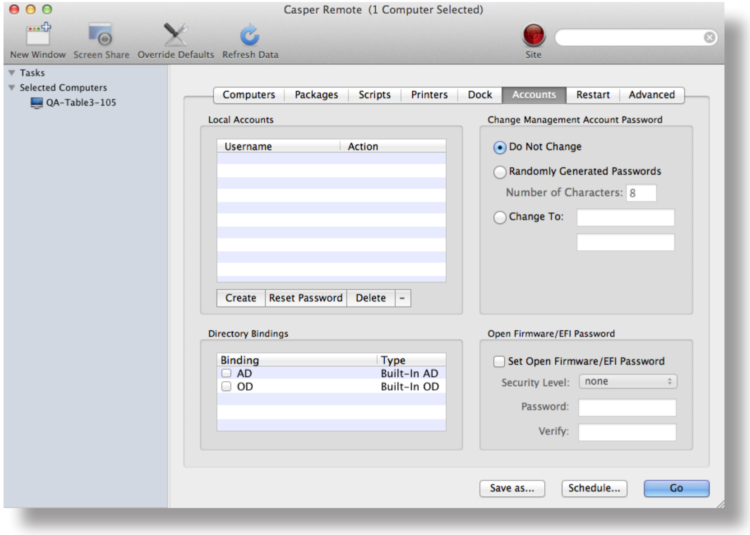
Computers

Computer Name	User Name	Asset Tag	IP Address
All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...   Poll Missing: Every 5 Min...

4. Click the **Accounts** tab.

5. Select the **Set Open Firmware/EFI Password** checkbox.



● Do Not Change

Number of Characters: 8

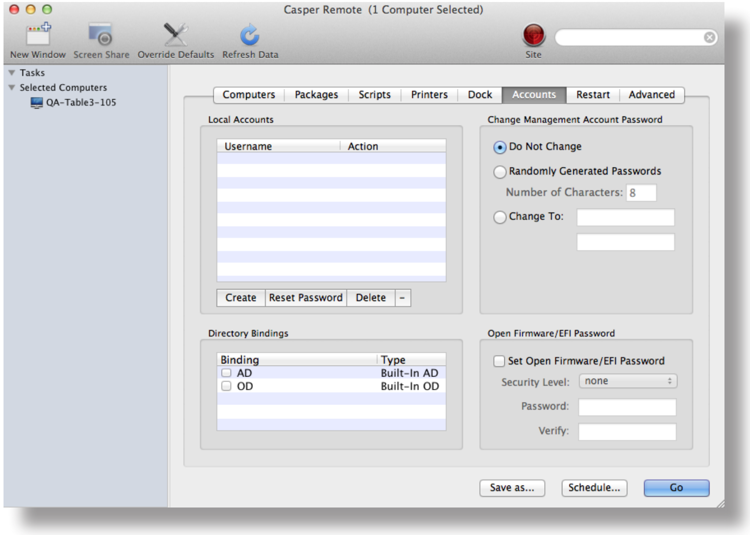
□ Set Open Firmware/EFI Password

Security Level: none

Binding	Type
□ AD	Built-In AD
□ OD	Built-In OD

6. Do one of the following:

- To set the password, choose "command" from the **Security Level** pop-up menu and enter and verify the password.
- To remove the password, choose "none" from the **Security Level** pop-up menu.



● Do Not Change

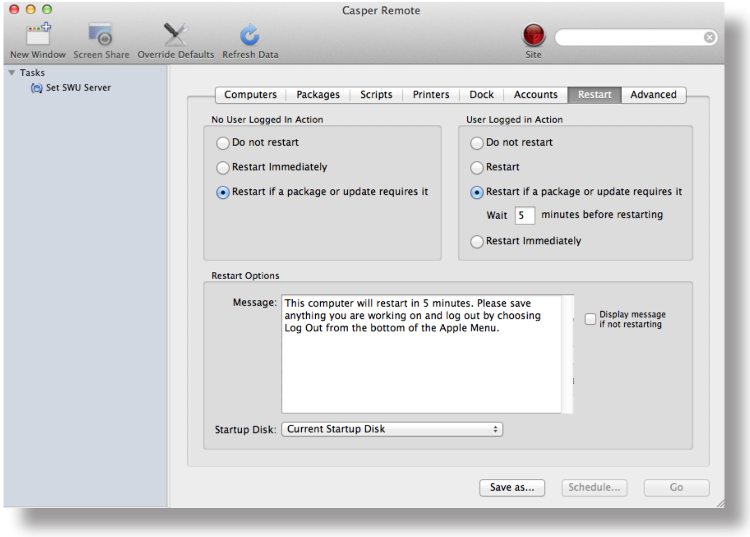
Number of Characters: 8

□ Set Open Firmware/EFI Password

Security Level: none

Binding	Type
□ AD	Built-In AD
□ OD	Built-In OD

7. Click the **Restart** tab and configure settings for restarting computers.



No User Logged In Action

○ Do not restart
○ Restart Immediately
● Restart if a package or update requires it

User Logged in Action

○ Do not restart
○ Restart
● Restart if a package or update requires it
Wait 5 minutes before restarting
○ Restart Immediately

Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

8. Do one of the following:
   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.
- Managing Policies

  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

Imaging

About Imaging

Imaging computers with the Casper Suite involves booting computers to a startup disk other than the target drive and then using the Casper Imaging application to deploy a configuration.

Some common startup disks used for imaging are USB or FireWire drives, Restore partitions, and NetBoot images.

There are four imaging methods:

- **Standard imaging**—Standard imaging allows you to configure the imaging settings for a computer at imaging time.
- **Autorun imaging**—Autorun imaging allows you to store imaging settings in the JAMF Software Server (JSS), so they don't have to be configured at imaging time. In addition, Autorun imaging can be completely automated to run on a schedule.
- **PreStage imaging**—PreStage imaging allows you to store imaging settings in the JSS and use them to image new computers as you add them to the network. This reduces the amount of time and interaction it takes to prepare new computers for use.
- **Target Mode Imaging (TMI)**—TMI allows you to image multiple computers subsequently by connecting them to a host computer using a Firewire or Thunderbolt cable. This can be ideal when using a network connection is not optimal, such as when imaging MacBook Airs that do not have built-in ethernet.

Related Information

For more information, see the following sections in this guide:

- Configurations

  Learn about configurations and find out how to create them.
- Standard Imaging

  Find out how to image computers using standard imaging.
- Autorun Imaging

  Find out how to image computers using Autorun imaging.

- PreStage Imaging

  Find out how to image computers using PreStage imaging.
- Target Mode Imaging

  Find out how to image computers using TMI.

For related information, see the following Knowledge Base article:

Creating a NetBoot Image and Setting Up a NetBoot Server

Configurations

Configurations are modular images that allow you to quickly specify what needs to be installed and configured on computers during imaging. Unlike standard images, you can easily make changes to configurations without rebuilding them.

You can include the following items in a configuration:

- Packages
- Scripts
- Printers
- Directory bindings
- Management account settings
- A homepage
- Partitions

You can manage configurations using Casper Admin or the JSS. When you create, edit, or delete a configuration in Casper Admin, the changes are reflected in the JSS, and vice versa.

Standard and Smart Configurations

There are two types of configurations: standard configurations and smart configurations.

Smart configurations inherit settings from another configuration (called a "parent configuration"). Making changes to the parent configuration automatically updates the smart configuration to reflect the changes. If there are settings in the parent configuration that you want to override, you can customize the packages, scripts, printers, or directory bindings in the smart configuration as needed.

Compiled Configurations

You can compile both standard and smart configurations. Compiling a configuration builds a single DMG, allowing you to block-copy the entire configuration during imaging and speed up the process. You can choose to make the DMG a compressed or uncompressed file.

Configurations can only be compiled using Casper Admin. You can only compile configurations if your master distribution point is a file share distribution point.

Configurations with Partitions

There are three ways to configure a partition in a configuration:

- Image the partition using another configuration
- Install a Winclone image on the partition
- Make the partition a Restore partition

Restore partitions are hidden partitions that have only an OS package and Casper Imaging installed. They allow you to re-image computers without using NetBoot or an external drive.

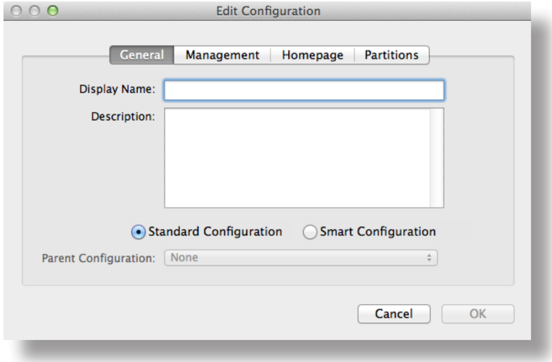
Note: As a safety mechanism, drives that already have visible partitions cannot be re-partitioned using the Casper Suite.

Creating a Configuration Using Casper Admin

Several settings in Casper Admin have tool tips. To read more about a specific setting, hover your mouse over it until a tool tip is displayed.

1. Open Casper Admin and authenticate to the JSS.
2. Click **New Config** .
3. Use the General pane to configure basic settings for the configuration.

   To create a smart configuration, select the **Smart Configuration** option and choose a parent configuration.

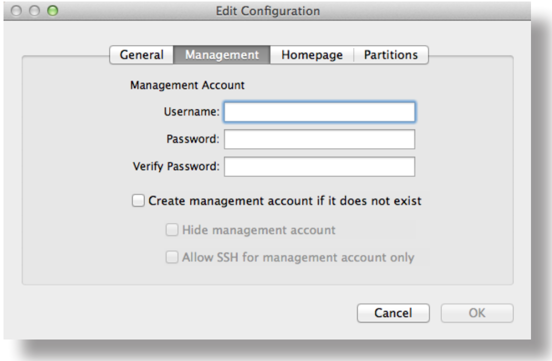


● Standard Configuration ○ Smart Configuration

Parent Configuration: None

4. (Optional) Click the **Management** tab and set or create a management account.

   This ensures that computers imaged with the configuration are managed.

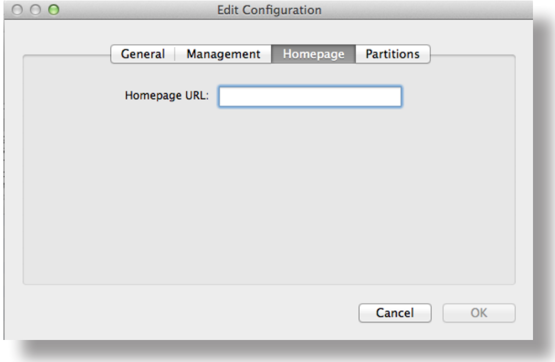


□ Create management account if it does not exist

□ Hide management account

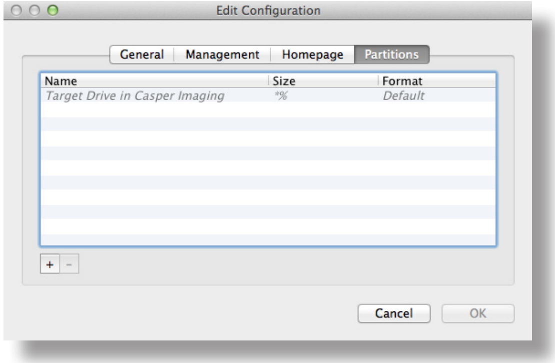
□ Allow SSH for management account only

5. (Optional) Click the **Homepage** tab and enter a homepage URL.



Homepage URL:

6. (Optional) Click the **Partitions** tab and click **Add** (+) to set up a partition.



Name	Size	Format
Target Drive in Casper Imaging	**%*	*Default*

7. Click **OK**.

   The configuration is added to the list of configurations in the sidebar.

8. Add packages, scripts, printers, and directory bindings by dragging them from the main repository to the configuration in the sidebar.

Creating a Configuration Using the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.

4. In the “Computer Management” section, click **Configurations** .
5. Click **New** + .
6. Use the General payload to configure basic settings for the configuration.

   To create a smart configuration, choose "Smart" from the **Type** pop-up menu and choose a parent configuration.

7. Use the Packages, Scripts, Printers, and Directory Bindings payloads to add items to the configuration.

8. (Optional) Use the Management payload to set or create a management account.
   This ensures that computers imaged with the configuration are managed.
9. (Optional) Use the Homepage payload to set the homepage.
10. (Optional) Use the Partitions payload to set up partitions.
11. Click **Save**.

Compiling a Configuration

The time it takes to compile a configuration depends on the amount of data in the configuration. For fastest results, use a wired connection.

You may be prompted to authenticate several times during the compilation process.

Note: If you compile a configuration that includes a package with an architecture type requirement and a substitute package, the package substitution will not work.

1. Open Casper Admin and authenticate to the JSS.
2. In the sidebar, select the configuration and click **Compile**.
3. Choose to create a compressed or an uncompressed DMG.
4. Enter credentials for a local administrator account.
5. Click **OK**.

Editing or Deleting a Configuration Using Casper Admin

Several settings in Casper Admin have tool tips. To read more about a specific setting, hover your mouse over it until a tool tip is displayed.

1. Open Casper Admin and authenticate to the JSS.
2. In the sidebar, select the configuration you want to edit or delete.
3. Do one of the following:
   - To edit the configuration, double-click it and make changes as needed. Then click **OK**.
   - To delete the configuration, click **Delete** 🚫 and then click **Delete** again to confirm.

Cloning, Editing, or Deleting a Configuration Using the JSS

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management" section, click **Configurations** .
5. Click the configuration you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the configuration, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the configuration, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the configuration, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Standard Imaging

  Find out how to image computers using a configuration and standard imaging.
- Autorun Imaging

  Find out how to image computers using a configuration and Autorun imaging.
- PreStage Imaging

  Find out how to image computers using a configuration and PreStage imaging.
- Target Mode Imaging

  Find out how to image computers using a configuration and Target Mode Imaging.

For related information, see the following Knowledge Base article:

Creating Images with Winclone for Deployment with Casper Imaging
Find out how to create a Winclone image that you can install on a partition during imaging.

Booting Computers to NetBoot Images

When you boot computers to a NetBoot image, you can choose which NetBoot server computers should use.

There are two ways to boot computers to a NetBoot image: using a policy or using Casper Remote.

Requirements

To boot computers to a NetBoot image, you need a NetBoot server in the JSS. (For more information, see NetBoot Servers.)

Booting Computers to a NetBoot Image Using a Policy

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.

   For an overview of the settings in the General payload, see General Payload.
6. Select the Restart Options payload.
7. Choose "NetBoot" from the **Startup Disk** pop-up menu.
8. Choose the server that hosts the NetBoot image you want to boot computers to.
9. Configure the rest of the settings for restarting computers.
10. Click the **Scope** tab and configure the scope of the policy.

    For more information, see Scope.
11. (Optional) Click the **Self Service** tab and make the policy available in Self Service.

    For more information, see Self Service Policies.
12. (Optional) Click the **User Interaction** tab and configure messaging and deferral options.

    For more information, see User Interaction.
13. Click **Save**.

The policy runs on computers in the scope the next time they check in with the JSS and meet the criteria in the General payload.

Boot Computers to a NetBoot Image Using Casper Remote

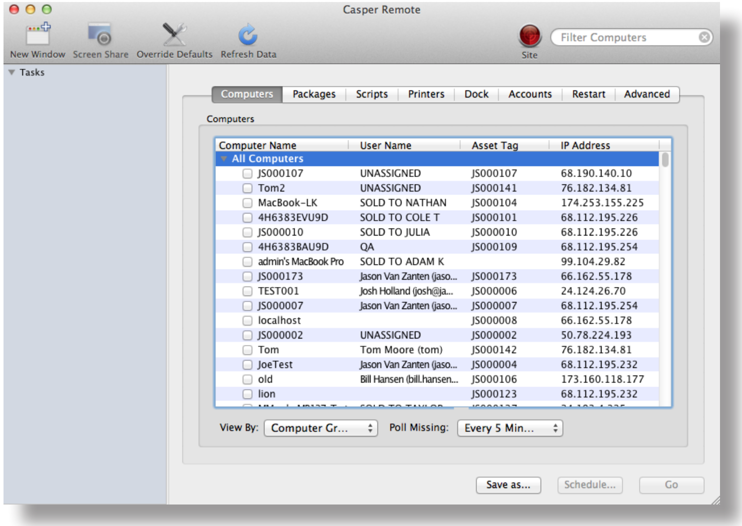
1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** ● and choose a site.

   This determines which items are available in Casper Remote.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

3. In the list of computers, select the checkbox for each computer that you want to boot to the NetBoot image.



Computers

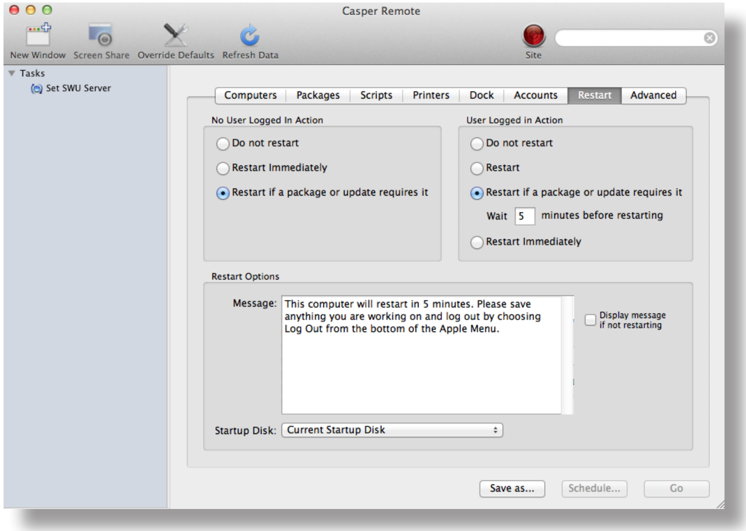
Computer Name	User Name	Asset Tag	IP Address
▾ All Computers			
□ JS000107	UNASSIGNED	JS000107	68.190.140.10
□ Tom2	UNASSIGNED	JS000141	76.182.134.81
□ MacBook-LK	SOLD TO NATHAN	JS000104	174.253.155.225
□ 4H6383EVU9D	SOLD TO COLE T	JS000101	68.112.195.226
□ JS000010	SOLD TO JULIA	JS000010	68.112.195.226
□ 4H6383BAU9D	QA	JS000109	68.112.195.254
□ admin's MacBook Pro	SOLD TO ADAM K		99.104.29.82
□ JS000173	Jason Van Zanten (jaso...	JS000173	66.162.55.178
□ TEST001	Josh Holland (josh@ja...	JS000006	24.124.26.70
□ JS000007	Jason Van Zanten (jaso...	JS000007	68.112.195.254
□ localhost		JS000008	66.162.55.178
□ JS000002	UNASSIGNED	JS000002	50.78.224.193
□ Tom	Tom Moore (tom)	JS000142	76.182.134.81
□ JoeTest	Jason Van Zanten (jaso...	JS000004	68.112.195.232
□ old	Bill Hansen (bill.hansen...	JS000106	173.160.118.177
□ lion		JS000123	68.112.195.232

View By: Computer Gr...

Poll Missing: Every 5 Min...

4. Click the **Restart** tab.

5. Choose "NetBoot" from the **Startup Disk** pop-up menu.



No User Logged In Action

○ Do not restart

○ Restart Immediately

● Restart if a package or update requires it

User Logged in Action

○ Do not restart

○ Restart

● Restart if a package or update requires it

Wait 5 minutes before restarting

○ Restart Immediately

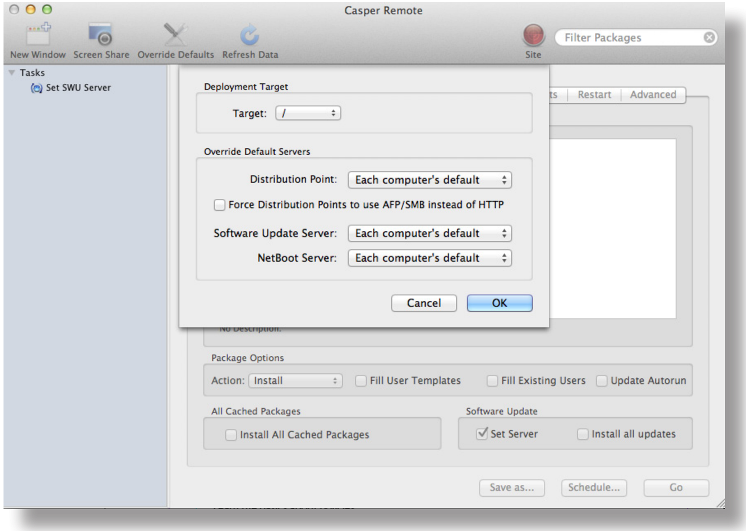
Restart Options

Message: This computer will restart in 5 minutes. Please save anything you are working on and log out by choosing Log Out from the bottom of the Apple Menu.

□ Display message if not restarting

Startup Disk: Current Startup Disk

6. If you want to change the NetBoot server that computers use, click **Override Defaults** and choose a NetBoot server.



Deployment Target

Target: /

Override Default Servers

Distribution Point: Each computer's default

☐ Force Distribution Points to use AFP/SMB instead of HTTP

Software Update Server: Each computer's default

NetBoot Server: Each computer's default

Package Options

Action: Install ☐ Fill User Templates ☐ Fill Existing Users ☐ Update Autorun

All Cached Packages

☐ Install All Cached Packages

Software Update

☑ Set Server ☐ Install all updates

7. Configure the rest of the settings for restarting computers.

8. Do one of the following:

   - To immediately perform the tasks on the specified computers, click **Go**.
   - To schedule the tasks to take place at a specific day and time, click **Schedule** and choose a day and time. Then click **Schedule** again.

Related Information

For related information, see the following sections in this guide:

- About Policies

  Learn the basics about policies.

- Managing Policies

  Find out how to create a policy, view the plan and status of a policy, and view and flush policy logs.

Standard Imaging

Standard imaging allows you to configure the imaging settings for a computer at imaging time. These settings include:

- The target drive
- The configuration to image with
- The distribution point to download files from

Requirements

To use standard imaging, you need:

- A configuration (For more information, see Configurations.)
- A distribution point (For more information, see About Distribution Points.)

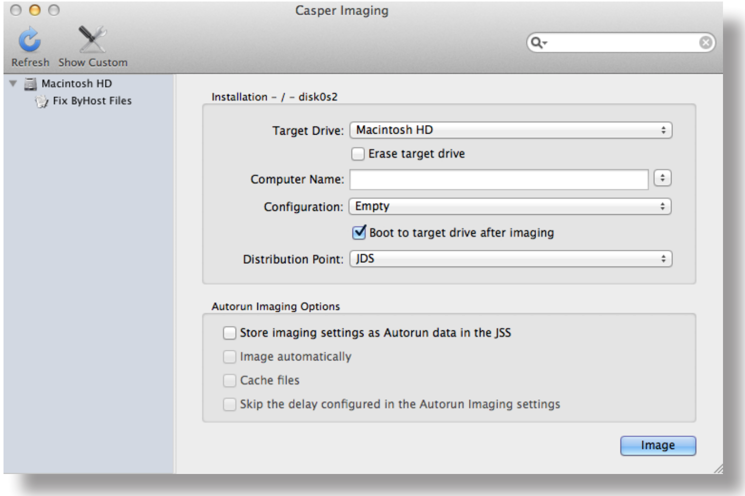
  Alternatively, you can use an external drive that is prepared for offline imaging. For more information, see the Offline Imaging Knowledge Base article.
- A startup disk other than the target drive that has Casper Imaging installed (For more information, see About Imaging.)

Using Standard Imaging

1. On the target computer, boot to a startup disk other than the target drive.
2. Open Casper Imaging and authenticate locally.
3. Authenticate to the JSS when prompted.
4. To add the computer to a site, click **Site** ● and choose a site.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

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



Installation – / – disk0s2

Target Drive: Macintosh HD

☐ Erase target drive

Computer Name:

Configuration: Empty

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

☐ Store imaging settings as Autorun data in the JSS

☐ Image automatically

☐ Cache files

☐ Skip the delay configured in the Autorun Imaging settings

6. To erase the target drive when the imaging process begins, select the **Erase target drive** checkbox.

7. Assign a name to the computer by entering a name in the **Computer Name** field.

   Alternatively, use the arrows to choose "Computer Name," MAC Address," or "Serial Number". The value for the option you choose populates in the field.

8. Choose a configuration from the **Configuration** pop-up menu.

9. To boot the computer to the target drive after imaging, select the **Boot to target drive after imaging** checkbox.

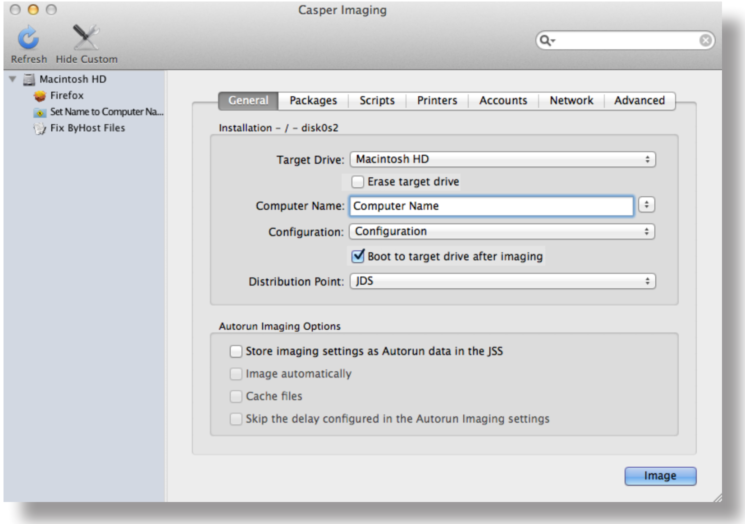
10. Choose a distribution point from the **Distribution Point** pop-up menu.

11. (Optional) Use the options in the Autorun Imaging Options group box to configure Autorun imaging options for the computer.

    For more information on Autorun imaging, see Autorun Imaging.

12. (Optional) Click **Show Custom** and use the tabs and options to customize the imaging process.

    For an overview of each pane, see Customizing the Imaging Process.



Installation – / – disk0s2

Target Drive: Macintosh HD

☐ Erase target drive

Computer Name: Computer Name

Configuration: Configuration

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

☐ Store imaging settings as Autorun data in the JSS

☐ Image automatically

☐ Cache files

☐ Skip the delay configured in the Autorun Imaging settings

13. Click **Image**.

Related Information

For related information, see the following section in this guide:

Viewing Casper Imaging Logs for a Single Computer
Find out how to view Casper Imaging logs for a single computer.

PreStage Imaging

PreStage imaging allows you to store imaging settings in the JAMF Software Server (JSS) and use them to image new computers as you add them to the network. This reduces the amount of time and interaction it takes to prepare new computers for use. PreStage imaging also enrolls computers with the JSS.

To use PreStage imaging, you need to create a PreStage in the JSS and then run Casper Imaging on target computers to image them. Creating a PreStage allows you to configure the imaging settings and specify the computers that should be imaged with the PreStage (called "scope"). When you open Casper Imaging on a computer in the scope, Casper Imaging is populated with the settings in the PreStage.

You can configure a PreStage to start the imaging process automatically the first time Casper Imaging is opened on a computer. Otherwise, you need to start the imaging process manually by clicking the **Image** button in Casper Imaging.

You can also bypass PreStage imaging to prevent Casper Imaging from being populated with the settings in the PreStage.

Requirements

To create a PreStage, you need:

- A configuration (For more information, see Configurations.)
- A distribution point (For more information, see About Distribution Points.)

To image a computer using a PreStage, you need a startup disk other than the target drive that has Casper Imaging installed. (For more information, see About Imaging.)

Creating a PreStage

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **PreStage Imaging**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the PreStage, including the activation and expiration date/time.

   To start the imaging process automatically when Casper Imaging is opened on a computer in the scope, select the **Image Automatically** checkbox.
6. Select the Computer Names payload and choose a method for assigning names to computers.

   Computer names are assigned as computers in the scope are imaged.

7. (Optional) Use the Purchasing Information payload to specify purchasing information for computers.

   This information is stored in the JSS for each computer imaged using the PreStage.

8. (Optional) Use the Attachments payload to upload attachments to store for computers.

   Attachments are stored in the JSS for each computer imaged using the PreStage.

9. Select the Install payload and configure the basic imaging settings, including the target drive, the configuration to image with, and the distribution point to download files from.

10. Enter credentials for a local account to bypass the prompt when Casper Imaging is opened on the computer.

11. To store the imaging settings as Autorun data for each computer, select the **Store PreStage settings as Autorun data** checkbox. Then configure additional options for Autorun imaging as needed.

    For more information on Autorun imaging, see Autorun Imaging.

12. (Optional) Use the rest of the payloads to customize the imaging process.

    For an overview of each payload, see Customizing the Imaging Process.

13. Click the **Scope** tab and configure the scope of the PreStage.

14. Click **Save**.

Cloning, Editing, or Deleting a PreStage

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

2. Click **Computers** at the top of the page.

3. Click **PreStage Imaging**.

   On a smartphone, this option is in the pop-up menu.

4. Click the PreStage you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the PreStage, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the PreStage, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the PreStage, click **Delete** and then click **Delete** again to confirm.

Imaging a Computer Using a PreStage

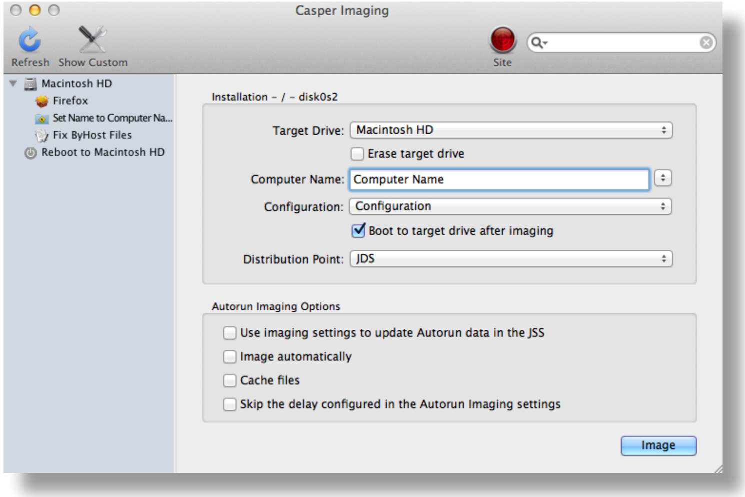
If you configured the PreStage to start the imaging process automatically, simply boot the target computer to a startup disk other than the target drive and open Casper Imaging.

If you did not configure the PreStage to start the imaging process automatically, complete the following instructions:

1. On a computer that is in the scope of the PreStage, boot to a startup disk other than the target drive and open Casper Imaging.

2. If prompted, authenticate locally.

3. (Optional) Make changes to the basic imaging settings as needed, including the target drive, the configuration to image with, and the distribution point to download files from.



- Macintosh HD
  - Firefox
  - Set Name to Computer Na...
  - Fix ByHost Files
- Reboot to Macintosh HD

Installation – / – disk0s2

Target Drive: Macintosh HD

□ Erase target drive

Computer Name: Computer Name

Configuration: Configuration

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

□ Use imaging settings to update Autorun data in the JSS

□ Image automatically

□ Cache files

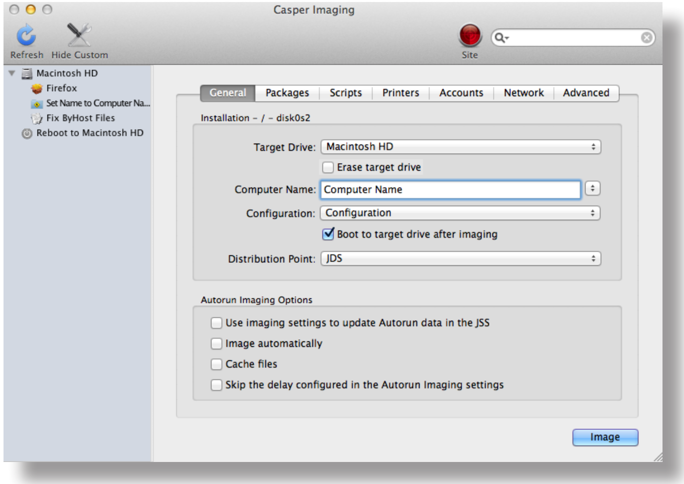
□ Skip the delay configured in the Autorun Imaging settings

4. (Optional) Use the options in the Autorun Imaging Options group box to configure Autorun imaging options for the computer.

   For more information on Autorun imaging, see Autorun Imaging.

5. (Optional) Click **Show Custom** and use the tabs and options to customize the imaging process.

   For an overview of each pane, see Customizing the Imaging Process.



- Macintosh HD
  - Firefox
  - Set Name to Computer Na...
  - Fix ByHost Files
- Reboot to Macintosh HD

Installation – / – disk0s2

Target Drive: Macintosh HD

□ Erase target drive

Computer Name: Computer Name

Configuration: Configuration

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

□ Use imaging settings to update Autorun data in the JSS

□ Image automatically

□ Cache files

□ Skip the delay configured in the Autorun Imaging settings

6. Click **Image**.

Bypassing PreStage Imaging

To bypass PreStage imaging, hold down the Shift key when opening Casper Imaging.

Viewing PreStage Logs

Each PreStage log includes a list of computers that were imaged using the PreStage and a list of the following information for each computer:

- The date/time that the computer was imaged
- The status of the imaging event
- The actions that took place during the imaging event

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **PreStage Imaging**.

   On a smartphone, this option is in the pop-up menu.
4. Click the PreStage you want to view logs for.
5. Click **Logs**.

   A list of computers imaged using the PreStage is displayed.
6. To view the list of actions that were performed when a computer was imaged, click **Show** for the computer.

Autorun Imaging Settings

The Autorun imaging settings in the JAMF Software Server (JSS) allow you to configure the following settings for Autorun imaging:

- The delay before the imaging process starts automatically

  This only applies if a computer's Autorun data is configured to start the imaging process automatically. During the delay, a pane is displayed that allows you to cancel the imaging process.

- The amount of space to leave available when caching files
- The attribute to use for comparing cached files to files on a distribution point

  This ensures that the most up-to-date files are cached on the computer.

Configuring the Autorun Imaging Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.

4. In the "Computer Management–Management Framework" section, click **Autorun Imaging** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Related Information

For related information, see the following section in this guide:

Autorun Imaging
Find out how to image computers using Autorun imaging.

Autorun Imaging

Autorun imaging allows you to store imaging settings in the JAMF Software Server (JSS) so you don't have to configure them at imaging time. It also allows you to fully automate the imaging process. (For more information, see the Automating the Imaging Process Knowledge Base article.)

To use Autorun imaging, you need to create Autorun data for each target computer and then run Casper Imaging on the computers to image them. Creating Autorun data allows you to configure and store the imaging settings you want to use to image each computer. When you open Casper Imaging on a target computer, Casper Imaging is populated with the Autorun data.

You can configure Autorun data to start the imaging process automatically each time Casper Imaging is opened on a computer. Otherwise, you need to start the imaging process manually by clicking the **Image** button in Casper Imaging.

You can also bypass Autorun imaging to prevent Casper Imaging from being populated with the Autorun data.

There are three ways to create Autorun data for a computer:

- Create the Autorun data using the JSS
- Store Autorun data using Casper Imaging
- Store Autorun data using a PreStage (For more information, see PreStage Imaging.)

Requirements

To create and manage Autorun data using the JSS, you need:

- A configuration (For more information, see Configurations.)
- A distribution point (For more information, see About Distribution Points.)

To store Autorun data using Casper Imaging, you need:

- A configuration (For more information, see Configurations.)
- A distribution point (For more information, see About Distribution Points.)

  Alternatively, you can use an external drive that is configured for offline imaging. (For more information, see the Offline Imaging Knowledge Base article.)
- A startup disk other than the target drive that has Casper Imaging installed (For more information, see About Imaging.)

To image a computer using Autorun data, you need a startup disk other than the target drive that has Casper Imaging installed. (For more information, see About Imaging.)

Creating Autorun Data Using the JSS

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.

   On a smartphone, this option is in the pop-up menu.
4. Perform a simple or advanced computer search.

   For instructions, see Simple Computer Searches or Advanced Computer Searches.
5. Click the computer you want to create Autorun data for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item name to view the computers related to that item.
6. Click **Autorun Data**.
7. Use the Install payload to configure basic imaging settings for the computer, including the target drive, the configuration to image with, and the distribution point to download files from.
8. Enter credentials for a local account to bypass the prompt when Casper Imaging is opened on the computer.

   This is required if you plan to fully automate the imaging process.
9. To cache a copy of each file used for imaging, select the **Cache Files** checkbox.
10. To skip the delay that occurs before the imaging process starts automatically, select the **Skip the delay that occurs before imaging automatically** checkbox.

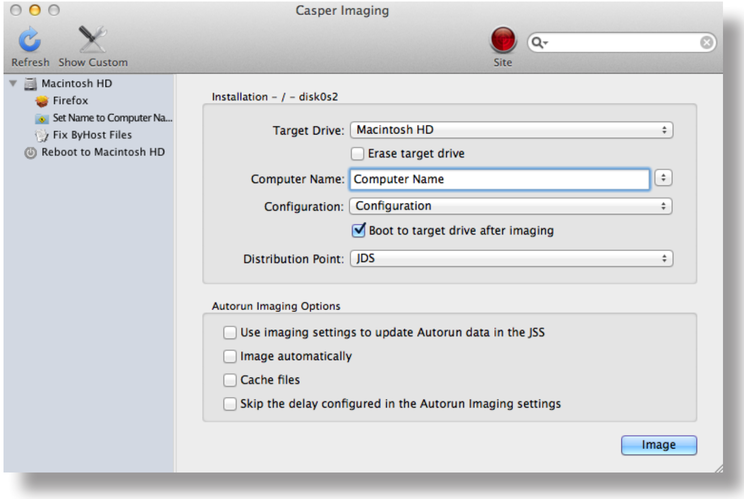
    You can change this delay by using the Autorun Imaging settings. For more information, see Autorun Imaging Settings.
11. (Optional) Use the rest of the payloads to customize the imaging process.

    For an overview of each payload, see Customizing the Imaging Process.
12. Click **Save**.

Storing or Editing Autorun Data Using Casper Imaging

1. On the target computer, boot to a startup disk other than the target drive and open Casper Imaging.
2. If prompted, authenticate locally.

3. (Optional) Configure or make changes to the basic imaging settings as needed, including the target drive, the configuration to image with, and the distribution point to download files from.



- Macintosh HD
  - Firefox
  - Set Name to Computer Na...
  - Fix ByHost Files
- Reboot to Macintosh HD

Installation – / – disk0s2

Target Drive: Macintosh HD

□ Erase target drive

Computer Name: Computer Name

Configuration: Configuration

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

□ Use imaging settings to update Autorun data in the JSS

□ Image automatically

□ Cache files

□ Skip the delay configured in the Autorun Imaging settings

4. In the Autorun Imaging Options group box, select the **Store imaging settings as Autorun data** checkbox.

5. To start the imaging process automatically each time Casper Imaging is opened on the computer, select the **Image Automatically** checkbox.

6. To cache a copy of each file used for imaging, select the **Cache Files** checkbox.

7. To skip the delay that occurs before the imaging process starts automatically, select the **Skip the delay that occurs before imaging automatically** checkbox.

   You can change this delay by using the Autorun Imaging settings in the JSS. For more information, see Autorun Imaging Settings.

8. (Optional) Click **Show Custom** and use the tabs and options to customize the imaging process.

   For an overview of each pane, see Customizing the Imaging Process.

9. Click **Image**.

   The Autorun data is stored in the JSS when the imaging process is complete.

Editing or Deleting Autorun Data Using the JSS

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

2. Click **Computers** at the top of the page.

3. Click **Search Inventory**.

   On a smartphone, this option is in the pop-up menu.

4. Perform a simple or advanced computer search.

   For instructions, see Simple Computer Searches or Advanced Computer Searches.

5. Click the computer you want to edit or delete Autorun data for.

   If you performed a simple search for an item other than computers, you must click **Expand** next to an item name to view the computers related to that item.

6. Click **Autorun Data**.

7. Do one of the following:
   - To edit the Autorun data, make changes as needed. Then click **Save**.
   - To delete the Autorun data, click **Delete** and then click **Delete** again to confirm.

Imaging a Computer Using Autorun Imaging

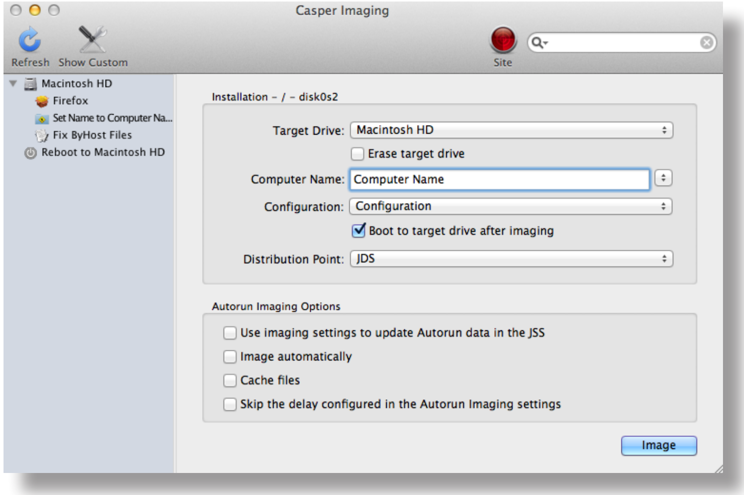
If you configured the Autorun data to start the imaging process automatically, simply boot the target computer to a startup disk other than the target drive and open Casper Imaging. The imaging process begins after the specified delay.

If you did not configure the Autorun data to start the imaging process automatically, complete the following instructions:

1. On the target computer, boot to a startup disk other than the target drive and open Casper Imaging.

2. If prompted, authenticate locally.

3. (Optional) Make changes to the basic imaging settings as needed, including the target drive, the configuration to image with, and the distribution point to download files from.



Installation – / – disk0s2

Target Drive: Macintosh HD

□ Erase target drive

Computer Name: Computer Name

Configuration: Configuration

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

□ Use imaging settings to update Autorun data in the JSS

□ Image automatically

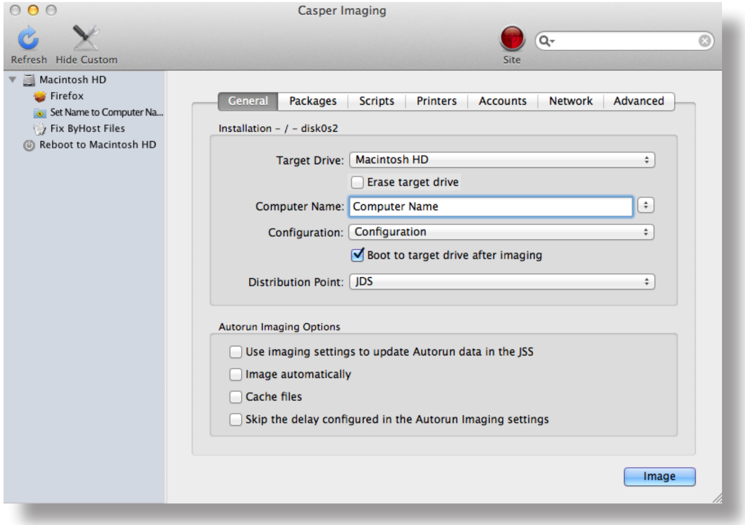
□ Cache files

□ Skip the delay configured in the Autorun Imaging settings

4. (Optional) Use the options in the Autorun Imaging Options group box to change Autorun imaging options for the computer.

5. (Optional) Click **Show Custom** and use the tabs and options to customize the imaging process.

   For an overview of each pane, see Customizing the Imaging Process.



Installation – / – disk0s2

Target Drive: Macintosh HD

□ Erase target drive

Computer Name: Computer Name

Configuration: Configuration

☑ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

□ Use imaging settings to update Autorun data in the JSS

□ Image automatically

□ Cache files

□ Skip the delay configured in the Autorun Imaging settings

6. Click **Image**.

Bypassing Autorun Imaging

To bypass Autorun imaging when imaging a computer, hold down the Shift key when you open Casper Imaging.

Viewing Autorun Logs

The Autorun logs for each computer allow you to view the following information for each imaging event:

- The date/time that the computer was imaged
- The status of the imaging event
- The actions that took place during the imaging event

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search Inventory**.

   On a smartphone, this option is in the pop-up menu.
4. Perform a simple or advanced computer search.

   For instructions, see Simple Computer Searches or Advanced Computer Searches.
5. Click the computer you want to view Autorun logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** next to an item name to view the computers related to that item.

6. Click **Autorun Data**.

7. Click **Logs**.
   A list of imaging events is displayed.

8. To view the actions that took place during an imaging event, click **Show** for the event.

Related Information

For related information, see the following sections in this guide:

- Autorun Imaging Settings
  Find out to configure the settings for Autorun imaging.
- Installing Packages
  Find out how to add packages to a computer's Autorun data when installing packages.
- Caching Packages
  Find out how to add packages to a computer's Autorun data when caching packages.
- Installing Cached Packages
  Find out how to add packages to a computer's Autorun data when installing a cached package.
- Performing Mass Actions for Computers
  Find out how to mass edit or delete Autorun data for computers.

Target Mode Imaging

Target Mode Imaging (TMI) allows you to image multiple computers subsequently by connecting them to a host computer using a Firewire or Thunderbolt cable. This can be ideal when using a network connection is not optimal, such as when imaging MacBook Airs that do not have built-in ethernet.

To use TMI, you run Casper Imaging on a host computer instead of a NetBoot image or an external drive. Then you boot target computers to target disk mode and connect them to the host computer.

Requirements

To use TMI, you need:

- Target computers that support target disk mode
- A host computer with Casper Imaging installed and a FireWire or Thunderbolt port
- A configuration (For more information, see Configurations.)
- A distribution point (For more information, see About Distribution Points.)

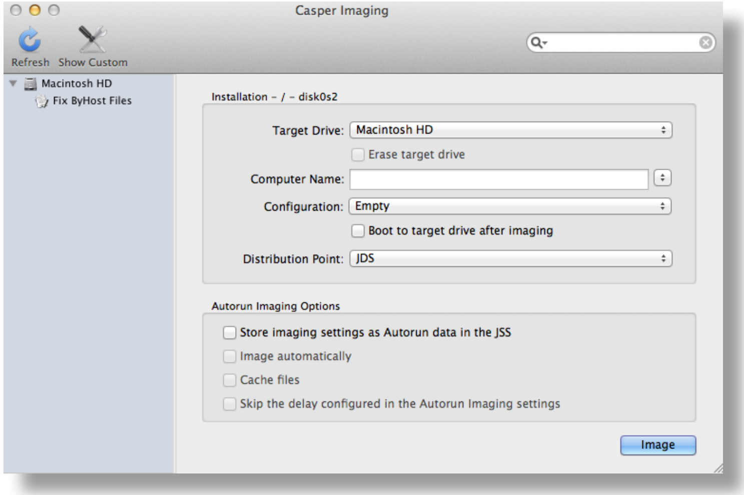
  Alternatively, you can use an external drive that is prepared for offline imaging. For more information, see the Offline Imaging Knowledge Base article.

Using TMI

1. On the host computer, open Casper Imaging and authenticate locally.
2. Authenticate to the JSS when prompted.
3. To add the computer to a site, click **Site** and choose a site.

> ***Note:*** This button is only displayed if you have a site configured in the JSS and are logged in with a JSS user account that has full access or access to multiple sites.

4. Choose "Target Mode Imaging" from the **Target Drive** pop-up menu.



Installation – / – disk0s2

Target Drive: Macintosh HD

□ Erase target drive

Computer Name:

Configuration: Empty

□ Boot to target drive after imaging

Distribution Point: JDS

Autorun Imaging Options

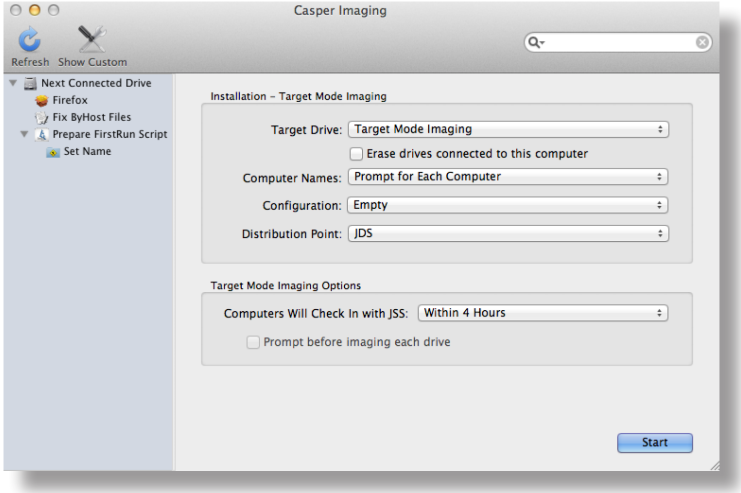
□ Store imaging settings as Autorun data in the JSS

□ Image automatically

□ Cache files

□ Skip the delay configured in the Autorun Imaging settings

5. To erase each target drive before it is imaged, select the **Erase drives connected to this computer** checkbox.



Installation – Target Mode Imaging

Target Drive: Target Mode Imaging

□ Erase drives connected to this computer

Computer Names: Prompt for Each Computer

Configuration: Empty

Distribution Point: JDS

Target Mode Imaging Options

Computers Will Check In with JSS: Within 4 Hours

□ Prompt before imaging each drive

6. From the **Computer Names** pop-up menu, choose how to assign names to target computers:
   - To be prompted to manually enter a name for each computer, choose "Prompt for Each Computer".
   - To automatically generate names in numerical order, choose "Use Numerical Order". Then enter a starting number, and a prefix and suffix as needed, and click **OK**.
   - To use each computer's MAC Address as the name, choose "Use MAC Address". Then enter a prefix and suffix for the MAC Address as needed and click **OK**.
   - To use each computer's serial number as the name, choose "Use Serial Number". Then enter a prefix and suffix for the serial number as needed and click **OK**.
   - To assign names based on the contents of a CSV file, choose "Upload CSV File" and upload the file.

     For more information on using a CSV file to assign computer names, see the Creating a CSV File to Assign Computer Names During Target Mode Imaging Knowledge Base article.

7. Choose a configuration from the **Configuration** pop-up menu.

8. Choose a distribution point from the **Distribution Point** pop-up menu.

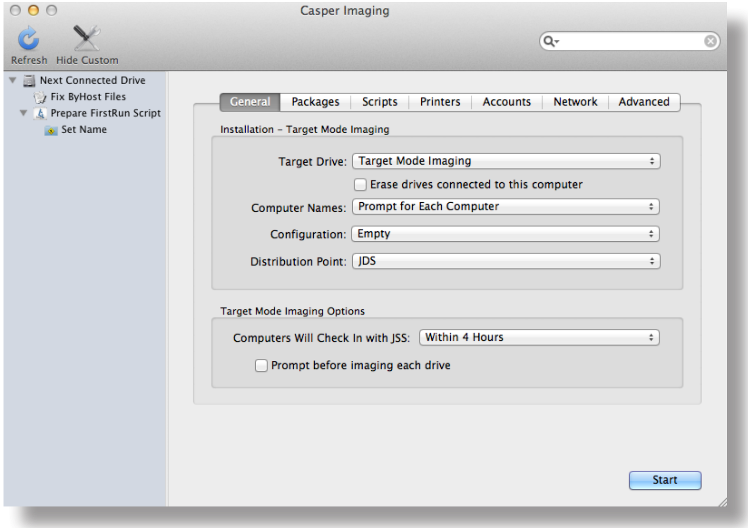
9. From **Computers Will Check In with JSS** pop-up menu, choose the approximate amount of time until computers will check in with the JSS.

> ***Important:*** Computers that do not check in within the specified amount of time will not be enrolled with the JSS.

10. To bypass the prompt displayed before imaging each computer, deselect the **Prompt before imaging each drive** checkbox.

11. (Optional) Click **Show Custom** and use the tabs and options to customize the imaging process.

    For an overview of each pane, see Customizing the Imaging Process.



Installation – Target Mode Imaging

Target Drive: Target Mode Imaging

□ Erase drives connected to this computer

Computer Names: Prompt for Each Computer

Configuration: Empty

Distribution Point: JDS

Target Mode Imaging Options

Computers Will Check In with JSS: Within 4 Hours

□ Prompt before imaging each drive

12. Click **Start**.

13. Boot a target computer to target disk mode.

    To do this, turn on the computer and immediately press and hold down the T key.

14. Use a FireWire or Thunderbolt cable to connect the target computer to the host computer, and then click **OK** if prompted.

    The imaging process starts immediately.

15. When the imaging process is complete, disconnect the target computer.

16. Repeat steps 13–15 for each target computer.

Related Information

For related information, see the following section in this guide:

Viewing Casper Imaging Logs for a Single Computer
Find out how to view Casper Imaging logs for a single computer.

Customizing the Imaging Process

Although configurations let you specify most of the items you want to install and configure during imaging, you can further customize the imaging process by using Casper Imaging or using the JSS to configure a PreStage or Autorun data.

The items that you can add when customizing the imaging process are:

- Packages
- Scripts
- Printers
- Local accounts
- Directory bindings
- Open Firmware/ EFI password
- Network settings
- Values for Apple Remote Desktop Info fields
- Post-imaging options, such as maintenance tasks and showing the OS X Setup Assistant after restart

When using Casper Imaging to customize the imaging process, you can also remove items that are in the selected configuration or items configured with a PreStage or Autorun data for the computer.

The interface you use to customize the imaging process depends on whether you are using Casper Imaging or the JSS. This section provides an overview of each pane displayed in Casper Imaging, but the information also applies to the payload-based interface in the JSS.

Packages

This pane allows you to specify which packages you want to install as part of the imaging process. To add or remove a package, select or deselect the checkbox for the package.

Note: In Casper Imaging, packages that do not exist on the selected distribution point are displayed in red.

Scripts

This pane allows you to specify which scripts you want to run as part of the imaging process.

To add or remove a script from the imaging process using Casper Imaging, select or deselect the checkbox for the script. Then specify parameter values as needed and choose a priority.

To add a script to the imaging process using the JSS, click **Add** for the script you want to add and then choose a priority and specify parameter values as needed. To remove a script, locate the script on the pane and click **Remove** ⊖.

Printers

This pane allows you to specify which printers you want to map as part of the imaging process. To add or remove a printer, select or deselect the checkbox for the printer.

Note: In Casper Imaging, printers that do not exist on the selected distribution point are displayed in red.

Accounts

This pane allows you to do the following as part of the imaging process:

- Create local accounts
- Bind computers to a directory service
- Set the Open Firmware/EFI password

Note: In the JSS, these are displayed in three separate payloads called Local Accounts, Directory Bindings, and EFI Password.

Local Accounts

To add a local account to the imaging process using Casper Imaging, click **Add** (+) and specify information about the account using the tabs and options provided. Then click **OK**. To remove a local account, select an account and click **Remove** (-).

To add a local account to the imaging process using the JSS, specify information about the account using the options provided. To remove an account, locate the account on the pane and click **Remove** ⊖.

Directory Bindings

To add or remove a directory binding from the imaging process, select or deselect the checkbox for the directory binding.

Open Firmware/EFI Password

To add an Open Firmware/EFI password to the imaging process using Casper Imaging, select the **Set Open Firmware/EFI Password** checkbox and choose "Command" from the **Security Level** pop-up menu. Then enter a password and type the password again to verify it. To remove an Open Firmware/EFI password, choose "None" from the **Security Level** pop-up menu.

To add an Open Firmware/EFI password to the imaging process using the JSS, choose "Command" from the **Security Level** pop-up menu. Then enter a password and type the password again to verify it. To remove the password, select "None" from the **Security Level** pop-up menu.

Network

This pane allows you to configure network settings as part of the imaging process.

To configure network settings, the network configuration (IPv4 connection method) must match the one built into the OS package you're installing or the one in System Preferences on the computer.

To add or remove network settings from the imaging process, configure the options on the pane.

If the network configuration in your OS package is different than the one you want to set on the computer, you must take two additional steps to ensure that the network configuration is set. For more information, see the following Knowledge Base article:

Computer-Specific Network Settings

Advanced

This pane allows you to configure the following items as part of the imaging process:

- Values for Apple Remote Desktop Info fields
- Post-imaging tasks, including:
  - Fix ByHost files
  - Fix disk permissions
  - Show OS X Setup Assistant after restart

Apple Remote Desktop Info Fields

To add or remove values for the Apple Remote Desktop Info fields, enter or remove values from the fields displayed.

In Casper Imaging, you can populate these fields with the values on the computer by clicking **Get Existing**.

Post-imaging Tasks

To add or remove a post-imaging task, select or deselect the checkbox for the task.

Removable MAC Addresses

Adding removable MAC addresses to the JAMF Software Server (JSS) ensures that the JSS ignores certain MAC addresses. For example, MAC addresses of USB Ethernet dongles are commonly added as removable MAC addresses to prevent the JSS from using them as identifiers for computers.

Adding a Removable MAC Address

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management.**

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Removable MAC Addresses** .
5. Click **New** + .
6. Enter the MAC address that you want the JSS to ignore.
7. Click **Save.**

Cloning, Editing, or Deleting a Removable MAC Address

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Computer Management.**

   On a smartphone, this option is in the pop-up menu.
4. In the "Computer Management–Management Framework" section, click **Removable MAC Addresses** .
5. Click the removable MAC address you want to clone, edit, or delete.
6. Do one of the following:
   - To clone the removable MAC address, click **Clone** and change the MAC address. Then click **Save.**
   - To edit the removable MAC address, click **Edit** and change the MAC address. Then click **Save.**
   - To delete the removable MAC address, click **Delete** and then click **Delete** again to confirm.

License Management

About Licensed Software

Licensed software allows you to store and track licenses for the software in your environment so you can easily access license and purchasing information and monitor license compliance.

For each software product that you want to track licenses for, you must create a licensed software record in the JAMF Software Server (JSS). These records allow you to store information about the licenses owned and the software titles that count toward each license (called "software definitions").

Each time a computer submits inventory to the JSS, the software on the computer is compared to the software definitions in the licensed software records. If they match, the computer counts toward the number of licenses in use.

After creating licensed software records, you can use the JSS to evaluate and monitor license compliance, view and report on the licenses in use, and view Application Usage information for the software you're tracking licenses for.

Related Information

For related information, see the following sections in this guide:

- Licensed Software Records

  Find out how to create licensed software records to store and track license information.
- License Compliance

  Find out how to evaluate license compliance by viewing the licensed software records in the JSS.
- Viewing License Usage

  Find out how to view the computers on which licenses are in use.
- Application Usage for Licensed Software

  Find out how frequently the licensed software in your environment is being used.

Licensed Software Records

For each software application you want to track licenses for, you must create a licensed software record in the JAMF Software Server (JSS). These records allow you to store the number of licenses owned and the software titles that count toward each license (called "software definitions"). They also allow you to store detailed license and purchasing information in the JSS.

Each time a computer submits inventory to the JSS, the software titles on the computer are compared to the software definitions in each record. If they match, the computer counts toward the number of licenses in use.

To monitor license compliance on an ongoing basis, you can enable email notifications for a licensed software record. This allows email notifications to be sent to JSS users when the number of licenses in use exceeds the number of licenses owned. (For information on setting up an SMTP server from which to send email notifications and enabling email notifications for a JSS user account, see Integrating with an SMTP Server and Email Notifications.)

Licensed software records also allow you to determine whether a license supersedes or is superseded by another license in the JSS. For example, you may have licenses for both Adobe Illustrator and Adobe CS 5.5 Design Standard, which contains Adobe Illustrator. The licenses for Adobe Illustrator will not be counted toward the licenses for CS 5.5 Design Standard even though CS 5.5 Design Standard contains Adobe Illustrator. Viewing the licensed software record for Adobe Illustrator would show that the licenses are superseded by CS 5.5 Design Standard. Alternatively, viewing the record for CS 5.5 Design Standard would show that the licenses supersede Adobe Illustrator.

There are several ways to create a licensed software record in the JSS. You can manually create the record, use a licensed software template available in the JSS, or upload a licensed software template obtained from JAMF Nation. All licensed software templates have predefined software definitions.

Software definitions can be based on one of two items: the name and version number of each application, font, and plug-in, or the software identification (SWID) tags associated with each software title. For more information on SWID tags and how they are useful for tracking licensed software with the Casper Suite, see the following Knowledge Base article:

Software Identification Tags and Tracking Licensed Software

Requirements

To create a licensed software record based on SWID tags, the software you want to track must have a SWID tag associated with it and the SWID tag must be in the JSS database.

Note: The JSS collects SWID tags from a computer each time the computer submits inventory. SWID tags are not listed in a computer's inventory information in JSS, but they are stored in the JSS database for use with licensed software.

Manually Creating a Licensed Software Record

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

2. Click **Computers** at the top of the page.

3. Click **Licensed Software**.

   On a smartphone, this option is in the pop-up menu.

4. Click **New** + .

5. Use the General pane to configure basic settings for the licensed software record.

   To enable email notifications, select the **Send email notification on violation** checkbox.

6. Click the **Licenses** tab and add license and purchasing information:
   a. Click **Add** + .
   b. Specify information about the license, including the license type and license count.
   c. (Optional) Click the **Purchasing Information** tab and enter purchasing information.
   d. (Optional) Click the **Attachments** tab and click **Upload** ↑ to upload an attachment.
   e. Click **Save**.
   f. Repeat steps a through e to add more license and purchasing information as needed.

7. Click the **Software Definitions** tab.

8. To specify software definitions based on applications, fonts, and plug-ins, do the following:
   a. Choose "Applications, Fonts, and Plug-ins" from the **Software Definitions Type** pop-up menu.
   b. Click **Add** + for the item you want to add.
   c. Specify a name, connector ("is" or "like"), and version number using the fields and pop-up menu provided.
   d. Click **Save**.
   e. Repeat steps a through d to specify additional software definitions as needed.

      The items you added are displayed in a list.

9. To specify software definitions based on SWID tags, do the following:
   a. Choose "Software ID Tags" from the **Software Definitions Type** pop-up menu.
   b. Browse for and choose a reg ID.
   c. Add a SWID tag by clicking **Add** + **.** Then browse for and choose the SWID tag you want to add.
   d. Select the activation statuses you want to include in the software definitions.

10. Click **Save**.

Creating a Licensed Software Record From a Template

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

2. Click **Computers** at the top of the page.

3. Click **Licensed Software**.
   On a smartphone, this option is in the pop-up menu.

4. Click **New From Template** □+ .

5. Click the licensed software template you want to use.

6. Use the General pane to change or configure basic settings for the licensed software record.
   To enable email notifications, select the **Send email notification on violation** checkbox.

7. Click the **Licenses** tab and add license and purchasing information:
   a. Click **Add** + .
   b. Enter information about the license, including the license type and license count.
   c. (Optional) Click the **Purchasing Information** tab and enter purchasing information.
   d. (Optional) Click the **Attachments** tab and click **Upload** ↑ to upload an attachment.
   e. Click **Save**.
   f. Repeat steps a through e to add more license and purchasing information as needed.

8. To view or edit software definitions, click the **Software Definitions** tab and make changes as needed.

9. Click **Save**.

Uploading a Licensed Software Template

You can create a licensed software record by uploading a licensed software template obtained from JAMF Nation. Licensed software templates are available in JAMF Nation at:

https://jamfnation.jamfsoftware.com/licensedSoftwareTemplates.html

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

2. Click **Computers** at the top of the page.

3. Click **Licensed Software**.
   On a smartphone, this option is in the pop-up menu.

4. Click **Upload** ↑ and upload the licensed software template.

5. Use the General pane to change or configure basic settings for the licensed software record.
   To enable email notifications, select the **Send email notification on violation** checkbox.

6. Click the **Licenses** tab and add license and purchasing information:
   a. Click **Add** + .
   b. Enter information about the license, including the license type and license count.
   c. (Optional) Click the **Purchasing Information** tab and enter purchasing information.
   d. (Optional) Click the **Attachments** tab and click **Upload** ↑ to upload an attachment.
   e. Click **Save**.
   f. Repeat steps a through e to add more license and purchasing information as needed.

7. To view or edit software definitions, click the **Software Definitions** tab and make changes as needed.

8. Click **Save**.

Cloning, Editing, or Deleting a Licensed Software Record

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

2. Click **Computers** at the top of the page.

3. Click **Licensed Software**.
   On a smartphone, this option is in the pop-up menu.

4. Click the licensed software record you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the licensed software record, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the licensed software record, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the licensed software record, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- License Compliance
  Find out how to evaluate license compliance by viewing the licensed software records in the JSS.
- Viewing License Usage
  Find out how to view the computers on which licenses are in use.
- Application Usage for Licensed Software
  Find out how frequently the licensed software in your environment is being used.
- Smart Computer Groups
  You can create smart computer groups based on licensed software.

License Compliance

You can evaluate license compliance by viewing the licensed software records in the JSS and comparing the number of licenses in use to the number of licenses owned.

You can also monitor software compliance by allowing email notifications to be sent to JSS users each time a license limit is exceeded. (For more information see, Licensed Software Records.)

Evaluating License Compliance

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Licensed Software**.

   On a smartphone, this option is in the pop-up menu.

   A list of licensed software records is displayed along with the number of licenses in use and the number of licenses owned for each record.

Viewing License Usage

If you are using licensed software records to track software licenses, you can view a list of computers with the licenses in use (called "license usage matches").

Viewing License Usage Matches

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Licensed Software**.

   On a smartphone, this option is in the pop-up menu.
4. Click the licensed software record you want to view license usage matches for.
5. Click **View Matches**.

> ***Note:*** This button is only displayed if the licenses associated with the record are in use on managed computers.

A list license usage matches is displayed.

Related Information

For related information, see the following sections in this guide:

- Computer Reports

  Find out how to export the data in a list of license usage matches to different file formats.
- Performing Mass Actions for Computers

  Find out how to perform mass actions for a list of license usage matches.
- Viewing and Editing Inventory Information for a Single Computer

  You can view the licensed software in use on a single computer by viewing the computer's inventory information in the JSS.

Application Usage for Licensed Software

You can find out how frequently licensed software is being used by viewing the Application Usage logs for a licensed software record. This allows you to view the amount of time that the software was open in the foreground on computers.

Requirements

To view Application Usage logs for a licensed software record, the Computer Inventory Collection settings must be configured to collect Application Usage information. (For more information, see Computer Inventory Collection Settings.)

Viewing Application Usage Logs for a Single Licensed Software Record

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Licensed Software**.

   On a smartphone, this option is in the pop-up menu.
4. Click the licensed software record you want to view Application Usage logs for.
5. Click **View Logs**.

Note: This button is only displayed if the licenses associated with the record are in use on managed computers.

Application Usage logs for the record are displayed.

Usage Management

Application Usage

Application Usage logs allow you to monitor how frequently applications are used on computers and track usage behaviors. You can view the Application Usage logs for a single computer or for a single licensed software record.

Computers submit Application Usage information to the JAMF Software Server (JSS) each time they submit inventory.

Requirements

To view Application Usage logs, the Computer Inventory Collection settings must be configured to collect Application Usage information. (For more information, see Computer Inventory Collection Settings.)

Viewing Application Usage Logs for a Single Computer

The Application Usage logs for a single computer consist of a pie chart that shows the amount of time each application was in the foreground on the computer during a specified date range.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view Application Usage logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab.

   Application Usage logs for the computer are displayed.
6. To view Application Usage logs for a different date range, specify the starting and ending dates using the **Date Range** pop-up menus. Then click **Update**.

Viewing Application Usage Logs for a Single Licensed Software Record

The Application Usage logs for a licensed software record allow you to view the amount of time that the software was open in the foreground on computers.

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Licensed Software**.

   On a smartphone, this option is in the pop-up menu.
4. Click the licensed software record you want to view Application Usage logs for.
5. Click **View Logs**.

> ***Note:*** This button is only displayed if the licenses associated with the record are in use on managed computers.

Application Usage logs for the record are displayed.

Related Information

For related information, see the following sections in this guide:

- Flushing Logs

  Find out how to schedule automatic log flushing or manually flush logs.
- Simple Computer Searches

  You can quickly search the Application Usage information in the JSS for a general range of results.

Computer Usage

Computer Usage logs allow you to monitor how frequently each computer is used and track usage behaviors. The following information is included in Computer Usage logs:

- Startup dates/times
- Login and logout dates/times
- Usernames used to log in and out of the computer

Requirements

To view Computer Usage logs, a startup script or login/logout hooks must be configured to log Computer Usage information. (For more information, see Startup Script and Login and Logout Hooks.)

Viewing Computer Usage Logs for a Single Computer

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Perform a simple or advanced computer search.

   For more information, see Simple Computer Searches or Advanced Computer Searches.
4. Click the computer you want to view Computer Usage logs for.

   If you performed a simple search for an item other than computers, you must click **Expand** ⊕ next to an item to view the computers related to that item.
5. Click the **History** tab, and then click the **Computer Usage Logs** category.

   Computer Usage logs for the computer are displayed.

Related Information

For related information, see the following section in this guide:

Flushing Logs
Find out how to schedule automatic log flushing or manually flush logs.

Restricted Software

Restricted software allows you to prevent users or groups of users from accessing certain applications. For instance, you might want to prevent all users from accessing a peer-to-peer file sharing application or restrict everyone except the IT staff from accessing common administrative utilities.

For each application that you want to restrict, you must create a restricted software record. This allows you to specify the users to which the restriction applies and control what happens when the application is opened by those users. For instance, you can kill the restricted process, delete the application, and even display a message to the user.

If there is an SMTP server set up in the JSS, you can enable email notifications for the restricted software record. This allows email notifications to be sent to JSS users each time a violation occurs. (For information on setting up an SMTP server and enabling email notifications for JSS user accounts, see Integrating with an SMTP Server and Email Notifications.)

Creating a Restricted Software Record

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Restricted Software**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Configure the restricted software record using the fields and options on the pane.
   To enable email notifications, select the **Send email notification on violation** checkbox.
6. Click the **Scope** tab and configure the scope of the restricted software record.
   For more information, see Scope.
7. Click **Save**.

The restriction is applied to computers in the scope the next time they check in with the JSS.

Cloning, Editing, or Deleting a Restricted Software Record

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Restricted Software**.
   On a smartphone, this option is in the pop-up menu.

4. Click the restricted software record you want to clone, edit, or delete.

5. Do one of the following:
    - To clone the restricted software record, click **Clone** and make changes as needed. Then click **Save**.
    - To edit the restricted software record, click **Edit** and make changes as needed. Then click **Save**.
    - To delete the restricted software record, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to computers in the scope the next time they check in with the JSS.

Related Information

For related information, see the following section in this guide:

Viewing Restricted Software for a Single Computer
Find out how to view the restricted software for a single computer.

For related information, see the following Knowledge Base article:

Finding the Name of Processes When Configuring Restricted Software
Learn how to find the exact name of the process you want create restricted software for.

Managing Mobile Devices

Enrollment

About Mobile Device Enrollment

Enrollment is the process of adding mobile devices to the JAMF Software Server (JSS) to establish a connection between the devices and the JSS. This allows you to perform inventory, configuration, security management, and distribution tasks on the devices.

When mobile devices are enrolled, inventory information for the devices is submitted to the JSS.

There are two ways to enroll mobile devices with the JSS:

- **User-initiated enrollment**—You can allow users to enroll their own mobile devices by having them log in to an enrollment portal where they follow the onscreen instructions to install the necessary profile and certificates. You can provide this URL by sending it in an email or SMS invitation from the JSS, or through any other means that fit your environment.
- **Enroll connected mobile devices**—You can create an enrollment profile using the JSS and install it on mobile devices by connecting them to a computer via USB. This enrollment method requires Apple Configurator or Apple's iPhone Configuration Utility (iPCU).

  Apple TV devices can only be enrolled by connecting them to a computer via USB and installing an enrollment profile using Apple Configurator.

Related Information

For more information, see the following sections in this guide:

- User-Initiated Enrollment for Mobile Devices

  Find out how to allow users to enroll their own mobile devices by having them log in to an enrollment portal.
- Enrollment Profiles

  Find out how to create and download enrollment profiles so you can enroll mobile devices by connecting them to a computer via USB.
- Components Installed on Mobile Devices

  Learn about the components installed on mobile devices during enrollment.

Components Installed on Mobile Devices

The following components are installed on mobile devices during enrollment:

- **Trust Profile**—This profile contains the CA certificate. The CA certificate establishes trust between the certificate authority (CA) and mobile devices.
- **MDM Profile**—This profile includes a SCEP enrollment request and an MDM enrollment request.
- **Device certificate**—This certificate verifies the identity of managed mobile devices each time they communicate with the JAMF Software Server (JSS).
- **Self Service web clip**—The Self Service web clip allows you to distribute iOS configuration profiles, apps, eBooks, and updated MDM profiles to mobile devices for users to install. Users tap the web clip to browse and then install items using an interface similar to the App Store.

  You can prevent the Self Service web clip from being installed on mobile devices if necessary. (For more information, see Self Service Web Clip.)

Note: The Self Service web clip is not installed on Apple TV devices.

User-Initiated Enrollment Settings for Mobile Devices

You can use the User-Initiated Enrollment settings for mobile devices to allow enrollment without an invitation and configure the enrollment process. When you configure the enrollment process, you can do the following:

- Require users to install the CA certificate.
- Customize the enrollment portal.
- Customize the appearance of the MDM profile.

Configuring the User-Initiated Enrollment Settings for Mobile Devices

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Mobile Device Management**.
   On a smartphone, this option is in the pop-up menu.
4. Click **User-Initiated Enrollment** 📱 .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- User-Initiated Enrollment for Mobile Devices
  Find out how to allow users to enroll their own mobile devices by having them log in to an enrollment portal.
- User-Initiated Enrollment Experience for Mobile Devices
  Learn about the steps users take to enroll their own mobile devices.
- Certificates
  Learn more about the CA certificate.

User-Initiated Enrollment for Mobile Devices

You can allow users to enroll their own mobile devices by having them log in to an enrollment portal where they are prompted to install the necessary profile and certificates.

To direct users to the enrollment portal, you need to provide them with the enrollment URL. This is the full URL for the JAMF Software Server (JSS) followed by "/enroll". For example:

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

You can provide this URL by sending it in an email or SMS invitation from the JSS, or through any other means that fit your environment. Sending an invitation from the JSS allows you to add mobile devices to a site during enrollment.

Users can log in to the enrollment portal using an LDAP directory account or a JSS user account. If users log in to the enrollment portal with an LDAP directory account, user and location information is submitted during enrollment.

Requirements

To send a mobile device enrollment invitation via email, you need an SMTP server set up in the JSS. (For more information, see Integrating with an SMTP Server.)

If you plan to provide the enrollment URL to users without using an email or SMS invitation, the User-Initiated Enrollment settings must be configured to allow enrollment without an invitation. (For more information, see User-Initiated Enrollment Settings for Mobile Devices.)

For users to log in to the enrollment portal with their LDAP directory account, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

Sending a Mobile Device Enrollment Invitation

You can send an enrollment invitation by email or SMS message.

Before you configure the invitation, make sure you have the email addresses or phone numbers of the users you want to send the invitation to.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Invitations**.
   On a smartphone, this option is in the pop-up menu.

4. Click **New** + .
5. Follow the onscreen instructions to send the enrollment invitation.

   An enrollment invitation is immediately sent to email addresses or phone numbers you specified.

   You can view the status of the enrollment invitation in the list of invitations.

Viewing Mobile Device Enrollment Invitation Usage

You can view a list of mobile devices that were enrolled with a single enrollment invitation.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Invitations**.
   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment invitation you want to view usage for.
5. Click **View Enrolled Mobile Devices**.

   A list of mobile devices enrolled with the invitation is displayed.

Deleting a Mobile Device Enrollment Invitation

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Invitations**.
   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment invitation you want to delete.
5. Click **Delete**, and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- User-Initiated Enrollment Experience for Mobile Devices

  Learn about the steps users take to enroll their own mobile devices.

- Enrollment Profiles

  Find out how to create and download enrollment profiles so you can enroll mobile devices by connecting them to a computer via USB.

- Components Installed on Mobile Devices

  Learn about the components installed on the mobile devices during enrollment.

User-Initiated Enrollment Experience for Mobile Devices

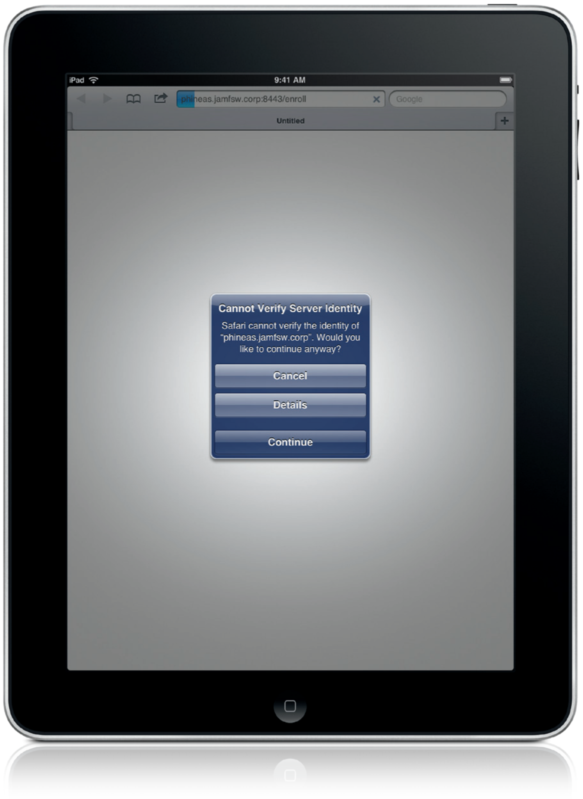
When a user taps the enrollment URL from their mobile device, they are guided through the following steps to enroll their device:

1. The user is prompted to enter credentials for an LDAP directory account or a JSS user account with user-initiated enrollment privileges, and then they must tap **Login**.

   The login prompt is not displayed if the enrollment portal was accessed via an enrollment invitation for which the **Require Login** option is disabled. (For more information, see User-Initiated Enrollment for Mobile Devices.)

2. If notified that the device cannot verify the identity of the JSS, the user must tap **Continue**.

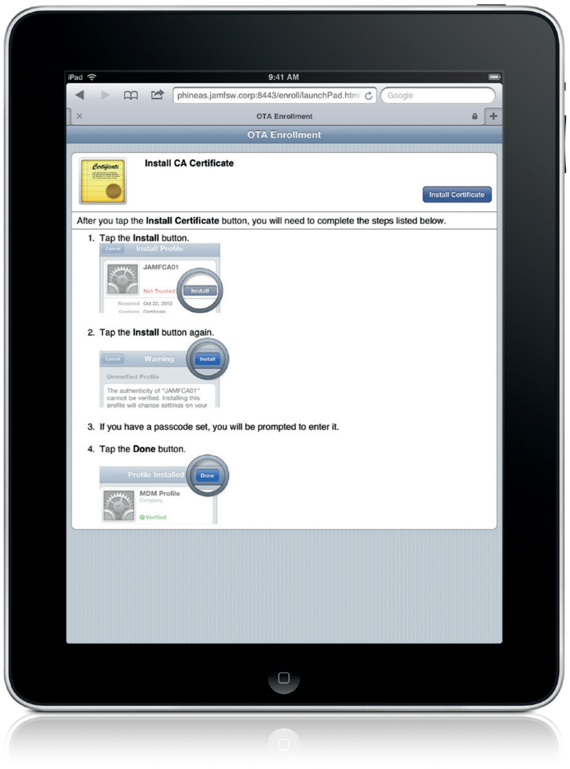
   This notification only appears if the SSL certificate is not natively trusted by the device.



Cannot Verify Server Identity

Safari cannot verify the identity of "phineas.jamfsw.corp". Would you like to continue anyway?

3. The user must tap **Install Certificate** to start the installation of the profile that contains the CA certificate.



Install CA Certificate

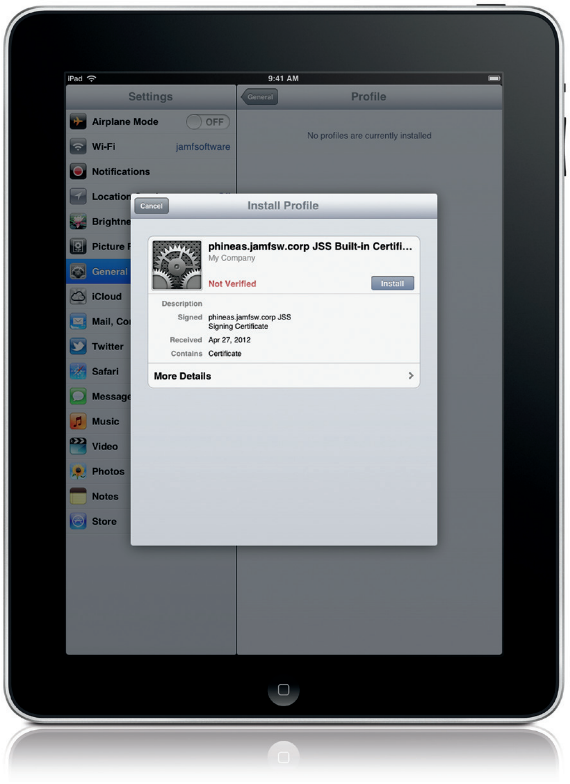
After you tap the **Install Certificate** button, you will need to complete the steps listed below.

1. Tap the **Install** button.
2. Tap the **Install** button again.

The authenticity of "JAMFCA01" cannot be verified. Installing this profile will change settings on your

3. If you have a passcode set, you will be prompted to enter it.
4. Tap the **Done** button.

4. The user must tap **Install** to continue.

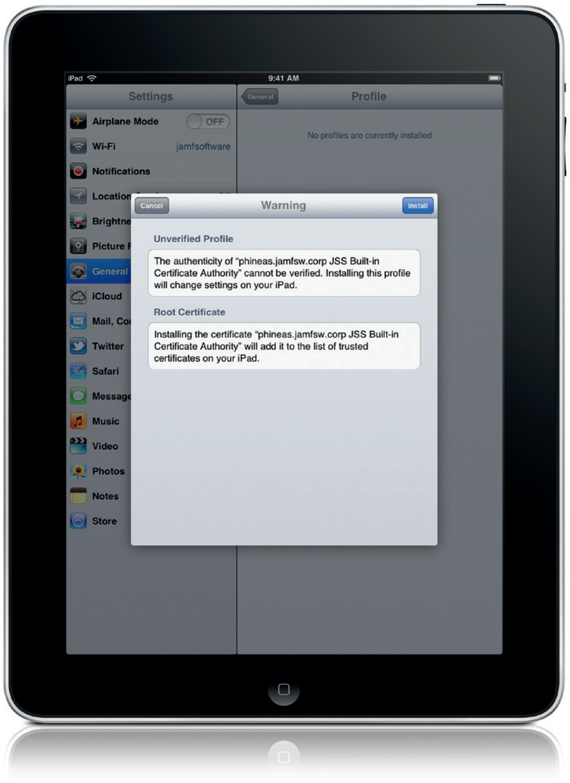


No profiles are currently installed

phineas.jamfsw.corp JSS Built-in Certifi...
My Company
Not Verified

Description
Signed phineas.jamfsw.corp JSS Signing Certificate
Received Apr 27, 2012
Contains Certificate

5. When notified that the profile will change settings on the device, the user must tap **Install Now**. If the device has a passcode, the user must enter the passcode.



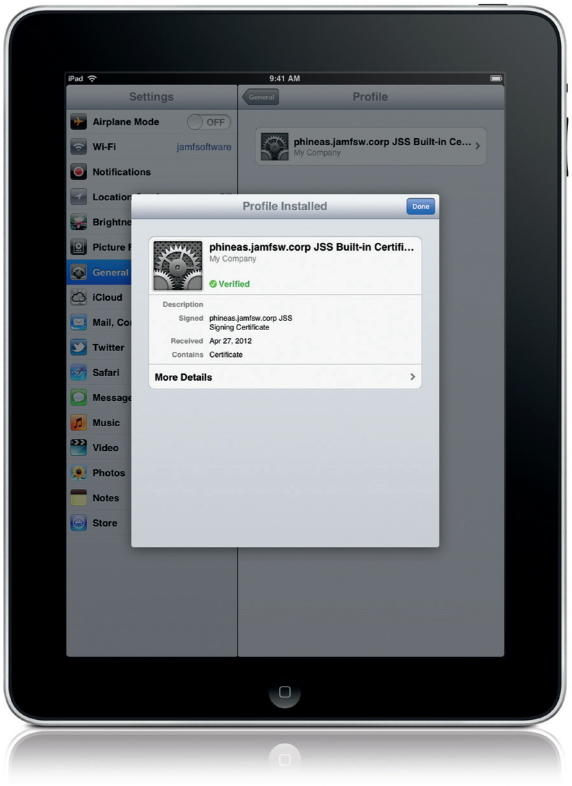
Unverified Profile

The authenticity of “phineas.jamfsw.corp JSS Built-in Certificate Authority” cannot be verified. Installing this profile will change settings on your iPad.

Root Certificate

Installing the certificate “phineas.jamfsw.corp JSS Built-in Certificate Authority” will add it to the list of trusted certificates on your iPad.

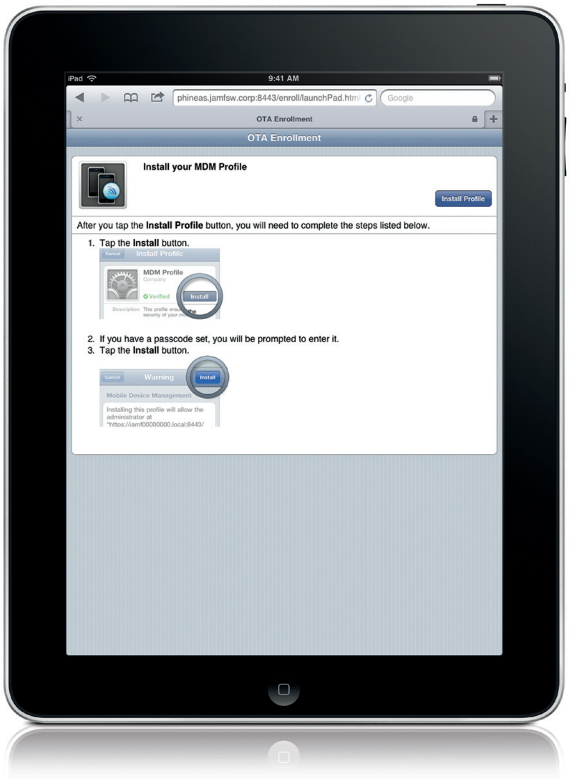
6. To complete the installation, the user must tap **Done**.



phineas.jamfsw.corp JSS Built-in Certifi...
My Company
✓ Verified

Description
Signed phineas.jamfsw.corp JSS Signing Certificate
Received Apr 27, 2012
Contains Certificate

7. The user must tap **Install Profile** to initiate the installation of the MDM profile.



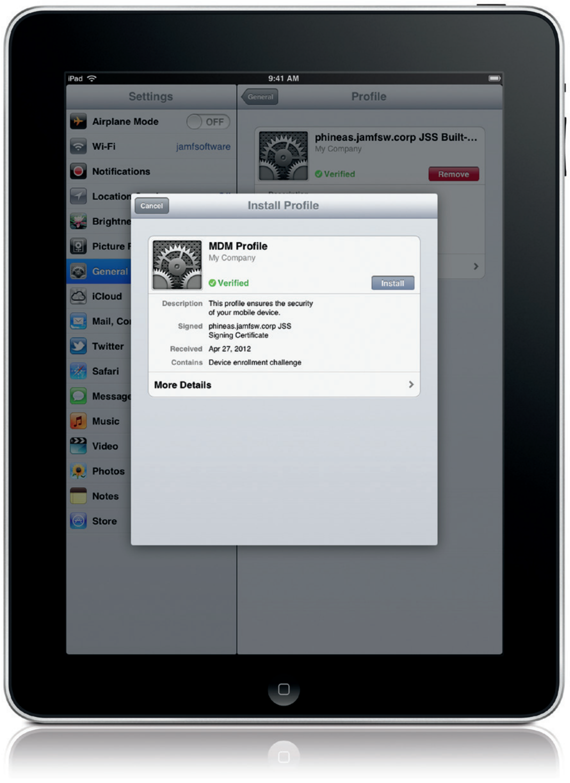
Install your MDM Profile

After you tap the **Install Profile** button, you will need to complete the steps listed below.

1. Tap the **Install** button.
2. If you have a passcode set, you will be prompted to enter it.
3. Tap the **Install** button.

Installing this profile will allow the administrator at "https://iamf00000000.local:8443/

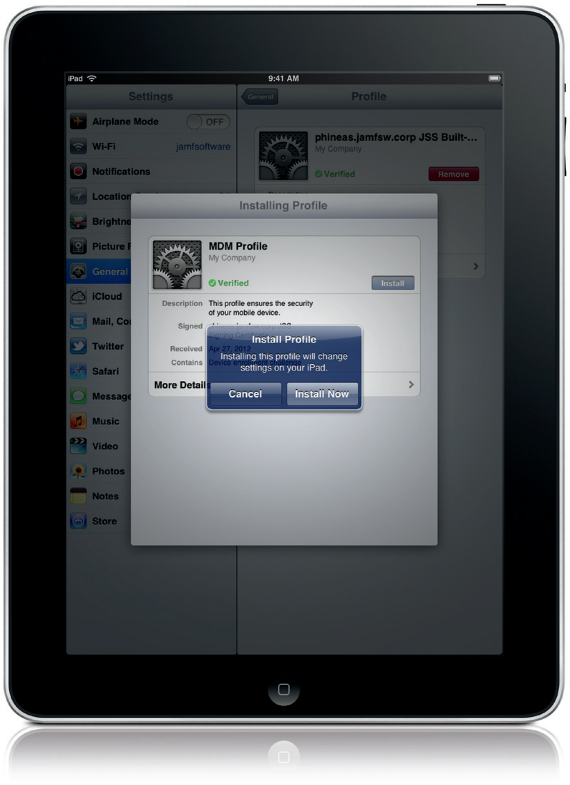
8. The user must tap **Install** to continue.



MDM Profile
My Company
Verified

Description: This profile ensures the security of your mobile device.
Signed: phineas.jamfsw.corp JSS Signing Certificate
Received: Apr 27, 2012
Contains: Device enrollment challenge

9. When notified that installing the profile will change settings on the device, the user must tap **Install Now**. If the device has a passcode, the user must enter the passcode.

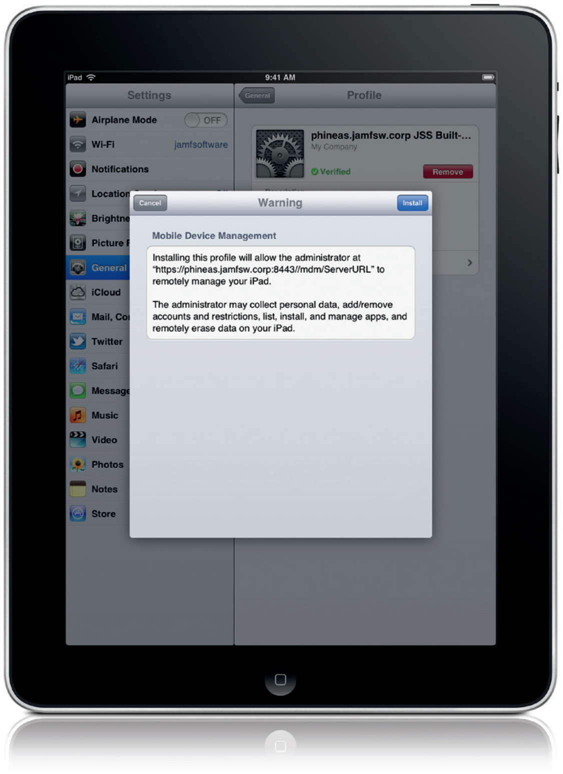


Description This profile ensures the security of your mobile device.

Install Profile

Installing this profile will change settings on your iPad.

10. When notified that installing the profile will allow an administrator to remotely manage the device, the user must tap **Install**.

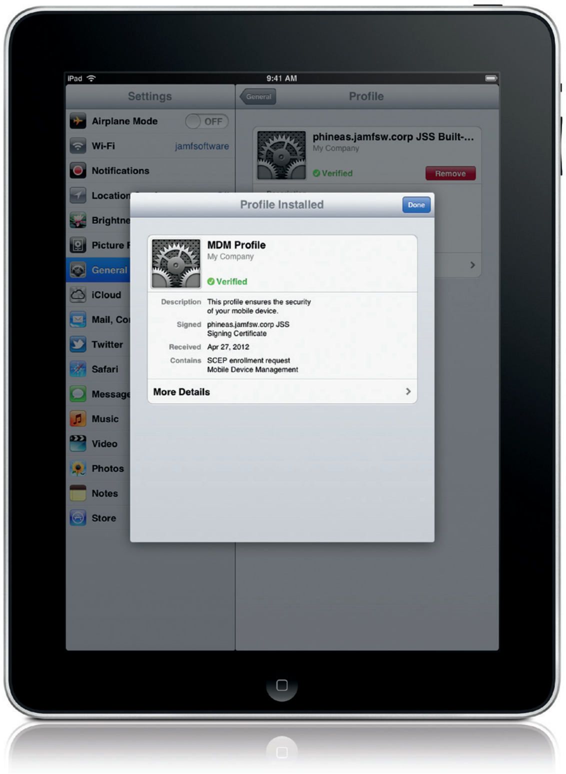


Mobile Device Management

Installing this profile will allow the administrator at "https://phineas.jamfsw.corp:8443//mdm/ServerURL" to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.

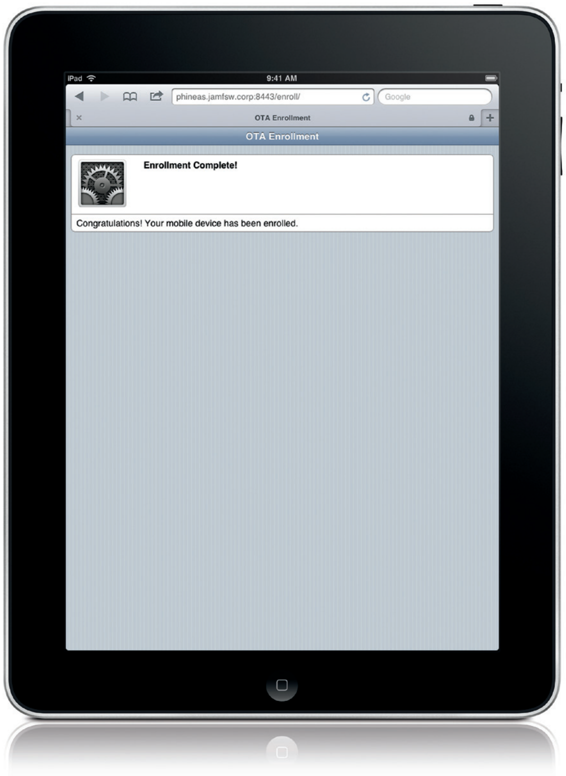
11. To complete the enrollment process, the user must tap **Done**.



MDM Profile
My Company
Verified

Description: This profile ensures the security of your mobile device.
Signed: phineas.jamfsw.corp JSS Signing Certificate
Received: Apr 27, 2012
Contains: SCEP enrollment request Mobile Device Management

When the enrollment is complete, the device is enrolled with the JSS.



Enrollment Complete!

Congratulations! Your mobile device has been enrolled.

Enrollment Profiles

Enrollment profiles are .mobileconfig files that allow you to enroll mobile devices with the JAMF Software Server (JSS). This involves creating an enrollment profile, connecting the devices to a computer via USB, and installing the enrollment profile using Apple Configurator or Apple's iPhone Configuration Utility (iPCU).

You can use the JSS to create and download enrollment profiles. When you create an enrollment profile, you can specify user and location information, purchasing information, and a site for mobile devices enrolled using the profile.

Important: You cannot distribute an updated MDM profile via the Self Service web clip to mobile devices enrolled using an enrollment profile. For information on updating an MDM profile, see the following Knowledge Base article:

Distributing Updated MDM Profiles

Tools for Installing Enrollment Profiles

Before creating an enrollment profile, you need to decide which tool you will use to install the profile on mobile devices. The tool you use to install enrollment profiles affects the way you manage the profiles in the JSS.

The following tools can be used to install enrollment profiles:

- **Apple Configurator**—By default, when you create an enrollment profile in the JSS, it is created for use with Apple Configurator. Before you can use Apple Configurator to enroll mobile devices, you need to download both the enrollment profile and its Trust Profile from the JSS so you can import these profiles to Apple Configurator.
- **iPCU**—You should only create an enrollment profile for use with iPCU if you plan to install the profile on mobile devices with iOS 6 or earlier. Before you can use iPCU to enroll mobile devices, you need to download the enrollment profile from the JSS so you can import it to iPCU.

Note: Enrollment profiles created using the JSS v9.0 or earlier cannot be used to enroll mobile devices with iOS 7 or later. If you plan to enroll mobile devices with iOS 7 or later, you need to create a new enrollment profile following the instructions in the Creating an Enrollment Profile for Use with Apple Configurator section.

For information on how to install enrollment profiles using Apple Configurator or iPCU, see the following Knowledge Base article:

Installing Enrollment Profiles Using Apple Configurator or iPCU

Creating an Enrollment Profile for Use with Apple Configurator

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General pane to configure basic settings for the enrollment profile.

   Ensure that the **Create profile for use with iPCU** checkbox is not selected.
6. (Optional) Click the **User and Location Information** tab and specify user and location information for the devices.
7. (Optional) Click the **Purchasing Information** tab and specify purchasing information for the devices.
8. Click **Save**.

Creating an Enrollment Profile for Use with iPCU

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General pane to configure basic settings for the enrollment profile.

   Select the **Create profile for use with iPCU** checkbox and choose a target iOS version.

   The target iOS must match the iOS on the devices that you plan to enroll.
6. (Optional) Click the **User and Location Information** tab and specify user and location information for the devices.
7. (Optional) Click the **Purchasing Information** tab and specify purchasing information for the devices.
8. Click **Save**.

Cloning, Editing, or Deleting an Enrollment Profile

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment profile you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the profile, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the profile, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the profile, click **Delete.** Then click **Delete** again to confirm.

Downloading an Enrollment Profile

You need to download the enrollment profile (.mobileconfig) from the JSS before using it to enroll mobile devices using Apple Configurator or iPCU.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment profile you want to download.
5. Click **Download**.

   On OS X v10.7 or later, you may be prompted to install the profile. Click **Cancel** to decline.

   The enrollment profile downloads immediately as a .mobileconfig file.

Note: When the enrollment profile is imported to Apple Configurator or iPCU, it displays in the Profiles list with a name that identifies it as the MDM profile.

Downloading a Trust Profile

The Trust Profile contains the CA certificate that establishes trust between the certificate authority (CA) and mobile devices.

When you create an enrollment profile for use with Apple Configurator, the JSS automatically creates an associated Trust Profile. You need to download the Trust Profile (`Trust Profile.mobileconfig`) from the JSS so that you can import it to Apple Configurator along with the enrollment profile.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click the enrollment profile for which you want to download a Trust Profile.
5. Click **Trust Profile**.

   On OS X v10.7 or later, you may be prompted to install the profile. Click **Cancel** to decline.

   The Trust Profile downloads immediately with the filename `Trust Profile.mobileconfig`.

> ***Note:*** When the Trust Profile is imported to Apple Configurator, it displays in the Profiles list with a name that identifies it as the CA certificate profile.

Related Information

For related information, see the following sections in this guide:

- User-Initiated Enrollment for Mobile Devices

  Find out how to allow users to enroll their own mobile devices by having them log in to an enrollment portal.
- Components Installed on Mobile Devices

  Learn about the components installed during mobile device enrollment.

Inventory

Mobile Device Inventory Collection Settings

The Mobile Device Inventory Collection settings allow you to do the following:

- Configure the frequency at which inventory is collected from mobile devices.
- Collect unmanaged apps as inventory.

By default, mobile devices submit inventory to the JAMF Software Server (JSS) once every day.

Configuring the Mobile Device Inventory Collection Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Mobile Device Management**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Inventory Collection** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Related Information

For related information, see the following sections in this guide:

- Simple Mobile Device Searches
  Learn how to quickly search the items in your inventory for a general range of results.
- Advanced Mobile Device Searches
  Lean how to create and save an advanced mobile device search.
- Viewing and Editing Inventory Information for a Single Mobile Device
  Find out how to view and edit inventory information for a single mobile device.

Mobile Device Extension Attributes

Mobile device extension attributes are custom fields that you can create to collect almost any type of data from a mobile device.

When you create a mobile device extension attribute, you specify the following information:

- Type of data being collected, such as string, integer, or date
- Inventory category in which to display the extension attribute in the JSS, such as Hardware or Purchasing
- Input type, which determines how the extension attribute is populated with data

Extension attributes can add time and network traffic to the inventory process depending on the type of data you choose to collect and the input type used to collect it.

Mobile Device Extension Attribute Input Types

You can choose to populate the value of a mobile device extension attribute using any of the following input types:

- **Text field—**This displays a text field in mobile device inventory information that you can enter a value into. Only extension attributes created manually can be populated using a text field.
- **Pop-up menu—**This displays a pop-up menu in mobile device inventory information from which you can choose a value. Only extension attributes created manually can be populated using a pop-up menu.
- **LDAP Attribute Mapping**—This populates the extension attribute with the value for an LDAP attribute. It also generates a variable that can be used to populate configuration profile settings with values for the LDAP attribute. The variable is `$EXTENSIONATTRIBUTE_<#>`, where <#> is the extension attribute ID. For more information on payload variables for configuration profiles, see iOS Configuration Profiles.

Requirements

To create a mobile device extension attribute with the "LDAP Attribute Mapping" input type, you need:

- An LDAP server set up in the JSS (For more information, see Integrating with LDAP Directory Services.)
- The Mobile Device Inventory Collection settings configured to collect user and location information from LDAP (For more information, see Mobile Device Inventory Collection Settings.)

Creating a Mobile Device Extension Attribute

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.

3. Click **Mobile Device Management**.

   On a smartphone, this option is in the pop-up menu.

4. Click **Extension Attributes** .

5. Click **New** + .

6. Configure the settings on the pane.

7. Click **Save**.

If the extension attribute has the "LDAP Attribute Mapping" input type, the LDAP attribute variable is displayed on the pane.

Cloning, Editing, or Deleting a Mobile Device Extension Attribute

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

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Mobile Device Management**.

   On a smartphone, this option is in the pop-up menu.

4. Click **Extension Attributes** .

5. Click the extension attribute you want to clone, edit, or delete.

6. Do one of the following:

   - To clone the extension attribute, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the extension attribute, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the extension attribute, click **Delete** and then click **Delete** again to confirm.

Related Information

For related information, see the following sections in this guide:

- Mobile Device Inventory Display Settings

  You can display extension attributes in the results of a simple mobile device search.

- Viewing and Editing Inventory Information for a Single Mobile Device

  You can view the extension attributes collected from a single mobile device and edit extension attribute values for that mobile device.

- Smart Mobile Device Groups

  You can create smart mobile device groups based on extension attributes.

Mobile Device Inventory Display Settings

The Mobile Device Inventory Display settings allow you to choose which attribute fields to display in the results of a simple mobile device search.

Configuring the Mobile Device Inventory Display Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Mobile Device Management**.

   On a smartphone, this option is in the pop-up menu.
4. Click **Inventory Display** .
5. On each pane, select the checkbox for each attribute field you want to display.
6. Click **Save**.

Related Information

For related information, see the following section in this guide:

Simple Mobile Device Searches
Learn how to quickly search the items in your inventory for a general range of results.

Simple Mobile Device Searches

A simple mobile device search functions like a search engine, allowing you to quickly search the items in your inventory for a general range of results.

The following table shows the items that you can search by and the attributes on which you can base each search:

Inventory Item	Searchable Attributes
Mobile devices	Mobile device name Wi-Fi MAC address Bluetooth MAC address UDID Serial number Username Full name Email address Phone number Position Department Building Room
Mobile device apps	Application name

Search Syntax

The following table explains the syntax to use for refining a simple search:

Function	Usage	Example
Wildcard search	Use an asterisk (*) before or after any characters or search terms to return all results that include those characters or terms. Use an asterisk (*) without any other characters or terms to return all results for the item you are searching.	Enter "555*" to return all results that begin with "555". Enter "*@mycompany.com" to return all results that include "@mycompany.com".
Include all search terms	Use a comma (,) between search terms to return results that include those search terms.	Enter "Design, Development" to return all results that include "Design" and "Development".

Function	Usage	Example
Exclude a search term	Use a hyphen (-) before a search term to exclude that term from all results.	Enter "Smith -John" to return all results for "Smith" except those that include "John".
Return all results	Perform a search with no criteria in the search field to return all results for the item you are searching. This only works when searching for mobile devices.	--

Performing a Simple Mobile Device Search

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.

   On a smartphone, this option is in the pop-up menu.
4. Choose an item from the **Search** pop-up menu.
5. Enter one or more search terms in the field(s) provided.

   For information on the syntax to use to refine your search, see Search Syntax.
6. Press the Enter key.

The list of search results is displayed.

If you searched for an item other than mobile devices, you can view the devices associated with a result by clicking **Expand** ⊕ next to the result. You can also change the item on which the results are based by choosing an item from the pop-up menu at the top of the page.

Related Information

For related information, see the following sections in this guide:

- Viewing and Editing Inventory Information for a Single Mobile Device

  Find out how to view and edit inventory information for a single mobile device.
- Mobile Device Reports

  Find out how to export the data in your search results to different file formats.
- Performing Mass Actions for Mobile Devices

  Find out how to perform mass actions on the results of a mobile device search.
- Advanced Mobile Device Searches

  Lean how to create and save an advanced mobile device search.
- Mobile Device Inventory Display Settings

  Learn how to change the attribute fields displayed in the results of a simple mobile device search.

Advanced Mobile Device Searches

Advanced mobile device searches allow you to use detailed search criteria to search for devices in the JAMF Software Server (JSS). These types of searches give you more control over your search by allowing you to do the following:

- Generate specific search results.
- Specify which attribute fields to display in the search results.
- Save the search.

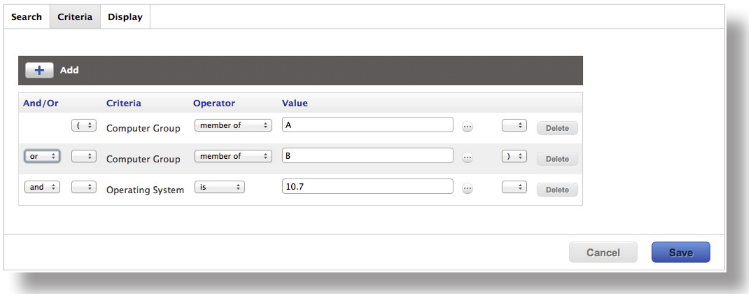
Creating an Advanced Mobile Device Search

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the Search pane to configure basic settings for the search.

   To save the search, select the **Save this Search** checkbox.
6. Click the **Criteria** tab and add criteria for the search:
   a. Click **Add** + .
   b. Click **Choose** for the criteria you want to add.

      To display additional criteria, click **Choose** for "Other Criteria".
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse** ⋯ .
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify relationships between criteria.
8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.



And/Or		Criteria	Operator	Value			
	(	Computer Group	member of	A	⋯		Delete
or		Computer Group	member of	B	⋯	)	Delete
and		Operating System	is	10.7	⋯		Delete

9. Click the **Display** tab and select the attribute fields you want to display in your search results.

10. Click **Save**.

    Operations in the search take place in the order they are listed (top to bottom).

    The results of a saved search are updated each time mobile devices contact the JSS and meet or fail to meet the specified search criteria.

    To view search results, click **View**.

Cloning, Editing, or Deleting a Saved Advanced Mobile Device Search

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Click the advanced mobile device search you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the search, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the search, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the search, click **Delete**. Then click **Delete** again to confirm.

Viewing Advanced Mobile Device Search Results

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu..
4. Click the advanced mobile device search you want to view the results for.
5. Click **View**.

   The list of search results is displayed.

Related Information

For related information, see the following sections in this guide:

- Mobile Device Reports

  Find out how to export the data in your search results to different file formats.
- Performing Mass Actions for Mobile Devices

  Find out how to perform mass actions on the results of a mobile device search.
- Viewing and Editing Inventory Information for a Single Mobile Device

  Find out how to view and edit inventory information for a single mobile device.
- Simple Mobile Device Searches

  Learn how to quickly search the items in your inventory for a general range of results.

Mobile Device Reports

The data displayed in smart or static group membership lists or mobile device search results can be exported from the JAMF Software Server (JSS) to the following file formats:

- Comma-separated values file (.csv)
- Tab delimited text file (.txt)
- XML file

You can change the way the data is organized by basing the export on any the following inventory items:

- Mobile devices
- Mobile device groups
- Apps
- Configuration profiles
- Certificates
- Provisioning profiles

The data is displayed in alphanumeric order by the selected inventory item.

Creating Mobile Device Reports

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Do one of the following:
   - View mobile device group memberships. (For more information, see Smart Mobile Device Groups or Static Mobile Device Groups.)
   - View simple or advanced mobile device search results. (For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.)

Note: You can only create a report from a simple mobile device search if you searched by devices.

4. At the bottom of the list, click **Export**.
5. Follow the onscreen instructions to export the data.

   The report downloads immediately.

Performing Mass Actions for Mobile Devices

Mass actions allow you to perform potentially tedious tasks for multiple mobile devices at the same time. You can use the JSS to perform the following mass actions:

- Edit the site.
- Look up and populate purchasing information from Apple's Global Service Exchange (GSX).
- Send a mass email to users.
- Delete the mobile devices from the JSS.

Mass actions can be performed on static or smart group membership lists or mobile device search results.

Mass Editing the Site for Mobile Devices

Mass editing the site for mobile devices allows you to add the devices to a site or change the site they belong to.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Do one of the following:
   - View mobile device group memberships. (For more information, see Smart Mobile Device Groups or Static Mobile Device Groups.)
   - View simple or advanced mobile device search results. (For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.)

> ***Note:*** You can only perform mass actions from a simple mobile device search if you searched by devices.

4. At the bottom of the list, click **Action**.
5. Select **Edit the Site**.

   This option is only displayed if there are one or more sites in the JSS. (For more information, see Sites.)
6. Follow the onscreen instructions to edit the site.

Mass Looking up and Populating Purchasing Information for Mobile Devices

You can mass look up purchasing information from Apple's Global Service Exchange (GSX) and populate the information in the JSS if desired.

This requires a GSX connection set up in the JSS. (For more information, see Integrating with GSX.)

> ***Note:*** GSX may not always return complete purchasing information. Only the information found in GSX is returned.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Do one of the following:
   - View mobile device group memberships. (For more information, see Smart Mobile Device Groups or Static Mobile Device Groups.)
   - View simple or advanced mobile device search results. (For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.)

> ***Note:*** You can only perform mass actions from a simple mobile device search if you searched by devices.

4. At the bottom of the list, click **Action**.
5. Select **Look up Purchasing Information from GSX**.
   This option is only displayed if there is a GSX connection set up in the JSS.
6. Follow the onscreen instructions to look up and populate the purchasing information.

Sending a Mass Email to Mobile Device Users

You can send a mass email to users associated with the mobile devices in the JSS. The email is sent to the email address associated with each device.

This requires an SMTP server set up in the JSS. (For more information, see Integrating with an SMTP Server.)

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.

3. Do one of the following:
   - View mobile device group memberships. (For more information, see Smart Mobile Device Groups or Static Mobile Device Groups.)
   - View simple or advanced mobile device search results. (For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.)

> ***Note:*** You can only perform mass actions from a simple mobile device search if you searched by devices.

4. At the bottom of the list, click **Action**.
5. Select **Send Email**.

   This option is only displayed if there is an SMTP server set up in the JSS.
6. Follow the onscreen instructions to create and send the email.

Mass Deleting Mobile Devices

You can mass delete mobile devices from the JSS.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Do one of the following:
   - View mobile device group memberships. (For more information, see Smart Mobile Device Groups or Static Mobile Device Groups.)
   - View simple or advanced mobile device search results. (For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.)

> ***Note:*** You can only perform mass actions from a simple mobile device search if you searched by devices.

4. At the bottom of the list, click **Action**.
5. Select **Delete Mobile Devices**.
6. Follow the onscreen instructions to delete the mobile devices.

Related Information

For related information, see the following section in this guide:

Viewing and Editing Inventory Information for a Single Mobile Device
Find out how to edit the site, or look up and populate purchasing information for a single mobile device.

Viewing and Editing Inventory Information for a Single Mobile Device

The JAMF Software Server (JSS) stores detailed inventory information for each enrolled mobile device. You can view and edit this information right from the JSS.

The following table describes the information that you can view and edit for each mobile device:

Category	Description	Editable Fields
General	View general information about the mobile device, including mobile device name, site, and management status.	Site Asset Tag AirPlay Password (Apple TV only)
User and Location	View information about the primary user and the mobile device's physical location. Look up and populate user information from an LDAP directory service. (This requires an LDAP server set up in the JSS. For more information, see Integrating with LDAP Directory Services.)	Username Full name Email address Phone number Department Building Room Position
Purchasing	View purchasing information, including PO details, warranty information, and purchasing contact. Look up and populate purchasing information from Apple's Global Service Exchange (GSX). (This requires a GSX connection set up in the JSS. For more information see Integrating with GSX.)	Purchased or leased PO number PO date Vendor Warranty expiration AppleCare ID Lease expiration Purchase price Life expectancy Purchasing account Purchasing contact
Extension Attributes	View custom data collected using extension attributes.	All extension attributes
Apps	View a list of applications installed on the mobile device.	--
Security	View security information about the mobile device, including data protection, hardware encryption, and passcode status.	--

Category	Description	Editable Fields
Network	View network information about the mobile device, including home carrier network, current carrier network, and phone number.	
Certificates	View a list of certificates installed on the mobile device.	--
Profiles	View a list of profiles installed on the mobile device.	--
Provisioning Profiles	View a list of active services.	--
Attachments	View a list of files attached to the inventory record. Upload attachments. Delete attachments.	--

Viewing Inventory Information for a Single Mobile Device

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view information for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the devices related to that item.

   The mobile device's inventory information is displayed.
5. Use the categories to view information for the mobile device.

Editing Inventory Information for a Single Mobile Device

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to edit information for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the devices related to that item.

   The mobile device's inventory information is displayed.

5. Select the category that contains the information you want to edit and click **Edit**.

6. Make changes as needed.

   If you are editing user and location information or purchasing information, you can click **Search** 🔍 to look up and populate information from an LDAP directory service or Apple's Global Service Exchange (GSX).

   > ***Note:*** This button is only displayed if you have an LDAP server or a GSX connection set up in the JSS.

7. Click **Save**.

Viewing Management Information for a Single Mobile Device

The JAMF Software Server (JSS) allows you to view the following management information for a single mobile device:

- Pending management commands
- iOS configuration profiles
- Apps
- eBooks
- Group memberships

Viewing the Pending Management Commands for a Single Mobile Device

When viewing management information for a single mobile device, you can view a list of pending management commands for the mobile device. The list includes all pending actions related to the following:

- Sending iOS remote commands
- Installing or removing iOS configuration profiles
- Installing or removing apps
- Installing or removing Provisioning Profiles
- Updating inventory

You can also cancel a pending management command.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view pending management commands for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.
5. Click the **Management** tab.

   A list of pending management commands for the mobile device is displayed.
6. To cancel a pending management command, click **Cancel** for the command.

Viewing Configuration Profiles for a Single Mobile Device

When viewing management information for a single mobile device, you can view a list of iOS configuration profiles that have the mobile device in the scope.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view configuration profiles for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.
5. Click the **Management** tab, and then click the **Configuration Profiles** category.

   A list of configuration profiles for the mobile device is displayed.

Viewing Apps for a Single Mobile Device

When viewing management information for a single mobile device, you can view a list of apps that have the mobile device in the scope.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view apps for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.
5. Click the **Management** tab, and then click the **Apps** category.

   A list of apps for the mobile device is displayed.

Viewing eBooks for a Single Mobile Device

When viewing management information for a single mobile device, you can view a list of eBooks that have the mobile device in the scope.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.

3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.

4. Click the mobile device you want to view eBooks for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.

5. Click the **Management** tab, and then click the **eBooks** category.

   A list of eBooks for the mobile device is displayed.

Viewing Group Memberships for a Single Mobile Device

When viewing management information for a single mobile device, you can view the smart and static group memberships for the device.

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

2. Click **Mobile Devices** at the top of the page.

3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.

4. Click the mobile device you want to view group memberships for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.

5. Click the **Management** tab, and then click the **Mobile Device Groups** category.

   A list of smart mobile device group memberships is displayed.

6. To view the static mobile device group memberships, click **Static Groups**.

   A list of static mobile device group memberships is displayed.

Related Information

For related information, see the following sections in this guide:

- Viewing Smart Mobile Device Group Memberships

  Find out how to view all group memberships for a smart group.

- Viewing Static Mobile Device Group Memberships

  Find out how to view all group memberships for a static group.

Viewing the History for a Single Mobile Device

The JAMF Software Server (JSS) allows you to view the history for a single mobile device. The information you can view includes:

- Management history (completed, pending, and failed management commands)
- User and location history
- Completed, pending, and failed app installations

Viewing Management History for a Single Mobile Device

The management history for a single mobile device allows you to view lists of completed, pending, and failed management commands for the mobile device. The lists include all actions related to the following:

- Sending iOS remote commands
- Installing or removing iOS configuration profiles
- Installing or removing apps
- Installing or removing Provisioning Profiles
- Updating inventory

You can also cancel a pending management command.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view management history for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.
5. Click the **History** tab.

   A list of completed management commands for the mobile device is displayed.
6. To view a list of pending management commands, click **Pending Commands**.

   You can cancel a pending management command by clicking **Cancel** for the command.
7. To view a list of failed management commands, click **Failed Commands**.

Viewing User and Location History for a Single Mobile Device

The user and location history for a single mobile device allows you to view a list of the user and location information associated with the mobile device over time. A record of the current information is added to the list whenever changes are made to the User and Location category in the mobile device’s inventory information.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view user and location history for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.
5. Click the **History** tab, and then click the **User and Location History** category.

   User and location history for the mobile device is displayed.

Viewing App Installations for a Single Mobile Device

You can view the completed, pending, and failed app installations for a single mobile device. You can also cancel pending app installations.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view app installation information for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the mobile devices related to that item.
5. Click the **History** tab, and then click the **Apps** category.

   A list of apps installed on the mobile device is displayed.
6. To view a list of apps that are pending installation, click **Pending Apps**.

   You can cancel a pending installation by clicking **Cancel** for the app.
7. To view a list of apps that failed to install, click **Failed Apps**.

Deleting a Single Mobile Device from the JSS

You can remove a mobile device from your inventory by deleting it from the JAMF Software Server (JSS).

The components installed during enrollment are not removed from the mobile device when it is deleted from the JSS. It is recommended that you unmanage the device before deleting it. (For more information on unmanaging a mobile device, see iOS Remote Commands.)

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.
   On a smartphone, this option is in the pop-up menu.
4. Perform a simple or advanced mobile device search.
   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
5. Click the mobile device you want to delete.
   If you performed a simple search for mobile device applications, you must click **Expand** ⊕ next to an item name to view the mobile devices related to that item.
6. Click **Delete**, and then click **Delete** again to confirm.

Related Information

For related information, see the following section in this guide:

Mass Deleting Mobile Devices
Find out how to mass delete mobile devices from the JSS.

Mobile Device Groups

About Mobile Device Groups

Mobile device groups allow you to organize mobile devices that share similar attributes. You can use these groups as a basis for performing advanced inventory searches and configuring the scope of remote management tasks.

There are two kinds of mobile device groups: smart mobile device groups and static mobile device groups. Smart mobile device groups are based on criteria and have dynamic memberships. Static mobile device groups have fixed memberships that you manually assign.

Related Information

For related information, see the following sections in this guide:

- Smart Mobile Device Groups

  Learn how to create mobile device groups that are based on criteria and have dynamic memberships.
- Static Mobile Device Groups

  Learn how to create mobile device groups that have fixed memberships.

Smart Mobile Device Groups

Smart mobile device groups give you a way to organize mobile devices based on one or more attributes, such as last inventory update, model, and username. These groups have dynamic memberships that are updated each time mobile devices contact the JAMF Software Server (JSS).

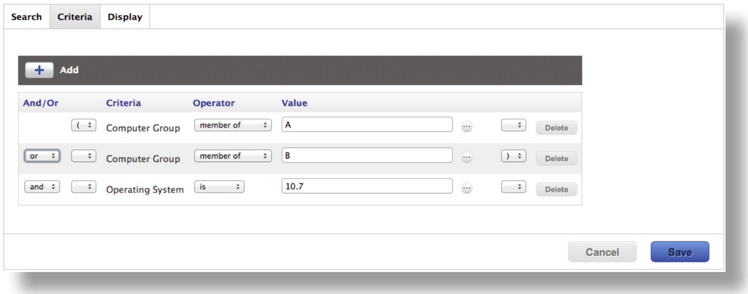
If there is an SMTP server set up in the JSS, you can enable email notifications for the group. This allows email notifications to be sent to JSS users each time the group membership changes. (For information on setting up an SMTP server and enabling email notifications for JSS user accounts, see Integrating with an SMTP Server and Email Notifications.)

After creating a smart mobile device group, you can view its memberships.

Creating a Smart Mobile Device Group

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Smart Mobile Device Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the Mobile Device Group pane to configure basic settings for the group.
   To enable email notifications, select the **Send email notification on membership change** checkbox.
6. Click the **Criteria** tab and add criteria to the group:
   a. Click **Add** + .
   b. Click **Choose** for the criteria you want to add.
      To display additional criteria, click **Choose** for "Other Criteria".
   c. Choose an operator from the **Operator** pop-up menu.
   d. Enter a value in the **Value** field or browse for a value by clicking **Browse** ⋯ .
   e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.

8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.



And/Or		Criteria	Operator	Value		
	(	Computer Group	member of	A		Delete
or		Computer Group	member of	B	)	Delete
and		Operating System	is	10.7		Delete

9. Click **Save**.

   Operations in the group take place in the order they are listed (top to bottom).

   Group memberships are updated each time mobile devices contact the JSS and meet or fail to meet the specified criteria.

   To view the group memberships, click **View**.

Cloning, Editing, or Deleting a Smart Mobile Device Group

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Smart Mobile Device Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the smart mobile device group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the group, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the group, click **Delete.** Then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices the next time they contact the JSS.

Viewing Smart Mobile Device Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Smart Mobile Device Groups**.
   On a smartphone, this option is in the pop-up menu.

4. Click the mobile device group you want to view memberships for.
5. Click **View**.

   A list of group memberships is displayed.

Related Information

For related information, see the following sections in this guide:

- Mobile Device Reports
  Find out how to export the data in group membership lists to different file formats.
- Performing Mass Actions for Mobile Devices
  Find out how to perform mass actions on group memberships.
- Scope
  Learn how to configure scope based on mobile device groups.

Static Mobile Device Groups

Static mobile device groups give you a way to organize mobile devices by assigning them to a group. These groups have fixed memberships that must be changed manually.

After creating a static mobile device group, you can view its memberships.

Creating a Static Mobile Device Group

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Static Mobile Device Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the Mobile Device Group pane to configure basic settings for the group.
6. Click the **Assignments** tab and select the checkbox for each device you want to add.
7. Click **Save**.

Mobile devices become members of the group the next time they contact the JSS.

To view the group memberships, click **View**.

Cloning, Editing, or Deleting a Static Mobile Device Group

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Static Mobile Device Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the group you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the group, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the group, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the group, click **Delete.** Then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices the next time they contact the JSS.

Viewing Static Mobile Device Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Static Mobile Device Groups**.
   On a smartphone, this option is in the pop-up menu.
4. Click the mobile device group you want to view memberships for.
5. Click **View**.

A list of group memberships is displayed.

Related Information

For related information, see the following sections in this guide:

- Mobile Device Reports
  Find out how to export the data in group membership lists to different file formats.
- Performing Mass Actions for Mobile Devices
  Find out how to perform mass actions on group memberships.
- Scope
  Learn how to configure scope based on mobile device groups.

Configuration

iOS Configuration Profiles

iOS configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for mobile devices.

You can use the JAMF Software Server (JSS) to manually create an iOS configuration profile or upload a configuration profile that was created using Apple's tools.

Before creating a configuration profile, you should have basic knowledge of configuration profile payloads and settings, and how they affect mobile devices. For detailed information about each payload and setting, see Apple's Profile Manager documentation at:

https://help.apple.com/profilemanager/mac

Some configuration profile settings are unique to the JSS. For more information on these settings, see the following Knowledge Base article:

Configuration Profiles Reference

There are two different ways to distribute an iOS configuration profile—install it automatically (requires no interaction from the user) or make it available in the Self Service web clip. You can also specify the mobile devices and users to which the profile should be applied (called "scope").

Payload Variables for iOS Configuration Profiles

There are several payload variables that you can use to populate settings in an iOS configuration profile with attribute values stored in the JSS. This allows you to create payloads containing information about each mobile device and user to which you are distributing the profile.

To use a payload variable, enter the variable into any text field when creating a profile in the JSS. When the profile is installed on a mobile device, the variable is replaced with the value of the corresponding attribute in the JSS.

Variable	Mobile Device Information
$DEVICENAME	Mobile Device Name
$SERIALNUMBER	Serial Number
$UDID	UDID
$USERNAME	Username
$FULLNAME or $REALNAME	Full Name
$EMAIL	Email Address
$PHONE	Phone Number
$ROOM	Room
$POSITION	Position
$MACADDRESS	MAC Address
$EXTENSIONATTRIBUTE_<#>	Value for any LDAP attribute

Note: An $EXTENSIONATTRIBUTE_<#> variable is generated each time you create an extension attribute with the "LDAP Attribute Mapping" input type. For more information, see Mobile Device Extension Attribute Input Types.

Manually Creating an iOS Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General payload to configure basic settings for the profile, including a distribution method.
6. If you chose to make the profile available in the Self Service web clip, do the following:
   a. Choose a **Security** setting.
   b. Click the **Self Service Web Clip** tab, and specify an icon to display in the Self Service web clip.
   c. Click the **Options** tab to continue configuring the profile.
7. Use the rest of the payloads to configure the settings you want to apply.
8. Click the **Scope** tab and configure the scope of the profile.
   For more information, see Scope.
9. Click **Save**.

The profile is distributed to mobile devices in the scope the next time they contact the JSS.

Uploading an iOS Configuration Profile

You can create an iOS configuration profile by uploading a profile that was created using Apple’s tools.

> ***Note:*** Some payloads and settings configured with Apple's tools are not displayed in the JSS. Although you cannot view or edit these payloads, they are still applied to mobile devices.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Upload** ↑ and upload the configuration profile (.mobileconfig).
5. Use the General payload to configure basic settings for the profile, including a distribution method.
6. If you chose to make the profile available in the Self Service web clip, do the following:
   a. Choose a **Security** setting.
   b. Click the **Self Service Web Clip** tab, and specify an icon to display in the Self Service web clip.
   c. Click the **Options** tab to continue configuring the profile.
7. Use the rest of the payloads to configure or edit settings as needed.
8. Click the **Scope** tab and configure the scope of the profile.
   For more information, see Scope.
9. Click **Save**.

The profile is distributed to mobile devices in the scope the next time they contact the JSS.

Cloning, Editing, or Deleting an iOS Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click the configuration profile you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the profile, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the profile, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the profile, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices in the scope the next time they contact the JSS.

Downloading an iOS Configuration Profile

If you want to view the contents of an iOS configuration profile for troubleshooting purposes, you can download the profile (.mobileconfig) from the JSS.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click the configuration profile you want to download.
5. Click **Download**.

The profile downloads immediately.

Related Information

For related information, see the following sections in this guide:

- Payload Capabilities for iOS Configuration Profiles
  Learn about the payload capabilities of each iOS version.
- Viewing the Pending Management Commands for a Single Mobile Device
  Find out how to view and cancel pending iOS configuration profile installations and removals for a single mobile device.
- Viewing Configuration Profiles for a Single Mobile Device
  Find out how to view the iOS configuration profiles in the scope for a single mobile device.
- Viewing Management History for a Single Mobile Device
  Find out how to view all completed, pending, and failed iOS configuration profile installations and removals for a single mobile device.

Payload Capabilities for iOS Configuration Profiles

The Casper Suite can be used to deploy iOS configuration profiles to the following types of mobile devices:

- iPads with iOS 4 or later
- iPhones with iOS 4 or later
- iPod touches with iOS 4 or later
- Apple TV devices with iOS 7 or later

The following table provides an overview of the payload capabilities by iOS version:

Payload	iOS 4	iOS 5	iOS 6	iOS 7
General	✓	✓	✓	✓
Passcode	✓	✓	✓	✓
Restrictions[1]	✓	✓	✓	✓
Wi-Fi[1]	✓	✓	✓	✓
VPN[1]	✓	✓	✓	✓
Mail	✓	✓	✓	✓
Exchange ActiveSync	✓	✓	✓	✓
LDAP	✓	✓	✓	✓
Calendar	✓	✓	✓	✓
Contacts	✓	✓	✓	✓
Subscribed Calendars	✓	✓	✓	✓
Web Clips	✓	✓	✓	✓
Certificate	✓	✓	✓	✓
SCEP	✓	✓	✓	✓
APN		✓	✓	
Cellular				✓
Single App Mode			✓	✓
Global HTTP Proxy				✓
Single Sign-On				✓
AirPlay				✓

Payload	iOS 4	iOS 5	iOS 6	iOS 7
AirPrint				✓
Font				✓
Web Content Filter				✓

Notes:

1. The Restrictions, Wi-Fi, and VPN payloads have additional settings that are specific to iOS 7. For more information on these payloads, see Apple's Configuration Profile Key Reference.

Related Information

For related information, see the following section in this guide:

iOS Configuration Profiles
Learn about iOS configuration profiles and how to create them.

Security Management

iOS Remote Commands

The iOS remote commands available in the JAMF Software Server (JSS) allow you to remotely perform the following tasks on a mobile device:

- Manage security by locking, wiping, or clearing the passcode on the device.
- Update inventory.
- Send a blank push notification.
- Manage settings for voice or data roaming (only for devices with cellular capability).

You can send an iOS remote command to a single mobile device.

Note: The remote commands available for a particular device vary depending on the type of device and the iOS version. For information on the iOS remote commands available by device type and iOS version, see Mobile Device Management Capabilities.

The following table describes the iOS remote commands that you can send from the JSS:

iOS Remote Command	Description
Update Inventory	Prompts the mobile device to contact the JSS and update its inventory
Lock Device	Locks the mobile device (Optional) Displays a message on the mobile device when it locks. This message is only sent if the mobile device has a passcode. (Optional) Displays a phone number on the mobile device when it locks. The phone number is only displayed if the mobile device has a passcode. If the mobile device has a passcode, the user must enter it to unlock the device.
Clear Passcode	Removes the passcode from the mobile device If a configuration profile with a Passcode payload is installed on the device, the user is prompted to create a new passcode.

iOS Remote Command	Description
Wipe Device	Permanently erases all data on the device and deactivates the device ***Note:*** Wiping a device does not remove the device from the JSS or change its inventory information. To restore the device to the original factory settings, you must manually reactivate the device.
Unmanage Device	Stops communication between the mobile device and the JSS, which means you can no longer perform management tasks on the device When you unmanage a device, the following items are removed from the device: ▪ MDM profile ▪ Device certificate ▪ Self Service web clip ▪ Any configuration profiles that were distributed with the Casper Suite ▪ Any managed apps that were distributed with the **Remove app when MDM profile is removed** checkbox selected ***Note:*** Although an unmanaged device can no longer submit inventory, its inventory record remains in the JSS.
Send Blank Push	Sends a blank push notification, prompting the device to check in with Apple Push Notification service (APNs)
Enable Voice Roaming **Disable Voice Roaming** **Enable Data Roaming** **Disable Data Roaming**	Enables/disables voice or data roaming on the device ***Note:*** Disabling voice roaming automatically disables data roaming.

Sending an iOS Remote Command

Log in to the JSS with a web browser.

1. Click **Mobile Devices** at the top of the page.
2. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
3. Click the mobile device you want to send the iOS remote command to.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** + next to an item to view the devices related to that item.

4. Click the **Management** tab, and then click the button for the remote command that you want to send.

   If you are sending a Lock Device command, enter a lock message and phone number if desired, and then click **Lock Mobile Device**.

   The remote command runs on the mobile device the next time the device contacts the JSS.

Viewing the Status of iOS Remote Commands

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device you want to view iOS remote commands for.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the devices related to that item.
5. Click the **History** tab.
6. Use the Management History pane to view completed, pending, or failed commands.

Canceling an iOS Remote Command

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Perform a simple or advanced mobile device search.

   For more information, see Simple Mobile Device Searches or Advanced Mobile Device Searches.
4. Click the mobile device for which you want to cancel an iOS remote command.

   If you performed a simple search for an item other than mobile devices, you must click **Expand** ⊕ next to an item to view the devices related to that item.
5. Click the **History** tab, and then click **Pending Commands**.
6. Find the command you want to cancel, and click **Cancel** across from it.

Self Service

Self Service Web Clip

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

By default, the Self Service web clip is installed on all managed mobile devices except Apple TV devices.

Configuring the Self Service Web Clip Settings

The Self Service Web Clip settings in the JSS allow you to do the following:

- Install or uninstall the Self Service web clip on managed mobile devices.
- Require users to log in to the Self Service web clip with an LDAP directory account.
- Display or hide the **Install All** button for in-house apps.
- Display the following updates in the Self Service web clip:
    - MDM profile updates
    - App Store app updates
    - In-house app updates

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙.
3. Click **Mobile Device Management**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Self Service Web Clip** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

The changes are applied the next time mobile devices contact the JSS.

Related Information

For related information, see the following sections in this guide:

- Integrating with LDAP Directory Services

  Find out how to add an LDAP server to the JSS so you can require users can log in to the Self Service web clip using their LDAP directory accounts.
- iOS Configuration Profiles

  Find out how to make iOS configuration profiles available in the Self Service web clip.
- App Store Apps

  Find out how to make App Store apps available in the Self Service web clip.
- In-House Apps

  Find out how to make in-house apps available in the Self Service web clip.
- eBooks Availble in the iBookstore

  Find out how to make iBookstore eBooks available in the Self Service web clip.
- In-House eBooks

  Find out how to make in-house eBooks available in the Self Service web clip.

For related information, see the following Knowledge Base articles:

- Customizing the Self Service Web Clip Icon

  Find out how to display a custom icon for the Self Service web clip.
- Distributing Updated MDM Profiles

  Find out why you may want to make updated MDM profiles available in the Self Service web clip and how to do so.

App Distribution

Understanding Unmanaged and Managed Apps

The JAMF Software Server (JSS) 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 configure some additional management settings.

The primary advantages to managing an app are that you can prompt users to install the app, and you can remove the app from mobile devices that have it installed.

The following table shows the differences between an unmanaged app and a managed app:

	Unmanaged app	Managed app
Distribution Methods		
Make available in Self Service web clip	✓	✓
Prompt users to install		✓
Removal Options		
Remove from Self Service web clip	✓	✓
Remove from mobile devices		✓
Additional Management Options		
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 kind of app

  The app must be an in-house app, an App Store app with VPP codes, or a free App Store app.

- The mobile devices to which you distribute the app

  Mobile devices must have iOS 5 or later and an MDM profile that supports app management.

  Mobile devices that have iOS 5 or later when they are enrolled with the JSS automatically obtain an MDM profile that supports app management. Managed iOS 4 devices that are upgraded to iOS 5 or later do not obtain this profile. For instructions on distributing an updated MDM profile that supports app management, see the following Knowledge Base article:

  Distributing Updated MDM Profiles

- The method you use to distribute the app

  When configuring the app for distribution in the JSS, you must choose one of the following distribution methods:

  - Prompt users to install
  - Make available in Self Service web clip and manage when possible

  For more information, see Understanding App Distribution Methods.

Understanding App Distribution Methods

The JAMF Software Server (JSS) allows you to distribute apps to mobile 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.

The distribution method that you choose affects the following:

- 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 mobile devices that support managed apps and mobile devices that do not.

On mobile 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 mobile devices.

On mobile 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 mobile devices that support managed apps and mobile devices that do not.

On mobile 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 mobile devices that have it installed and from the Self Service web clip.

On mobile 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 mobile 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.

Related Information

For related information, see the following sections in this guide:

- In-House Apps

  Find out how to distribute in-house apps.
- App Store Apps

  FInd out how to distribute App Store apps.
- Understanding Unmanaged and Managed Apps

  Learn about unmanaged and managed apps. Also, find out which mobile devices support managed apps.

Provisioning Profiles

Provisioning profiles (.mobileprovision) authorize the use of in-house apps. For an in-house app to work, the provisioning profile that authorizes it must be installed on mobile devices.

If the provisioning profile that authorizes an in-house app is not bundled in the app archive (.ipa) file, you must upload the profile to the JAMF Software Server (JSS) before distributing the app.

Uploading a Provisioning Profile

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Provisioning Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click **Upload** ↑ and upload the provisioning profile.
5. Enter a display name for the profile.
6. Click **Save**.

Editing or Deleting a Provisioning Profile

If a provisioning profile expires, you can edit the provisioning profile record in the JSS and replace the existing profile with the new version.

Deleting a provisioning profile removes it from mobile devices that have it installed.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Provisioning Profiles**.
   On a smartphone, this option is in the pop-up menu.
4. Click the provisioning profile you want to edit or delete.
5. Do one of the following:
   - To edit the profile, click **Edit** and upload the new profile. Then click **Save**.
   - To delete the profile, click **Delete** and then click **Delete** again to confirm.

The edit or delete action is applied to mobile devices with the profile installed the next time they contact the JSS.

Downloading a Provisioning Profile

If you no longer have access to the original .mobileprovision file for a provisioning profile in the JSS, you can download it from the JSS.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Provisioning Profiles**.

   On a smartphone, this option is in the pop-up menu.
4. Click the provisioning profile you want to download.
5. Click **Download**.

The profile is downloaded immediately.

Related Information

For related information, see the following sections in this guide:

- In-House Apps

  Find out how to distribute an in-house app and its provisioning profile.
- Viewing and Editing Inventory Information for a Single Mobile Device

  You can view the provisioning profiles installed on a single mobile device by viewing the device's inventory information in the JSS.
- Viewing the Pending Management Commands for a Single Mobile Device

  Find out how to view and cancel pending provisioning profile installations and removals for a single mobile device.
- Viewing Management History for a Single Mobile Device

  Find out how to view the completed, pending, and failed provisioning profile installations and removals for a single mobile device.

In-House Apps

In-house apps are enterprise apps developed through Apple's iOS Developer Enterprise Program. The JAMF Software Server (JSS) allows you to distribute in-house apps to mobile devices. After an in-house app has been distributed, you can also use the JSS to distribute an update or remove the app from mobile devices.

For more information on Apple's iOS Developer Enterprise Program or to register, visit the following website:

https://developer.apple.com/programs/ios/enterprise/

Before you distribute an in-house app, it is important to consider where the app will be hosted. There are three hosting locations you can use for in-house apps:

- **Distribution points**—If your master distribution point is a JDS instance or the cloud distribution point, you can use the JSS to upload the app to the master distribution point.

Note: Apps cannot be replicated to file share distribution points.

- **jamfsoftware database**—If your master distribution point is a file share distribution point, you can use the JSS to upload the app and host it in the jamfsoftware database.
- **Web server**—To use this location, the app must be hosted on a web server before you distribute it. Then, when you distribute the app, you specify the URL where it is hosted.

  If your master distribution point is a file share distribution point, it is recommended that you host large apps on a web server.

When you distribute an in-house app, you configure settings for the app, such as the hosting location, distribution method, and whether to manage the app. (For more information, see Understanding Unmanaged and Managed Apps and Understanding App Distribution Methods.) If you have an iOS configuration profile with a Per-App VPN connection, you can also map a managed app to the Per-App VPN connection on mobile devices. Then, you specify the users and mobile devices that should receive it (called "scope").

Managed App Configuration

You can configure preferences and settings in the JSS for a managed app before distributing it to mobile devices.

There are also several variables that you can also use to populate settings in a managed app with attribute values stored in the JSS. This allows you to create preferences containing information about each mobile device and user to which you are distributing the app.

When the app is installed on a mobile device, the variable is replaced with the value of the corresponding attribute in the JSS.

Variable	Mobile Device Information
`$DEVICENAME`	Mobile Device Name
`$SERIALNUMBER`	Serial Number
`$UDID`	UDID
`$USERNAME`	Username
`$FULLNAME` or `$REALNAME`	Full Name
`$EMAIL`	Email Address
`$PHONE`	Phone Number
`$ROOM`	Room
`$POSITION`	Position
`$MACADDRESS`	MAC Address
`$JSSID`	JSS ID

Requirements

To distribute an in-house app, you need:

- The bundle identifier for the app (located in the PLIST file for the app)
- The archived app file (.ipa) 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 or bundled in the archived app file (For more information, see Provisioning Profiles.)

Managed App Configuration only applies to mobile devices with iOS 7 or later.

Per-App VPN connections are only applied to mobile devices with iOS 7 or later.

Distributing an In-House App

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Select **In-house app** and click **Next**.

6. Use the General pane to configure settings for the app, including the distribution method and hosting location.

   If you choose "Distribution Points" or "jamfsoftware database" from the **Hosting Location** pop-up menu, be sure to upload the archived app file.

7. Click the **Scope** tab and configure the scope of the app.

   For more information, see Scope.

8. (Optional) Click the **Self Service Web Clip** tab and configure the way the app is displayed in the Self Service web clip.

   > ***Note:*** The **Self Service Web Clip** tab is only displayed if "Make Available in Self Service Web Clip" is chosen in the **Distribution Method** pop-up menu.

9. (Optional) Click the **App Configuration** tab and configure the preferences as needed.

   > ***Note:*** The **App Configuration** tab is only displayed if the **Manage app when possible** checkbox is selected.

10. Click **Save**.

The app is distributed the next time mobile devices in the scope contact the JSS.

Cloning, Editing, or Deleting an In-House App

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.

   On a smartphone, this option is in the pop-up menu.

4. Click the app you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the app, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the app, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the app, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices in the scope the next time they contact the JSS.

Distributing an In-House App Update

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.

3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click the app you want to update.
5. Do one of the following:
   - To distribute an update for an in-house app that is hosted on a web server, upload the new archived app file to the web server and update app URL.
   - To distribute an update for an in-house app that is hosted on distribution points or in the jamfsoftware database, upload the new archived app file using the JSS.
6. Enter the new version number for the app.

> ***Important:*** Do not change the bundle identifier. The JSS uses the existing bundle identifier to distribute the update.

7. Click **Save**.

The update is distributed the next time mobile devices in the scope contact the JSS.

Removing an In-House App from Mobile Devices

To remove an in-house app from one or more devices, you remove the mobile device(s) from the scope.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click the app you want to remove.
5. Click the **Scope** tab and remove mobile devices from the scope as needed.
   For more information, see Scope.
6. Click **Save**.

The app is removed the next time the mobile devices contact the JSS.

Related Information

For related information, see the following sections in this guide:

- App Store Apps
  Find out how to distribute, update, and remove App Store apps.
- Viewing Apps for a Single Mobile Device
  Find out how to view the apps in the scope of a single mobile device.

- Viewing the Pending Management Commands for a Single Mobile Device

  Find out how to view and cancel pending app installations and removals for a single mobile device.

- Viewing App Installations for a Single Mobile Device

  Find out how to view the completed, pending, and failed app installations for a single mobile device. Also, find out how to cancel pending app installations.

- iOS Configuration Profiles

  You can create an iOS configuration profile with a Per-App VPN connection.

For related information, see the following Knowledge Base article:

Hosting In-House eBooks and Apps on a Tomcat Instance
Find out how to hosting in-house apps on the Tomcat instance that hosts the JSS.

App Store Apps

The JAMF Software Server (JSS) allows you to distribute App Store apps to mobile devices. After an App Store app has been distributed, you can also use the JSS to distribute an update or remove the app from mobile devices.

When you distribute an App Store app, you add it to the JSS and configure settings for the app, such as the distribution method and whether to manage the app. (For more information, see Understanding Unmanaged and Managed Apps and Understanding App Distribution Methods.) If you have an iOS configuration profile with a Per-App VPN connection, you can also map a managed app to the Per-App VPN connection on mobile devices. Then, you specify the users and mobile devices that should receive it (called "scope").

You can also associate Volume Purchase Program (VPP) codes with an App Store app and track their redemption.

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/

Managed App Configuration

You can configure preferences and settings in the JSS for a managed app before distributing it to mobile devices.

There are also several variables that you can also use to populate settings in a managed app with attribute values stored in the JSS. This allows you to create preferences containing information about each mobile device and user to which you are distributing the app.

When the app is installed on a mobile device, the variable is replaced with the value of the corresponding attribute in the JSS.

Variable	Mobile Device Information
`$DEVICENAME`	Mobile Device Name
`$SERIALNUMBER`	Serial Number
`$UDID`	UDID
`$USERNAME`	Username
`$FULLNAME` or `$REALNAME`	Full Name
`$EMAIL`	Email Address

Variable	Mobile Device Information
$PHONE	Phone Number
$ROOM	Room
$POSITION	Position
$MACADDRESS	MAC Address
$JSSID	JSS ID

Requirements

To install an App Store app or update, users must enter an Apple ID.

To associate VPP codes with an App Store app, you need an Excel spreadsheet (.xls) that contains VPP codes for the app.

Managed App Configuration only applies to mobile devices with iOS 7 or later.

Per-App VPN connections are only applied to mobile devices with iOS 7 or later.

Distributing an App Store App

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Select **App Store app** and click **Next**.
6. Do one of the following:
   - To add the app by browsing the App Store, enter the name of the app, choose an App Store country, and click **Next**. Then click **Add** for the app you want to add.
   - To add the app by uploading a VPP code spreadsheet, click **Choose File** and upload the Excel spreadsheet (.xls) that contains VPP codes for the app.
   - To add the app by manually entering information about it, click **Enter Manually**.
7. Use the General pane to configure settings for the app, including the distribution method.
8. Click the **Scope** tab and configure the scope of the app.
   For more information, see Scope.

9. (Optional) Click the **Self Service Web Clip** tab and configure the way the app is displayed in the Self Service web clip.

> ***Note:*** The **Self Service Web Clip** tab is only displayed if "Make Available in Self Service Web Clip" is chosen in the **Distribution Method** pop-up menu.

10. (Optional) If you have not already uploaded a VPP code spreadsheet, click the **VPP Codes** tab and upload the Excel spreadsheet (.xls) that contains VPP codes for the app.

> ***Note:*** The **VPP Codes** tab is only displayed if the **Free** checkbox is not selected.

11. (Optional) Click the **App Configuration** tab and configure the preferences as needed.

> ***Note:*** The **App Configuration** tab is only displayed if the **Manage app when possible** checkbox is selected.

12. Click **Save**.

The app is distributed the next time mobile devices in the scope contact the JSS.

Cloning, Editing, or Deleting an App Store App

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click the app you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the app, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the app, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the app, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices in the scope the next time they contact the JSS.

Distributing an App Store App Update

To distribute an update for an App Store app, you update the version number and URL for the app in the JSS.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.

3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click the app you want to update.
5. Enter the new version number and URL.

   Important: Do not change the bundle identifier. The JSS uses the existing bundle identifier to distribute the update.

6. Click **Save**.

The update is distributed the next time mobile devices in the scope contact the JSS.

Removing an App Store App from Mobile Devices

To remove an App Store app from one or more devices, you remove the mobile device(s) from the scope.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
   On a smartphone, this option is in the pop-up menu.
4. Click the app you want to remove.
5. Click the **Scope** tab and remove mobile devices from the scope as needed.
   For more information, see Scope.
6. Click **Save**.

The app is removed the next time the mobile devices contact the JSS.

Related Information

For related information, see the following sections in this guide:

- In-House Apps
  Find out how to distribute, update, and remove in-house apps.
- Viewing and Editing Inventory Information for a Single Mobile Device
  You can view the apps installed on a single mobile device by viewing the device's inventory information in the JSS.
- Viewing Apps for a Single Mobile Device
  Find out how to view the apps in the scope of a single mobile device.

- Viewing the Pending Management Commands for a Single Mobile Device

  Find out how to view and cancel pending app installations and removals for a single mobile device.
- Viewing App Installations for a Single Mobile Device

  Find out how to view the completed, pending, and failed app installations for a single mobile device. Also, find out how to cancel pending app installations.
- iOS Configuration Profiles

  You can create an iOS configuration profile with a Per-App VPN connection.

eBook Distribution

In-House eBooks

In-house eBooks are eBooks that are not available from the iBookstore. The JAMF Software Server (JSS) allows you to distribute in-house eBooks to 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.

Before you distribute an in-house eBook, it is important to consider where the eBook will be hosted. There are two hosting locations that you can use for in-house eBooks:

- **Distribution points**—This hosting location is only available if your master distribution point is a JDS instance or the cloud distribution point. To use this hosting location, you upload the eBook to the master distribution point when configuring settings for the eBook in the JSS.

Note: eBooks cannot be replicated to file share distribution points.

- **Web server**—This hosting location is always available, regardless of what type of distribution point the master is. To use this hosting location, the eBook must be hosted on a web server before you distribute it. Then, when you distribute the eBook, you specify the URL where it is hosted.

When you distribute an in-house eBook, you configure settings for the eBook. Then, you specify the users and mobile devices that should receive it (called "scope").

Requirements

To distribute an in-house eBook, the eBook must be one of the following types of files:

- ePub file (.epub)
- iBooks file (.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 an In-House eBook

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **eBooks**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Select **In-house eBook** and click **Next**.
6. Use the General pane to configure settings for the app, including the display name.

   If your master distribution point is a JDS instance or the cloud distribution point and you choose "Distribution Points" from the **Hosting Location** pop-up menu, be sure to upload the eBook file.
7. Click the **Scope** tab and configure the scope of the eBook.

   For more information, see Scope.
8. Click the **Self Service Web Clip** tab and configure the way the eBook is displayed in the Self Service web clip.
9. Click **Save**.

The eBook is distributed the next time mobile devices in the scope contact the JSS.

Cloning, Editing, or Deleting an In-House eBook

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **eBooks**.

   On a smartphone, this option is in the pop-up menu.
4. Click the eBook you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the eBook, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the eBook, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the eBook, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices in the scope the next time they contact the JSS.

Related Information

For related information, see the following sections in this guide:

- eBooks Availble in the iBookstore

  Find out how to distribute eBooks that are available in the iBookstore.
- Viewing eBooks for a Single Mobile Device

  Find out how to view the eBooks in the scope of a single mobile device.

For related information, see the following Knowledge Base article:

Hosting In-House eBooks and Apps on a Tomcat Instance
Find out how to hosting in-house eBooks on the Tomcat instance that hosts the JSS.

eBooks Available in the iBookstore

The JAMF Software Server (JSS) allows you to distribute eBooks that are available in the iBookstore. Distributing an eBook displays it in the Self Service web clip for users to install. After users install an eBook, they can view it using Apple’s iBooks app.

When you distribute an eBook available in the iBookstore, you add it to the JSS and configure settings for the eBook. Then, you specify the users and mobile devices that should receive it (called “scope”).

> ***Note:*** Teachers can also distribute eBooks (ePub format only) to classes using Casper Focus v9.1 or later. This automatically adds the eBook to the JSS and distributes the eBook to the student mobile devices in the class(es) that the teacher specifies. For more information on Casper Focus features, see the *Casper Focus User Guide*. This guide is available at:
>
> http://www.jamfsoftware.com/product-documentation/administrators-guides

You can also associate Volume Purchase Program (VPP) codes with an eBook from the iBookstore and track their redemption.

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/

Requirements

To distribute an eBook available in the iBookstore, the eBook must be an ePub file (.epub) or iBooks file (.ibooks).

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 an eBook Available in the iBookstore

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **eBooks**.
   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .

5. Select **eBook available in the iBookstore** and click **Next**.

6. Do one of the following:
   - To add the eBook by browsing the iBookstore, enter the name of the eBook, choose an iBookstore country, and click **Next**. Then click **Add** for the eBook you want to add.
   - To add the eBook by uploading a VPP code spreadsheet, click **Choose File** and upload the Excel spreadsheet (.xls) that contains VPP codes for the eBook.
   - To add the eBook by manually entering information about it, click **Enter Manually**.

Note: iBooks files (.ibooks) may need to be added manually.

7. Use the General pane to configure distribution settings for the eBook, including the display name.

8. Click the **Scope** tab and configure the scope of the eBook.

   For more information, see Scope.

9. Click the **Self Service Web Clip** tab and configure the way the eBook is displayed in the Self Service web clip.

10. (Optional) If you have not already uploaded a VPP code spreadsheet, click the **VPP Codes** tab and upload the Excel spreadsheet (.xls) that contains VPP codes for the eBook.

Note: The **VPP Codes** tab is only displayed if the **Free** checkbox is not selected.

11. Click **Save**.

The eBook is distributed the next time mobile devices in the scope contact the JSS.

Cloning, Editing, or Deleting an eBook Available in the iBookstore

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

2. Click **Mobile Devices** at the top of the page.

3. Click **eBooks**.

   On a smartphone, this option is in the pop-up menu.

4. Click the eBook you want to clone, edit, or delete.

5. Do one of the following:
   - To clone the eBook, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the eBook, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the eBook, click **Delete** and then click **Delete** again to confirm.

The clone, edit, or delete action is applied to mobile devices in the scope the next time they contact the JSS.

Related Information

For related information, see the following sections in this guide:

- In-House eBooks

  Find out how to distribute in-house eBooks.
- Viewing eBooks for a Single Mobile Device

  Find out how to view the eBooks in the scope of a single mobile device.

Casper Focus

About Casper Focus

Casper Focus is designed to be used by teachers in the classroom. It gives teachers control over the devices used during class time by allowing the teacher to "focus" the devices on a single app. Focusing a device locks it on the app, preventing students from accessing any other screens or applications. Teachers can also switch the focus from one app to another, or remove the focus from student devices.

In addition to focusing student devices, teachers can also perform the following actions in Casper Focus:

- Clear passcodes on student devices.
- Use AirPlay Mirroring to show the screen of a student device on Apple TV.
- Distribute eBooks (ePub format only) so that students can install the eBooks on their devices from the Self Service web clip.

Casper Focus is available for free from the App Store.

Related Information

For related information, see the following sections in this guide:

- Preparing to Use Casper Focus

  Learn how to prepare Casper Focus for teachers to use in the classroom.
- Classes

  Learn how to create classes in the JSS so teachers can control student devices using Casper Focus.

For instructions on how to use Casper Focus in the classroom, see the *Casper Focus User Guide*. This guide is available at:

http://www.jamfsoftware.com/product-documentation/administrators-guides

Preparing to Use Casper Focus

Before teachers can use Casper Focus, you need to prepare it for use in the classroom.

Device Requirements

You must ensure that teacher and student mobile devices meet the minimum requirements for use, as well as the feature-specific device requirements for each Casper Focus feature that teachers plan to use.

Minimum Device Requirements

Teacher device:

- iPad, iPhone, or iPod touch with iOS 5.1.1 or later

Student device:

- iPad, iPhone, or iPod touch with iOS 5.1.1 or later
- Managed by the Casper Suite v8.7 or later

Feature-Specific Device Requirements

The following table shows the feature-specific device requirements that must be met to perform Casper Focus actions on student mobile devices. These requirements are in addition to the minimum device requirements.

	Student Device Requirements	**Other Requirements**
Focus on App	• iOS 6 or later • Supervised by Apple Configurator	--
Clear Passcodes	(Minimum requirements only)	--
Mirror Device on Apple TV	• iOS 7 or later • Managed by the Casper Suite v9.1 or later	Apple TV with iOS 7 or later, managed by the Casper Suite v9.1 or later
Distribute eBooks	• Managed by the Casper Suite v9.1 or later • Self Service web clip installed • For students to install an eBook (ePub format only) that was distributed using Casper Focus, the student device must have iOS 4 or later and iBooks 1.0 or later	--

For more information on Casper Focus features, see the *Casper Focus User Guide*. This guide is available at:

http://www.jamfsoftware.com/product-documentation/administrators-guides

Before Using Casper Focus

In addition to ensuring that mobile devices meet the requirements for using Casper Focus, you also need to perform the following tasks to allow teachers to use Casper Focus:

- **Create classes in the JSS**—The classes you create in the JAMF Software Server (JSS) allow teachers to use Casper Focus to control student devices during class time. (For more information, see Classes.)
- **Preconfigure the connection to the JSS**—Casper Focus must be able to connect to the JSS to work. To do this, the JSS URL setting in Casper Focus must be populated with the JSS URL. With this setting preconfigured, teachers can log in and use Casper Focus without having to manually configure the JSS URL themselves.

  For more information on preconfiguring the JSS URL, see the following Knowledge Base article:

  Configuring Server Settings for Casper Focus
- **(Optional) Add an LDAP server to the JSS**—Integrating with an LDAP directory service allows teachers to log in to Casper Focus using the username and password for their LDAP directory account. (For more information, see Integrating with LDAP Directory Services.)

  If you do not have an LDAP server set up in the JSS, teachers can log in to Casper Focus with a JSS user account.
- **(Optional) Specify AirPlay passwords for Apple TV devices**—If teachers will be mirroring student devices on Apple TV using Casper Focus and the Apple TV devices are configured with AirPlay passwords, you will need to specify the AirPlay password for each Apple TV by editing its inventory information in the JSS. (For more information, see Viewing and Editing Inventory Information for a Single Mobile Device.)

Classes

For a teacher to control student devices using Casper Focus, a class that specifies the teacher(s), student devices, and meeting times of the class (optional) must exist in the JSS.

When you create a class, you specify the following information:

- A display name for the class
- The username for each teacher

  Teacher usernames can be usernames for JSS user accounts or, if you have an LDAP server set up in the JSS, LDAP directory accounts. (For more information on setting up an LDAP server, see Integrating with LDAP Directory Services.)
- The method to use to assign student devices to the class

  You can use the username associated with each student's mobile device, or a smart or static mobile device group that contains the devices used in the class.
- The student devices to assign to the class
- (Optional) Meeting times for the class (times/days that the class takes place)

  Specifying meeting times allows teachers to access the class in Casper Focus during the scheduled meeting times only.
- (Optional) Apple TV devices to assign to the class

  With one or more Apple TV devices assigned to a class, the teacher can use AirPlay Mirroring to show the screen of a student device on Apple TV.

After you create a class in the JSS, the teacher assigned to the class can log in to Casper Focus and control the student devices in that class.

Creating a Class

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Classes**.

   On a smartphone, this option is in the pop-up menu.
4. Click **New** + .
5. Use the General pane to configure settings for the class, such as the teacher usernames, method, and student devices.
6. (Optional) Click the **Meeting Times** tab and specify the times and days the class meets.
7. (Optional) Click the **Apple TV** tab and add targets to assign Apple TV devices to the class.
8. Click **Save**.

Cloning, Editing, or Deleting a Class

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Classes**.
   On a smartphone, this option is in the pop-up menu.
4. Click the class you want to clone, edit, or delete.
5. Do one of the following:
   - To clone the class, click **Clone** and make changes as needed. Then click **Save**.
   - To edit the class, click **Edit** and make changes as needed. Then click **Save**.
   - To delete the class, click **Delete.** Then click **Delete** again to confirm.

The clone, edit, or delete action is applied to Casper Focus the next time the app is launched or the Classes are refreshed in the sidebar.

Related Information

For related information, see the following section in this guide:

Preparing to Use Casper Focus
Learn how to prepare Casper Focus for teachers to use in the classroom.