Casper Suite Administrator's Guide

Version 9.100.0

jamf

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 at:
  https://www.jamf.com/resources/casper-suite-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:
  https://www.jamf.com/resources/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:
  https://www.jamf.com/resources/manually-installing-the-jamf-software-server/

- 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 at:
  https://www.jamf.com/resources/product-documentation/quickstart-guides/

- Technical papers
  Jamf 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:
  https://www.jamf.com/resources/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 Casper Suite administrators 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://www.jamf.com/jamf-nation/

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 or website. Focusing a device locks it on the app or website, preventing students from accessing any other screens or content on the device.

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 Self Service.

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.

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

```
/usr/local/jamf/bin/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/local/jamf/bin/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 Mac 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://www.jamf.com/jamf-nation/my/products

Management Action

The Management Action application displays User Interaction messages in Notification Center. It is stored in the following location on managed computers:

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

Recon

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

Self Service for macOS

The Self Service application allows users to browse and run policies, install configuration profiles, Mac App Store apps and eBooks, 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, configuration profile, Mac App Store app, or eBook 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 for iOS

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

There are two kinds of Self Service for iOS devices: the Self Service Mobile app and the Self Service web clip. Self Service Mobile can be installed on devices with iOS 7 or later. By default, Self Service Mobile is installed on all managed mobile devices except Apple TV devices and personally owned devices.

Self Service Mobile for iOS is available for free from the App Store.

Self Service Mobile for Android

Self Service Mobile for Android is used in conjunction with personal device profiles to enroll and manage personally owned Android devices. Users install Self Service Mobile for Android from Google Play during user-initiated enrollment. After enrollment, Self Service Mobile must remain installed on an enrolled Android device to keep the device managed by the JSS.

Self Service Mobile for Android is available for free from Google Play.

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) using the latest version of Transport Layer Security (TLS) the operating system is capable of using. The following table shows the TLS version capabilities for the macOS and iOS operating systems:

TLS Version	macOS Version						iOS Version						
	10.7	10.8	10.9	10.10	10.11	10.12	4	5	6	7	8	9	10
1.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1.1			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
1.2			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓

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 macOS. For more information, go to:
http://openssh.com/

Transport Layer Security (TLS)

TLS is a security protocol for Internet communication. For more information, go to:
http://tools.ietf.org/html/rfc5246

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.

In the JSS, you can choose to use a built-in CA, integrate with a trusted third-party CA (Symantec), or configure your own PKI if you have access to an external CA that supports the Simple Certificate Enrollment Protocol (SCEP). The certificate authorities can be used to issue certificates to both computers and mobile devices.

Note: An external CA can also be used to issue certificates to computers, but this is not enabled by default. For more information, contact Jamf Support.

For more information on certificate authorities in the JSS, see PKI Certificates.

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 computers and mobile devices each time they communicate with the JSS.
- **CA Certificate**—This certificate establishes trust between the CA and computers, and between the CA and mobile devices.
- **Signing Certificate**—This certificate is used to sign messages passed between the JSS and Mac 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).

- **Anchor Certificate**—This certificate allows mobile devices and computers to trust the SSL certificate.

Signed Applications

The following applications are signed by Jamf:

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

Related Information

For related information, see the following Knowledge Base article:

Network Ports Used by the Casper Suite
Learn about the network ports used by the Casper Suite.

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
- Self Service Mobile
- JDS Installers

Jamf Software Server

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

- Java 1.7 or Java 1.8 (Java 1.8 is recommended)
- MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
- Apache Tomcat 7 or 8.0.x (Tomcat 8.0.x is recommended)

Tested operating systems include:

- macOS 10.10
- macOS 10.11
- macOS 10.12
- Ubuntu 14.04 LTS Server
- Ubuntu 16.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6.8 and 7.3
- Windows Server 2012 R2
- Windows Server 2016

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:

https://www.jamf.com/resources/product-documentation/installation-guides/

Tested browsers for the JSS are as follows:

- Safari
- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 10 or later

Package Building

Composer can run on the following operating systems:

- macOS 10.7.x (Composer v9.81 or earlier)
- macOS 10.8.x
- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x

Composer v9.81 or earlier is available from Jamf Nation.

Inventory

Recon can run locally on the following operating systems:

- macOS 10.7.x (Recon v9.93 or earlier)
- macOS 10.8.x
- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Recon v9.93 or earlier is available from Jamf Nation.

Recon can enroll computers with the following operating systems:

- macOS 10.7.x
- macOS 10.8.x

- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x

Imaging

Casper Imaging can image computers with the following operating systems, provided they do not have PowerPC processors:

- macOS 10.7.x (Casper Imaging v9.93 or earlier)
- macOS 10.8.x
- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x

Casper Imaging v9.93 or earlier is available from Jamf Nation.

Remote Management

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

- macOS 10.7.x
- macOS 10.8.x
- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x

Casper Remote can be used to manage computers with the following operating systems, provided they do not have PowerPC processors:

- macOS 10.7.x (Casper Remote v9.93 or earlier)
- macOS 10.8.x
- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x

Casper Remote v9.93 or earlier is available from Jamf Nation.

Self Service

Self Service can run on the following operating systems:

- macOS 10.7.x
- macOS 10.8.x
- macOS 10.9.x
- macOS 10.10.x
- macOS 10.11.x
- macOS 10.12.x

Managing Mobile Devices

The Casper Suite can be used to enroll and manage institutionally owned iOS and tvOS devices, and personally owned iOS and Android devices.

You can enroll and manage institutionally owned mobile devices that meet the following requirements:

- iPads, iPhones, or iPod touches with iOS 4 or later
- Apple TV devices with Apple TV software based on iOS 7 or later, or devices with tvOS 10.2 or later

For information on the management capabilities available for institutionally owned mobile devices, see Management Capabilities for Institutionally Owned Devices.

You can enroll and manage personally owned mobile devices that meet the following requirements:

- iPads, iPhones, or iPod touches with iOS 4 or later (iOS 7 or later is recommended)
- Smart phones or tablets with Android 4.0.3 or later

For information on the management capabilities available for personally owned mobile devices, see Management Capabilities for Personally Owned Devices.

Casper Focus

Casper Focus can run on teacher mobile devices with iOS 7 or later.

Student mobile devices that are assigned to classes in Casper Focus must have iOS 7 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 Casper Focus.

Self Service Mobile

Self Service Mobile for iOS can run on mobile devices with iOS 7 or later that are managed by the Casper Suite v9.4 or later.

Self Service Mobile for Android can run on mobile devices with Android 4.0.3 or later. In addition, a JSS v9.4 or later must be installed in your environment.

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
- macOS 10.7 or later with macOS Server 1.4.3 or later installed

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) 6.4, 6.5, 6.6, or 7.0

To install a JDS instance on a Linux operating system that is running on a virtual machine, you need a virtualization platform that provides SMBIOS information.

Computer Management Capabilities

The Casper Suite can be used to enroll and manage Mac computers. The management capabilities available for computers vary depending on the macOS version.

For information on the requirements for managing computers, see Requirements.

Management Capabilities for Computers

The following table provides an overview of the management capabilities available with the Casper Suite for computers by macOS version:

macOS Version	10.7	10.8	10.9	10.10	10.11	10.12
Enrollment						
Via user-initiated enrollment	✓	✓	✓	✓	✓	✓
Via QuickAdd package created using Recon	✓	✓	✓	✓	✓	✓
Via the network scanner[1]	✓	✓	✓	✓	✓	✓
Via remote enrollment using Recon[2]	✓	✓	✓	✓	✓	✓
Via local enrollment using Recon	✓	✓	✓	✓	✓	✓
Via Apple's DEP using a PreStage enrollment[3]			✓	✓	✓	✓
Via imaging using Casper Imaging	✓	✓	✓	✓	✓	✓
Inventory						
Submit inventory to the JSS	✓	✓	✓	✓	✓	✓
Extension attributes	✓	✓	✓	✓	✓	✓
Simple searches	✓	✓	✓	✓	✓	✓
Advanced searches	✓	✓	✓	✓	✓	✓
Computer reports	✓	✓	✓	✓	✓	✓
Mass actions	✓	✓	✓	✓	✓	✓
Computer Groups						
Static groups	✓	✓	✓	✓	✓	✓

macOS Version	10.7	10.8	10.9	10.10	10.11	10.12
Smart groups	✓	✓	✓	✓	✓	✓
Self Service						
Self Service	✓	✓	✓	✓	✓	✓
Display badges on the Self Service icon in the Dock	✓	✓	✓	✓	✓	✓
Display notifications in Notification Center		✓	✓	✓	✓	✓
Software Distribution						
VPP-managed distribution for computers					✓	✓
VPP-managed distribution for users			✓	✓	✓	✓
Mac App Store apps	✓	✓	✓	✓	✓	✓
Install packages	✓	✓	✓	✓	✓	✓
Remote Control						
Screen sharing[4]	✓	✓	✓	✓	✓	✓
Configuration						
macOS configuration profiles	✓	✓	✓	✓	✓	✓
Run scripts	✓	✓	✓	✓	✓	✓
Administer printers	✓	✓	✓	✓	✓	✓
Administer Dock items	✓	✓	✓	✓	✓	✓
Administer local accounts[5]	✓	✓	✓	✓	✓	✓
Administer the management account[6]	✓	✓	✓	✓	✓	✓
Bind to directory services	✓	✓	✓	✓	✓	✓
Deploy disk encryption configuration		✓	✓	✓	✓	✓
Issue a new FileFault 2 recovery key			✓	✓	✓	✓
Administer open Firmware or EFI passwords	✓	✓	✓	✓	✓	✓
Perform an authenticated restart on FileVault 2-enabled computers[7]		✓	✓	✓	✓	✓

macOS Version	10.7	10.8	10.9	10.10	10.11	10.12
Remote Commands for Computers						
Lock computer	✓	✓	✓	✓	✓	✓
Remove MDM profile	✓	✓	✓	✓	✓	✓
Wipe computer	✓	✓	✓	✓	✓	✓
Send blank push	✓	✓	✓	✓	✓	✓
Update OS version and built-in apps[8]					✓	✓
Usage Management						
View Application Usage logs	✓	✓	✓	✓	✓	✓
View Computer Usage logs	✓	✓	✓	✓	✓	✓
Restrict software	✓	✓	✓	✓	✓	✓
eBook Distribution						
VPP-managed distribution for users			✓	✓	✓	✓
Install ePub file	✓	✓	✓	✓	✓	✓
Install iBooks file			✓	✓	✓	✓
Install PDF	✓	✓	✓	✓	✓	✓

Notes:

1. To enroll computers using the network scanner, SSH (Remote Login) must be enabled on the computers.

2. To enroll a computer by running Recon remotely, you need the IP address of the computer and SSH (Remote Login) must be enabled on the computer.

3. When computers with macOS 10.10 or later are enrolled using a PreStage enrollment, they are also automatically managed if user-initiated enrollment is enabled for macOS in the JSS.

4. If the target computer has macOS 10.10 or later, screen sharing must also be enabled on the computer.

5. To enable or disable an account for FileVault 2, the computer must have macOS 10.9 or later.

6. To enable or disable the management account for FileVault 2, the computer must have macOS 10.9 or later.

7. To perform an authenticated restart, the target computer must have macOS 10.8.2 or later and be FileVault 2-enabled.

8. Requires enrollment via a PreStage enrollment.

Mobile Device Management Capabilities

The Casper Suite can be used to enroll and manage institutionally owned iOS and tvOS devices, and personally owned iOS and Android devices. The management capabilities available for a particular device vary depending on the device ownership type, device platform, device type, and OS version.

For information on the requirements for managing mobile devices, see Requirements.

Management Capabilities for Institutionally Owned Devices

The following table provides an overview of the management capabilities available with the Casper Suite for institutionally owned mobile devices by iOS version:

Device Type	iPad, iPhone, iPod touch						
iOS Version	4	5	6	7	8	9	10
Enrollment							
Via user-initiated enrollment	✓	✓	✓	✓	✓	✓	✓
Via an enrollment profile and Apple Configurator	✓	✓	✓	✓	✓	✓	
Via an enrollment profile and Apple Configurator 2						✓	✓
Via an enrollment profile and Apple's iPCU	✓	✓	✓				
Via Apple's DEP using a PreStage enrollment				✓	✓	✓	✓
Via Apple's DEP using a PreStage enrollment and Apple Configurator 2						✓	✓
Via Apple Configurator 2 using an enrollment URL						✓	✓
Inventory							
Submit inventory to the JSS	✓	✓	✓	✓	✓	✓	✓

Device Type	iPad, iPhone, iPod touch						
iOS Version	4	5	6	7	8	9	10
Mobile Device Groups							
Static groups	✓	✓	✓	✓	✓	✓	✓
Smart groups	✓	✓	✓	✓	✓	✓	✓
Configuration							
iOS configuration profiles[1]	✓	✓	✓	✓	✓	✓	✓
Remote Commands for Mobile Devices							
Update inventory	✓	✓	✓	✓	✓	✓	✓
Lock device	✓	✓	✓	✓	✓	✓	✓
Clear passcode	✓	✓	✓	✓	✓	✓	✓
Update passcode lock grace period						✓	✓
Clear restrictions[2]					✓	✓	✓
Wipe device[3]	✓	✓	✓	✓	✓	✓	✓
Unmanage device	✓	✓	✓	✓	✓	✓	✓
Send blank push	✓	✓	✓	✓	✓	✓	✓
Set wallpaper[2]				✓	✓	✓	✓
Enable/disable voice or data roaming[4]		✓	✓	✓	✓	✓	✓
Update iOS version via mass action[5]						✓	✓
Log out user[6]						✓	✓
Enable/disable Lost Mode[2]						✓	✓
Update location[7]						✓	✓
Enable/disable diagnostic and usage reporting[6]						✓	✓
Enable/disable app analytics[6]						✓	✓
Shut down device[6]							✓
Restart device							✓

Device Type	iPad, iPhone, iPod touch						
iOS Version	4	5	6	7	8	9	10
Self Service for iOS							
Self Service Mobile app				✓	✓	✓	✓
iBeacon region monitoring[8]				✓	✓	✓	✓
Self Service web clip	✓	✓	✓	✓	✓	✓	✓
App Distribution							
Managed apps		✓	✓	✓	✓	✓	✓
VPP-managed distribution for mobile devices						✓	✓
VPP-managed distribution for users				✓	✓	✓	✓
In-house apps	✓	✓	✓	✓	✓	✓	✓
App Store apps	✓	✓	✓	✓	✓	✓	✓
eBook Distribution							
Managed eBooks					✓	✓	✓
VPP-managed distribution				✓	✓	✓	✓
Install ePub file	✓	✓	✓	✓	✓	✓	✓
Install iBooks file[9]		✓	✓	✓	✓	✓	✓
Install PDF	✓	✓	✓	✓	✓	✓	✓
Casper Focus[10]							
Focus on app				✓	✓	✓	✓
Focus on website				✓	✓	✓	✓
Clear passcodes				✓	✓	✓	✓
Mirror device on Apple TV				✓	✓	✓	✓

Notes:
1. For detailed information on payload capabilities for iOS devices, see Payload Capabilities for Mobile Device Configuration Profiles.
2. Requires supervision.
3. The Wipe Device command can be used to clear Activation Lock for mobile devices with iOS 7.1 or later.

4. Remote commands for voice or data roaming are only available for devices with cellular capability.
5. Requires supervision and enrollment via PreStage enrollment.
6. Available for Shared iPad only on iPads with iOS 9.3 or later.
7. The Update Location command can be used to update the Global Positioning System (GPS) coordinates collected for a mobile device with iOS 9.3 or later while Lost Mode is enabled.
8. iBeacon region monitoring requires mobile devices with Self Service Mobile for iOS installed.
9. iBooks files (.ibooks) can only be installed on iPad.
10. Management capabilities available for Casper Focus apply only to student mobile devices, not teacher devices.

Management Capabilities for Personally Owned Devices

The following table provides an overview of the management capabilities available with the Casper Suite for personally owned mobile devices by device platform:

Device Platform	iOS	Android
Enrollment		
Via user-initiated enrollment	✓[1]	✓[1]
Via an enrollment profile and Apple Configurator		
Via an enrollment profile and Apple Configurator 2		
Via an enrollment profile and Apple's iPCU		
Via Apple's DEP using a PreStage enrollment		
Via Apple's DEP using a PreStage enrollment and Apple Configurator 2		
Via Apple Configurator 2 using an enrollment URL		
Inventory		
Submit inventory to the JSS	✓[2]	✓[2]
Extension attributes		
Simple searches	✓	✓
Advanced searches	✓	✓
Mobile device reports	✓	✓
Mass actions	✓	✓[3]
Mobile Device Groups		
Static groups		
Smart groups		

Device Platform	iOS	Android
Configuration		
iOS configuration profiles		
Personal device profiles	✓	✓
Remote Commands		
Update inventory	✓	✓
Lock device	✓	✓
Clear passcode		
Update passcode lock grace period		
Clear restrictions		
Wipe device		
Unmanage device		
Wipe institutional data	✓	✓
Send blank push	✓	✓
Set wallpaper		
Enable/disable voice or data roaming		
Update iOS version via mass action		
Log out user		
Enable/disable Lost Mode		
Update location		
Enable/disable diagnostic and usage reporting		
Enable/disable app analytics		
Shut down device		
Self Service for iOS		
Self Service Mobile app		
iBeacon region monitoring[4]		
Self Service web clip		
App Distribution		
Managed apps	✓	
VPP-managed distribution for mobile devices		
VPP-managed distribution for users	✓	
In-house apps	✓[5]	

Device Platform	iOS	Android
App Store apps	✓[5]	
eBook Distribution		
Managed eBooks		
VPP-managed distribution		
Install ePub file		
Install iBooks file		
Install PDF		
Casper Focus [6]		
Focus on app		
Focus on website		
Clear passcodes		
Mirror device on Apple TV		

Notes:

1. Enrolling a personal device using user-initiated enrollment requires an enabled personal device profile for the site that the user belongs to, or an enabled personal device profile for the full JSS. For more information, see Personal Device Profiles.
2. A limited subset of inventory information is collected for personal devices. For more information, see Viewing and Editing Inventory Information for a Mobile Device.
3. The Clear Passcode mass action does not apply to personally owned devices.
4. iBeacon region monitoring requires mobile devices with Self Service Mobile for iOS installed.
5. Only managed apps can be distributed to personal devices.
6. Management capabilities available for Casper Focus apply only to student mobile devices, not teacher devices.

Management Capabilities for Apple TV

The following table provides an overview of the management capabilities available with the Casper Suite for institutionally owned Apple TV devices by OS version:

Operating System	Apple TV Software Based on iOS[1]				tvOS
OS Version	7	8	9	10	10.2
Enrollment					
Via an enrollment profile and Apple Configurator	✓	✓	✓		

Operating System	Apple TV Software Based on iOS[1]				tvOS
OS Version	7	8	9	10	10.2
Via an enrollment profile and Apple Configurator 2	✓	✓	✓	✓	✓
Via Apple's DEP using a PreStage enrollment					✓
Via Apple's DEP using a PreStage enrollment and Apple Configurator 2					✓
Inventory					
Submit inventory to the JSS	✓	✓	✓	✓	✓
Mobile Device Groups					
Static groups	✓	✓	✓	✓	✓
Smart groups	✓	✓	✓	✓	✓
Configuration					
Mobile device configuration profiles[2]	✓	✓	✓	✓	✓
Remote Commands					
Update inventory	✓	✓	✓	✓	✓
Unmanage device	✓	✓	✓	✓	✓
Wipe device					✓
Send blank push	✓	✓	✓	✓	✓
Restart device					✓
App Distribution					
In-house apps					✓

Notes:
1. The iOS verison is equivalent to the OS build version on which the Apple TV software is based.
2. For detailed information on payload capabilities for Apple TV devices, see Payload Capabilities for Mobile Device Configuration Profiles.

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.

Related Information

For related information, see the following Knowledge Base article:
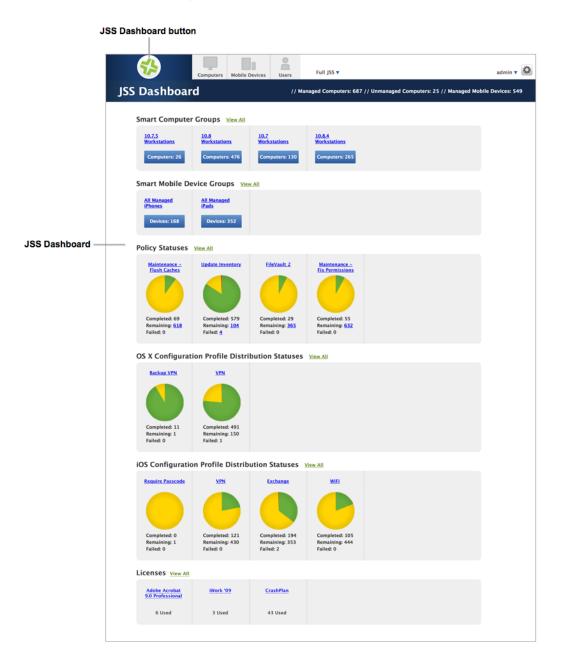
Network Ports Used by the Casper Suite
Learn about the network ports that you may need to configure when setting up the JSS.

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.

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
- macOS configuration profiles
- iOS configuration profiles
- Patch reports
- Licensed software
- PKI certificate authorities

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.

JSS Objects

JSS objects provide the foundation for performing administrative and management tasks using the Jamf Software Server (JSS). Examples of JSS objects include policies, configuration profiles, and network segments.

For detailed information about a specific JSS object, including instructions for navigating to the JSS object, see the appropriate section in this guide. Common actions that can be taken on JSS objects are cloning, editing, deleting, and viewing history.

Note: Available actions are dependent on the particular JSS object. (For example, a package cannot be cloned, so the Clone button is not displayed for the Packages object.) In addition, an action will not be available if the required privileges have not been granted for that JSS object.

Cloning a JSS Object

1. Log in to the JSS with a web browser.
2. Navigate to the JSS object you want to clone.
3. Click **Clone** and make changes as needed.
4. Click **Save**.

Editing a JSS Object

1. Log in to the JSS with a web browser.
2. Navigate to the JSS object you want to edit.
3. Click **Edit** and make changes as needed.
4. Click **Save**.

Deleting a JSS Object

1. Log in to the JSS with a web browser.
2. Navigate to the JSS object you want to delete.
3. Click **Delete**.
4. Click **Delete** again to confirm.

Viewing the History of a JSS Object

The JSS allows you to view the history of each JSS object. The information you can view includes:

- The date/time the JSS object was created or edited
- The username of the administrator who made the change
- Notes associated with the changes
- Details about a change

Note: This information is displayed for any JSS object changes made using v9.31 or later.

1. Log in to the JSS with a web browser.
2. Navigate to the JSS object you want to view the history of.
3. Click **History**.
4. (Optional) Click **Add Note** to add a note to the history record.
5. (Optional) Click **Details** to view details about a change.

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.

The JSS User Accounts and Groups settings also allow you to do the following:

- Configure account preferences for each JSS user account.
- Configure the password settings in the Password Policy for all standard JSS user accounts.
- Unlock a JSS user account that is locked.

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**.

4. Click **JSS User Accounts & 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**.

4. Click **JSS User Accounts & 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**.

Configuring Account Preferences

You can configure Language & Region and Search preferences for each JSS user account. Language & Region preferences allow you to configure settings such as date format and time zone. Search preferences allow you to configure settings for computer, mobile device, and user searches.

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 **Preferences**.

3. Click the **Language & Region** tab and use the pop-up menus to configure language and region preferences.

4. Click the **Search Preferences** tab and use the pop-up menus to configure search preferences.
   Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains".

5. Click **Save**.

Configuring the Password Policy

The Password Policy in the JSS allows you to configure the password settings. The Password Policy applies to all standard JSS user accounts. You can configure the following password settings:

- Number of login attempts allowed before a JSS user is locked out of the account
- Password length and age
- Password reuse limitations
- Password complexity
- Settings to allow a user to unlock their own account

Note: The settings configured in the Password Policy do not apply to JSS user accounts added from an LDAP directory service.

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**.

4. Click **JSS User Accounts & Groups** 👤 .

5. Click **Password Policy** 🔑 .

6. Click **Edit**.

7. Use the settings on the pane to specify the password settings.

8. Click **Save**.

The settings are applied immediately.

Unlocking a JSS User Account

A JSS user could be locked out of their account if they exceed the specified number of allowed login attempts. If the Password Policy is configured to allow the user to unlock their account, the user can reset their password to unlock their account. In this case, an email is immediately sent to the email address associated with the account in the JSS allowing the user to unlock their account by resetting their password. For an email to be sent, an SMTP server must be set up in the JSS. (For more information, see Integrating with an SMTP Server.)

In addition, a JSS user account that is locked can be manually unlocked from the JSS by another JSS user with the Administrator privilege set.

The access status of the account is displayed as "Disabled" in the JSS until the account is unlocked.

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**.

4. Click **JSS User Accounts & Groups** 👤 .
   A list of JSS user accounts and groups is displayed.

5. Click the JSS user account that has an access status of "Disabled", which means the account is locked.

6. Click **Edit**.

7. Choose "Enabled" from the **Access Status** pop-up menu to unlock the account.

8. Click **Save**.

   The JSS user account is unlocked immediately.

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.
- Require users to log in during mobile device setup 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 configuring attribute mappings. This allows you to integrate with additional directory services.

After you have configured an LDAP directory service in the JSS, you can configure an LDAP Proxy. The LDAP Proxy creates a secure tunnel to allow traffic to pass between a JSS and an LDAP directory service. (For more information, see LDAP Proxy.)

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**.
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**.
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**.

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**.
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.

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

- Self Service Mobile
  Find out how to require users to log in to the Self Service app 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.

- Mobile Device PreStage Enrollments
  Find out how to require users to log in during mobile device setup using their LDAP directory accounts before enrolling their mobile devices using a PreStage enrollment.

- 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).

Single Sign-On

The Single Sign-On (SSO) feature allows you to integrate with a third-party Identity Provider (IdP) and implement SSO for portions of the Casper Suite. When SSO is enabled, by default users are redirected to the Identity Provider login page. After successful authentication, users are directed back to the URL they were attempting to log into.

Single Sign-On can be enabled for:

- Jamf Software Server (JSS)
- User-Initiated Enrollment (iOS and macOS)
- Self Service for macOS

Identity Providers

Single Sign-On can be implemented by integrating with a Security Assertion Markup Language 2.0 (SAML 2.0) Identity Provider. For information on configuring SSO in the JSS with selected Identity Providers, see the Configuring Single Sign-On Settings to Work with an Identity Provider section of this guide.

Single Sign-On Settings

To configure SSO, log in to the JSS with a web browser and in the top-right corner of the page, navigate to **Settings > System Settings > Single Sign-On**.

The following table describes Single Sign-On settings:

Setting	Description	Example
Single Sign-On (SSO) Utilization	Enables Single Sign-On access for selected applications or services.	
Allow bypass for all users	When this setting is selected, users will not be redirected to the Identity Provider login page for authentication, but can log in to the JSS directly instead. When a user tries to access the JSS via the Identity Provider, IdP-initiated SSO authentication and authorization occurs.	
Additional login URL for users with privileges	Allows a JSS user account with Single Sign-On (SSO) privileges to access the JSS directly when SSO is enabled. It is recommended that you copy and save the failover URL.	

Setting	Description	Example
User Mapping: SAML	By default, this setting is set to "NameID" but you may define a custom attribute. To complete the information exchange between the JSS and the IdP, the SAML assertion sent by the IdP must contain the `NameID` attribute. If using a custom attribute, the SAML assertion must contain the `NameID` attribute (any value) and the specified user attribute.	"NameID" or custom attribute (e.g., "User")
User Mapping: JSS	The JSS maps SAML attributes sent by the IdP in the following ways: by users and by groups. When a user tries to access the JSS, by default the JSS gets information about the user from the Identity Provider and matches it against JSS user accounts. If the incoming user account does not exist in the JSS, then group name matching occurs.	"Username" or "Email"

Group Attribute Name	In the Group Attribute Name, you may define a custom attribute. Group information should be provided in the SAML attribute sent by the IdP and can contain a list of group names. The JSS matches each group from the JSS database and compares group names. Users will be granted access privileges from all of the groups in the same manner as a local JSS user would.
	
	```<Attribute Name="http://schemas.xmlsoap.org/claims/Group"> <AttributeValue>Administrators</AttributeValue> <AttributeValue>JSS_Auditor</AttributeValue></Attribute>```
	
	Group name lists can consist of separate <AttributeValue> elements as in the example above. The JSS is able to extract the list of group names from a single <AttributeValue> element if it contains a string of group names separated by semicolons.
	
	```<Attribute Name="http://schemas.xmlsoap.org/claims/Group"> <AttributeValue>Administrators;JSS_Auditor</AttributeValue></Attribute>```
		http://schemas.xmlsoap.org/claims/Group

RDN Key for LDAP Groups	Setting used to extract the name of the group from strings sent in LDAP format, Distinguished Names (DN). The JSS will search the incoming string for a Relative Distinguished Name (RDN) with the specified key and use the value of the RDN Key as an actual name of the group. If the LDAP directory service string contains several RDN parts with the same key (i.e., CN=Administrators, CN=Users, O=YourOrganization), then the JSS will extract group names from the left-most RDN Key (CN=Administrators). If the RDN Key for LDAP Groups field is left blank, the JSS will use the entire LDAP format string.	"CN", "DC", "O" or similar

Setting	Description	Example
Entity ID	By default, Entity ID is prefilled in the JSS. Use the same Entity ID when configuring your IdP settings.	https://jss. example.com /saml /metadata
Identity Provider	The JSS supports any SAML 2.0 Identity Provider. Select your IdP to populate the Token Expiration value.	"Active Directory Federation Services", "Okta", "One Login", "Ping Identity", "OneLogin", "Shibboleth", or "Other"
JSS Signing Certificate	Optionally, you may want to generate or upload the JSS Signing Certificate to have JSS messages to the IdP signed. Although this setting is optional, it is recommended that you always secure SAML communication with a digital signature. If uploading the JSS Signing Certificate, upload a signing certificate keystore (.jks or .p12) with a private key to sign and encrypt SAML tokens, enter the password to the KeyStore file, select a private key alias, and enter the password for this key.	
Token Expiration	Specifies Identity Provider session timeout in minutes. The Token Expiration field is populated depending on the Identity Provider you select. Ensure the value matches your IdP settings.	"460"
JSS Metadata	To get metadata from the JSS, download an XML metadata file from the Single Sign-On settings page after saving your SSO configuration, or use the JSS metadata URL.	https://jss. example.com /saml /metadata

Authentication Using Single Sign-On

When Single Sign-On is enabled, by default Identity Providers handle the authentication of users. Authorization is based on access levels set in JSS User Accounts and Groups.

JSS Authentication

By default, every time an unauthenticated user attempts to access the JSS they will be redirected to the IdP login page unless the **Allow bypass for all users** checkbox is selected in the Single Sign-On settings.

Self Service for macOS Authentication

When SSO is enabled for Self Service for macOS, the username entered into the IdP during authentication will be the username the JSS utilizes for scope calculations. Self Service authentication will be granted for any username that exists in the IdP.

Note: If the Self Service **User Login** setting was previously set to "No Login", enabling SSO for Self Service will change the setting to "Allow users to log in to the login menu". In other cases, settings remain the same.

Authentication with LDAP	Authentication without LDAP
If LDAP is integrated with the JSS, LDAP limitations and exclusions can be used. They will be calculated by matching the username entered into the IdP during Self Service login with the LDAP username.	If LDAP is not integrated with the JSS, targets and exclusions for a username will be calculated by matching the username entered into the IdP during Self Service login with JSS users accounts and groups.

User-Initiated Enrollment Authentication

When SSO is enabled for User-Initiated Enrollment, the username entered into the IdP during authentication will be the username the JSS inputs into the Username field in the User and Location category when updating inventory information for a computer or mobile device.

Authentication with LDAP	Authentication without LDAP
If LDAP is integrated with the JSS, the User and Location information will be fully populated using a lookup from the JSS to LDAP.	If LDAP is not integrated with the JSS, the Username field will be the only item populated in the User and Location category. User lookup will not work during enrollment.

Single Logout

The JSS uses service provider-initiated SAML Single Logout (SLO) during enrollment to ensure users can end all sessions started with the JSS and the IdP. When users complete the enrollment process, they will be presented with a Logout button allowing them to perform SLO. Use the Messaging pane in User-Initiated Enrollment settings to customize the text displayed during the enrollment experience.

Single Logout will not be available if the selected IdP does not provide any SLO endpoints in the metadata, or if there is no JSS Signing Certificate set up. In such a case, users will be provided with a message advising that the IdP session might still be active. This is important for JSS administrator users who won't be able to fully log out after performing the enrollment process for other users.

Note: To support uncommon IdP configurations, the GET binding (less secure than POST) can be used for SAML Single Logout.

Requirements

To enable Single Sign-On, you need:

- An Identity Provider (IdP) using SAML 2.0 protocols
- JSS User Accounts and Groups that have matching Identity Provider usernames or groups
- User with administrator privileges to the JSS and the Identity Provider

Configuring Single Sign-On Settings to Work with an Identity Provider

To fully implement the Single Sign-On feature, you must also configure your Identity Provider settings. The workflow varies depending on the Identity Provider you use.

See the following Knowledge Base articles for recommended workflows during Identity Provider configuration:

- Configuring Single Sign-On with Okta
- Configuring Single Sign-On with Active Directory Federation Services
- Configuring Single Sign-On with Shibboleth
- Configuring Single Sign-On with OneLogin
- Configuring Single Sign-On with Ping Identity
- Configuring Single Sign-On with G Suite (Google Apps)

Further Considerations

- It is recommended that you use SSL (HTTPS) endpoints and the POST binding for transmission of the SAML protocol.
- If using LDAP users or groups for SSO, they should first be added as JSS users in the JSS User Accounts and Groups settings.
- When configuring your Identity Provider settings, it is recommended that you use SHA-256 or higher signatures for SAML assertions.

To resolve common errors that users might experience while using Single Sign-On, see the Troubleshooting Single Sign-On in the JSS Knowledge Base article.

Related Information

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

- Integrating with LDAP Directory Services
  Find out how to configure LDAP and test LDAP attribute mappings.

- JSS User Accounts and Groups
  Find out more about configuring a JSS user account or group.

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

- User-Initiated Enrollment for Computers
  Find out where to set the logout message text.

- 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.

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**.
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**.
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 to 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 an Imaging 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.
- Smart user 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.
- An instance of the JSS web application in a clustered environment fails.
- The VPP service token for a VPP account is approaching its expiration date.
  Note: The first email notification is sent 31 days before the token expires. Email notifications are sent once a week until the token is 7 days from its expiration date, at which time the email notifications are sent every day until the token expires. After the token has expired, no email notifications are sent.
- A Jamf Infrastructure Manager instance has not checked in with the JSS.
  Note: An email notification is sent if the Infrastructure Manager fails to check in with the JSS after three attempts. Only one notification is sent for this event.

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 **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**.

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 changes that happen in the Jamf Software Server (JSS), such as the creation of a JSS user account. The Change Management settings in the JSS allow you to log those changes to a log file (JAMFChangeManagement.log) on the JSS host server and/or log the changes to a syslog server.

The Change Management logs can also be viewed in the JSS. The information displayed includes:

- Date/time the change took place
- Username of the administrator who made the change
- Object type (such as a JSS user account)
- Object name (such as the username of a JSS user account)
- Action (such as "Created")
- Details about the change

In addition, you can view the changes to a specific object in that object's history. (For more information, see Viewing the History of a JSS Object.)

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**.

4. Click **Change Management** ▦ .

5. Click **Edit**.

6. Configure the settings on the pane.

7. Click **Save**.

Viewing Change Management Logs 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**.

4. Click **Change Management** ▦ .

5. Click **Logs**.
   The Change Management logs are displayed on the pane.

6. Do one of the following:

   - To view the object associated with a change, click the object in the Object Name column.

   - To view details about the change, click **Details** in the Details column.

Related Information

For related information, see the following Knowledge Base article:

Change Management with the Casper Suite: macOS Setup Guide
If you are hosting the JSS on a server with macOS Server installed, 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.

Note: If your environment is hosted in Jamf Cloud, the Apache Tomcat settings are managed by Jamf Cloud and are not accessible.

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**.

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)
- JSS access logs
- Change Management logs
- Event logs

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.

For information on the types of data flushed with each log and the database tables affected, see the following Knowledge Base article:

[Data and Tables Affected by Log Flushing](#)

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**.

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**.

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

- Viewing and Flushing Logs for a Policy
  Find out how to view and flush logs for a policy.

- Viewing the History for a Computer
  Find out how to view the logs and the management history for a computer.

- Viewing Management History for a Mobile Device
  Find out how to view the management history for a mobile device.

Maintenance Pages

The Maintenance Pages setting allows you to create a custom maintenance page for each language used in your environment.

The maintenance page is displayed to users when the JSS is starting up or being upgraded under the following conditions:
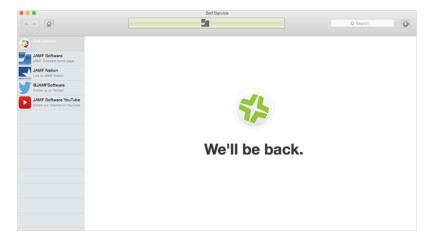
- When using Self Service for macOS
- When using the Self Service web clip
- During enrollment

A maintenance page configuration is preconfigured in the JSS for each of the following languages: English, French, and German. When a computer or mobile device has a preferred language set on it, it displays the maintenance page configuration that corresponds with that language. The English version of the maintenance page is displayed if the computer or mobile device does not have a preferred language set on it.

In addition to the language, the message and the graphic displayed on the maintenance page can be customized. The preconfigured maintenance page message is "We'll be back." You can use Markdown to format the maintenance page message and image.

For information about Markdown, see the following Knowledge Base article:
Using Markdown to Format Text

The screen shot below shows the English version of the default maintenance page.

Creating a Maintenance Page Configuration

The Maintenance Pages setting allows you to create a custom maintenance page for each language used in your environment.

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**.

4. Click **Maintenance Pages** ⬜ .

5. Click **New** ➕ and then use the **Language** pop-up menu to specify the language that will be contained within the message. Computers and mobile devices with a preferred language that matches the specified language will display this version of the maintenance page.

6. Use the **Maintenance Page Message** field to customize the message displayed during the JSS maintenance process.

7. Click **Save**.

8. Repeat this process as needed for other languages.

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 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
- Users
- 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.

Requirements

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

To create a Jamf Nation account, go to:
https://www.jamf.com/jamf-nation/users/new

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**.

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

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**.

4. Click **JSS Summary** 📋 .

5. Select the checkboxes next to the items you want to include.

6. Click **Send Summary to Jamf**.

7. Enter your Jamf Nation credentials, and then click **Send**.

   The JSS Summary is sent to Jamf via Jamf Nation.

Related Information

For information about Customer Experience Metrics (CEM), see the following Knowledge Base article:

[Customer Experience Metrics](#)
Learn about Customer Experience Metrics and how to configure the setting in your JSS environment.

For additional information about Customer Experience Metrics, visit the following webpage:
https://www.jamf.com/products/jamf-pro/customer-experience-metrics/

JSS Health Check Page

The Jamf Software Server (JSS) health check page allows you to view the status of your environment. This can be useful for identifying performance and configuration issues. For example, you can use the JSS health check page to ensure all instances of the JSS web application in a clustered environment are running without error.

Note: The JSS health check page is not the same as the JSS Health Check service provided by Jamf Support.

The following table lists the possible status the JSS health check page may return:

Status	Description
[{"healthCode":1,"httpCode":503," description":"DBConnectionError"}]	An error occurred while testing the database connection.
[{"healthCode":2,"httpCode"200:," description":"SetupAssistant"}]	The JSS Setup Assistant was detected.
[{"healthCode":3,"httpCode":503," description":"DBConnectionConfigError"}]	A configuration error occurred while attempting to connect to the database.
[{"healthCode":4,"httpCode":503," description":"Initializing"}]	The JSS web application is initializing.
[{"healthCode":5,"httpCode":503," description":"ChildNodeStartUpError"}]	An instance of the JSS web application in a clustered environment failed to start.
[{"healthCode":6,"httpCode":503," description":"InitializationError"}]	A fatal error occurred and prevented the JSS web application from starting.
[ ]	The JSS web application is running without error.

Using the JSS Health Check Page

To navigate to the JSS health check page, append "healthCheck.html" to your JSS URL. For example:

https://jss.mycompany.com:8443/healthCheck.html

The status of your environment displays on the screen.

Once you have identified the status of your environment, you can take steps to resolve any issues that were found.

Global Management Settings

Push Certificates

The JSS requires a valid push certificate to communicate with APNs. This communication is required to do the following:

- Send macOS configuration profiles and macOS remote commands to computers.
- Distribute Mac App Store apps to computers.
- Enroll and manage iOS 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://www.jamf.com/jamf-nation/users/new
- 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**.
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**.
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**.
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 macOS configuration profiles and macOS remote commands to computers, and managing iOS devices. In addition, without a push certificate, Mac App Store apps cannot be distributed to computers. 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**.

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 macOS configuration profiles and macOS remote commands to managed computers.

- PKI Certificates
  Learn how to configure public key infrastructure certificates to ensure secure communication with APNs.

For related information, see the following Knowledge Base article:

Network Ports Used by the Casper Suite
Find out which ports the JSS uses to communicate with APNs.

Jamf Push Proxy

The Jamf Push Proxy enables communication between the Jamf Software Server (JSS) and devices with Self Service Mobile for iOS installed, and between the JSS and personally owned Android devices. Push notifications trigger the following types of communication between the JSS and devices in your environment:

- Sending Notification Center notifications to mobile devices with Self Service Mobile for iOS
- Requesting management check-ins from personally owned Android devices

The JSS requires a valid proxy server token to authenticate to the Jamf Push Proxy. An assistant in the JSS guides you through the process to request a new proxy server token from the Jamf Authorization Server and upload it to the JSS.

Requirements

To request or renew a proxy server token, you need a valid Jamf Nation account.

To create a Jamf Nation account, go to:
https://www.jamf.com/jamf-nation/users/new

Requesting and Uploading a Proxy Server Token

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**.
4. Click **Push Certificates** .
5. Click **New** .
6. Select **Get proxy server token from Jamf Authorization Server**.
7. Follow the onscreen instructions to get the proxy server token and upload it to the JSS.

Renewing the Proxy Server Token

Note: The proxy server token will be renewed automatically, however, the following steps can be used for troubleshooting purposes.

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**.

4. Click **Push Certificates** .

5. Click the push proxy and then click **Renew**.

Related Information

For related information, see the following Knowledge Base article:

Jamf Push Proxy Communication
Learn about push proxy network communication and ports.

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, which involves entering GSX account information and uploading an Apple certificate.

You can also use the JSS to test the connection and upload a renewed Apple certificate when needed.

Requirements

To configure the GSX Connection settings, you need:

- A GSX account with the "Manager" role, access to Web Services, and access to coverage/warranty information
- An Apple certificate (.pem or .p12)

For instructions on creating a GSX account and obtaining an Apple certificate, 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**.

4. Click **GSX Connection** 🌐 .

5. Click **Edit**.

6. Select **Enable Connection to GSX**.
   Note: This and some of the other settings on this pane may already be configured if the JSS was used to generate a CSR.

7. Enter the username and account number for the GSX account.

8. Configure the region and URI settings as needed.

9. Select **Certificate-based Authentication** and click **Upload**.

10. Follow the onscreen instructions to upload the Apple certificate (.pem or .p12).

Testing the GSX Connection

Once the GSX Connection settings are configured, you can test the connection to make sure it works .

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**.

4. Click **GSX Connection** 🌐 .

5. Click **Test**.

6. Click **Test** again.

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

Renewing the Apple Certificate

You can use the JSS to upload a renewed Apple certificate without removing the existing certificate so the connection with GSX is not lost. A notification is displayed 31 days prior to the expiration date of the Apple 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**.

4. Click **GSX Connection** 🌐 .

5. Click **Edit.**

6. Click **Renew.**

7. Follow the onscreen instructions to upload a renewed Apple certificate.

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 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 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.

User-Initiated Enrollment Settings

Enrollment is the process of adding computers and mobile devices to the Jamf Software Server (JSS). This establishes a connection between the computers and mobile devices and the JSS.

User-initiated enrollment allows users to initiate the enrollment process on their own.

Users can enroll the following:

- Mac computers
- Institutionally owned iOS devices
- Personally owned iOS and Android devices

The User-Initiated Enrollment settings allow you to do the following:

- Enable user-initiated enrollment for the appropriate platforms.
- Customize text displayed for each step in the enrollment process, including adding different languages.
- Restrict re-enrollment so that a user is only allowed to re-enroll a computer or mobile device if one of the following conditions is met:
  - The user is a JSS user with the "Computers" or "Mobile Devices" privilege.
  - The username of the user re-enrolling the computer or mobile device matches the Username field in the User and Location category in inventory information.
  - The Username field in the User and Location category in inventory information is blank.
- Require users to install the CA certificate (mobile devices only).
- Specify a management account (computers only).
- Ensure that SSH (Remote Login) is enabled (computers only).
- Ensure that Self Service is launched after enrollment (computers only).
- Sign the QuickAdd package used for enrollment (computers only).
  Signing the QuickAdd package ensures that it appears as verified to users who 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:
  - An installer certificate (.p12) from Apple. For instructions on how to obtain an installer certificate, see the following Knowledge Base article:
    Obtaining an Installer Certificate from Apple
  - A Certification Authority intermediate certificate from Apple in the System keychain in Keychain Access on computers. 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

Customizing the User-Initiated Enrollment Experience

You can customize the text displayed in each step of the enrollment experience using Markdown. You can also add different languages.

For information about Markdown, see the following Knowledge Base article:
Using Markdown to Format Text

The following table describes each step that can be customized and the platform each step is displayed on:

Enrollment Step	Description	macOS	Institutionally Owned iOS Devices	Personally Owned iOS and Android Devices
Login Page	Customize how you want the Login page to be displayed to users.	✓	✓	✓
Device Ownership	Customize the text that prompts the user to specify the device ownership type if user-initiated enrollment is enabled for both institutionally owned and personally owned devices. **Note:** Because Android devices cannot be enrolled as institutionally owned devices, the text, button name, and management description are not displayed to users. You can also specify the device management description that displays to users to provide custom messaging on the IT management capabilities for each device ownership type.		✓	✓
EULA	Enter text for the End User License Agreement (EULA). If the EULA is left blank, it is not displayed to users during enrollment. The EULA is not displayed for users logging in with a JSS user account.	✓	✓	✓

Enrollment Step	Description	macOS	Institutionally Owned iOS Devices	Personally Owned iOS and Android Devices
Sites	Customize the message that prompts users to choose a site. If a user logs in with a JSS user account, they can assign an LDAP user to the computer or mobile device. If you have more than one site in the JSS and have entered information on the Messaging Pane in Personal Device Profiles in the JSS, this information is displayed to users when they are prompted to choose a site. (For more information, see Personal Device Profiles.)	✓	✓	✓
Certificate	Customize the message that prompts users to install the CA certificate for mobile devices to trust at enrollment.		✓	iOS only
Institutional MDM Profile	Customize the message that prompts users to install the MDM profile for institutionally owned devices.			
Personal MDM Profile	Customize the message that prompts users to install the MDM profile for personally owned devices.			iOS only
QuickAdd Package	Customize the message that prompts users to download and install the QuickAdd package.	✓		
App for Android	Customize the message that prompts users to install Self Service Mobile for Android from Google Play.			Android only
Complete Page	Customize the messages that are displayed to users if enrollment is successful or if it fails.	✓	✓	iOS only

Configuring the User-Initiated Enrollment 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**.

4. Click **User-Initiated Enrollment** 🖥️ .

5. Click **Edit**.

6. Use the General pane to restrict re-enrollment and to skip certificate installation.

7. Use the Messaging pane to customize the text displayed during the enrollment experience and add languages.
   Note: English is the default language if the computer or mobile device does not have a preferred language set on it.

   - To add a language, click **Add** [+] and then choose the language from the **Language** pop-up menu. You can repeat this process as needed for other languages.

   - To customize the text for a language already listed, click **Edit** or **View** depending on what's displayed. Then click **Done**.

8. Use the Platforms pane to enable user-initiated enrollment and configure the enrollment settings for each platform as needed.

9. Use the Access pane to choose the site you want to display to LDAP user groups during enrollment. Then, click **Done**.
   If an LDAP user belongs to more than one LDAP user group in the JSS, the user will have the option to select the sites you assign to each group that user belongs to.

10. Click **Save**.

Related Information

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

- User-Initiated Enrollment for Computers
  Find out how to allow users to enroll computers.

- User-Initiated Enrollment for Mobile Devices
  Find out how to allow users to enroll mobile devices.

- User-Initiated Enrollment Experience for Computers
  Learn about the steps users take to enroll computers.

- User-Initiated Enrollment Experience for Mobile Devices
  Learn about the steps users take to enroll mobile devices.

Integrating with the Device Enrollment Program

The Device Enrollment Program settings allow you to integrate with Apple's Device Enrollment Program (DEP), part of Apple Deployment Programs. Integrating with DEP is the first step to enrolling a device with the Jamf Software Server (JSS) using a PreStage enrollment. After the JSS is integrated with DEP, you can use the JSS to configure enrollment and device setup settings.

To integrate with DEP, you need to do the following:

1. Download a public key (.pem) from the JSS.

2. Obtain a server token file (.p7m) from Apple.

3. Upload the server token file to the JSS to configure an instance of DEP.

   For more information about DEP, see the following websites:

   - Device Enrollment Program for Business
     https://www.apple.com/business/dep/

   - Device Enrollment Program for Education
     https://www.apple.com/education/it/dep/

Requirements

To obtain a server token file from Apple, you need an Apple Deployment Programs account. You can apply for an account at:
https://deploy.apple.com

Downloading a Public Key

Before you can obtain the server token file from Apple, you need to download a public key 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 **Global Management**.

4. Click **Device Enrollment Program** ▢ .

5. Click **Public Key** to download the public key.

   The public key (.pem) is downloaded immediately.

Obtaining the Server Token File

To download the server token file, you need to upload your public key to the Apple Deployment Program website.

1. Log in to the Apple Deployment Program website at http://deploy.apple.com.

2. In the sidebar, select **Device Enrollment Program** .

3. Follow the onscreen instructions to verify your identity.

4. In the sidebar, select **Manage Servers**, and then click **Add MDM Server**.

5. Enter a name for your MDM server, and then click **Next**.

6. Click **Choose File**, and then upload the public key (.pem) you downloaded from the JSS.

7. Click **Next** to download the server token file (.p7m).

   The server token file (.p7m) is downloaded immediately.

Uploading the Server Token File to Configure an Instance of DEP

This process creates one instance of DEP in the JSS. To meet the needs of your organization, you can repeat the process to create multiple instances of DEP.

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**.

4. Click **Device Enrollment Program** .

5. Click **New** .

6. Enter a display name for the DEP instance.

7. Click **Upload Server Token File** to upload the server token file (.p7m) you downloaded from Apple.
   This creates one instance of the program in the JSS.
   The information contained in the server token file is displayed.

8. (Optional) Choose a supervision identity to associate with the DEP instance. (For more information, see Supervision Identities.)

9. Click **Save**.

10. To configure another instance of DEP, repeat steps 5-9.

Refreshing DEP Instance Information

The JSS allows you to manually refresh information in the DEP instance as needed.

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**.

4. Click **Device Enrollment Program** ⬚ .
   A list of program instances is displayed.

5. Click the program instance you want to refresh.

6. Click **Refresh**.

   If there is updated information in DEP, this information is displayed in the JSS.

Further Considerations

- If you upload a new server token file (.p7m) to renew an expired DEP instance, it is recommended that you do not delete the expired instance from the JSS before uploading the new server token file.

- Deleting a DEP instance removes the instance from the JSS but does not delete the settings in DEP.

- If necessary, you can remove a device from DEP by disowning the device using the Apple Deployment Programs website. Disowning a device that is currently enrolled with the JSS does not remove the device from the JSS. For detailed information on disowning devices, see Apple Deployment Programs Help at:
  https://help.apple.com/deployment/business/

Related Information

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

- Mobile Device PreStage Enrollments
  Find out how to enroll mobile devices using a mobile device PreStage enrollment.

- Computer PreStage Enrollments
  Find out how to enroll Mac computers using a computer PreStage enrollment.

- Supervision Identities
  Find out how to create, upload, and download a supervision identity for use with Apple Configurator 2.

Re-enrollment Settings

The Re-enrollment settings in the JSS allow you to clear certain information from inventory for a computer or mobile device when it is re-enrolled with the JSS.

The Re-enrollment settings are applied to computers and mobile devices when they are re-enrolled with the JSS via the following enrollment methods:

- User-initiated enrollment
- PreStage enrollment
- Apple Configurator 2 enrollment methods (mobile devices only)

The following table lists the settings that you can apply to inventory information during re-enrollment:

Setting	Description
Clear user and location information on mobile devices and computers	This setting clears all information from the User and Location category on the **Inventory** tab in computer and mobile device inventory information during re-enrollment with the JSS. When devices are re-enrolled, the user and location fields display a blank value. Information is not cleared, however, when the following happens: - If a user logs in to the enrollment portal using an LDAP directory account, or a JSS user logs in and assigns an LDAP user to the device, then the user and location information associated with the LDAP account is assigned to the device during re-enrollment. If the user chooses a site at enrollment, the device is associated with the selected site. - If there is an extension attribute displayed on the User and Location category on the **Inventory** tab, the value for the extension attribute is not cleared during re-enrollment. - If a PreStage enrollment is used to enroll devices and the **Use existing location information, if applicable** option is selected, the user and location information of the user logging in is populated in the device's inventory information. For more information about user and location information, see Viewing and Editing Inventory Information for a Computer and Viewing and Editing Inventory Information for a Mobile Device.
Clear user and location history information on mobile devices and computers	This setting clears all information from the User and Location History category on the **History** tab in computer and mobile device inventory information during re-enrollment with the JSS. For more information about user and location history information, see Viewing the History for a Computer and Viewing the History for a Mobile Device.

Setting	Description
Clear policy logs on computers	This setting clears all information from the Policy Logs category on the **History** tab in computer inventory information during re-enrollment with the JSS. For more information about the policy logs for computers, see Viewing the History for a Computer.
	In addition, this setting clears the logs for a policy for re-enrolled computers that have run the policy. For information on viewing and flushing logs for a policy, see Managing Policies.
	When the computer is re-enrolled with the JSS, any policies that the computer is in the scope of are re-run on the computer at the policy's next trigger.
Clear management history on mobile devices and computers	This setting clears all information from the Management History category on the **History** tab in computer and mobile device inventory information during re-enrollment with the JSS.
	You can clear the following information: ▪ Completed, pending, and failed commands ▪ Pending and failed commands ▪ Failed commands ▪ Nothing The default setting is to clear pending and failed commands.
	Note: If there are pending commands at the time of re-enrollment, these commands are cleared.
	For more information about management history information, see Viewing the History for a Computer and Viewing the History for a Mobile Device.

Configuring the Re-enrollment 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**.

4. Click **Re-enrollment** 🖥 .

5. Choose the settings that you want to apply to device inventory information during re-enrollment.

6. Click **Save**.

When computers and mobile devices are re-enrolled with the JSS, the settings are applied to inventory information.

Related Information

For related 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.

- Computer PreStage Enrollments
  Find out how to enroll Mac computers using a PreStage enrollment.

- User-Initiated Enrollment for Mobile Devices
  Find out how to allow users to enroll mobile devices by having them log in to an enrollment portal.

- Mobile Device PreStage Enrollments
  Find out how to enroll mobile devices using a PreStage enrollment.

- Apple Configurator Enrollment Settings
  Find out how to enable Apple Configurator enrollment so you can enroll mobile devices using Apple Configurator and an enrollment URL.

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).

Note: If your environment is hosted in Jamf Cloud, the JSS URL setting is managed by Jamf Cloud and is not accessible.

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**.

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 download enrollment profiles so you can enroll mobile devices by connecting them to a computer via USB.

PKI Certificates

The PKI Certificates settings allow you to manage the certificate lifecycle directly in the Jamf Software Server (JSS). To ensure secure communication with the Apple Push Notification service (APNs), the JSS requires a public key infrastructure (PKI) that supports certificate-based authentication. The PKI must include the following components:

- A certificate authority (CA)
- A signing certificate
- A CA certificate

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

You can choose to use a built-in CA, integrate with a trusted third-party CA (Symantec), or configure your own PKI if you have access to an external CA that supports the Simple Certificate Enrollment Protocol (SCEP).

The PKI Certificates settings in the JSS allow you to perform the following tasks:

- View a list of active, expiring, inactive or all certificates issued by a CA.
- Add a PKI certificate authority to the JSS Dashboard.
- View details of a specific certificate that was issued.
- Export a certificate list for a CA.

Using the Built-in CA

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 Certificates settings in the JSS to perform the following tasks related to the built-in CA:

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

Downloading the Built-in CA Certificate

You can use the PKI Certificates 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**.

4. Click **PKI Certificates** 📜 .

5. Click the **Management Certificate Template** tab, and then click **Built-in CA**.

6. Click **Download CA Certificate**.

   The certificate (.pem) downloads immediately.

Viewing or Revoking Built-in CA Certificates

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

- Subject name
- Serial number
- Device name associated with the certificate
- Username associated with certificate
- CA configuration 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**.

4. Click **PKI Certificates** 📜 .

5. To view a list of Expiring, Active, Inactive or All certificates, click the number displayed in the corresponding column on the Certificate Authorities pane.
   A list of certificates issued by the built-in CA is displayed.

6. Click the certificate subject 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** to return to the list of built-in certificates.

Manually Creating a Built-in CA 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 Certificates 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**.
4. Click **PKI Certificates** .
5. Click the **Management Certificate Template** tab, and then click **Built-in CA**.
6. Click **Create Certificate from CSR**.
7. In the **CSR** field, paste the CS R.
   The request must begin with
   ----BEGIN CERTIFICATE REQUEST----
   and end with
   ----END CERTIFICATE REQUEST----
8. Click **Create**.
   The certificate (.pem) is downloaded immediately.
9. Click **Back** to return to the Built-in CA pane.

Creating a Backup of the Built-in 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**.
4. Click **PKI Certificates** .
5. Click the **Management Certificate Template** tab, and then click **Built-in CA**.
6. Click **Create CA Backup**.
7. Create and verify a password to secure the backup of the built-in CA certificate.
   You will need to enter this password to restore the certificate backup.

8. Click **Create Backup**.
   The backup file (.p12) is downloaded immediately.

9. Click **Back** to return to the Built-in CA pane.

Integrating with a Symantec CA

In the JSS, you can add Symantec as a certificate authority. Symantec certificates are managed in the JSS using the Symantec Managed PKI service.

Use the PKI Certificates settings in the JSS to perform the following tasks related to the Symantec CA:

- Configure Symantec as a PKI provider.
- View or refresh Symantec certificates.
- Export Symantec certificates.

Once communication with Symantec is successfully established, you can define which certificate to deploy to computers or mobile devices. For more information on how to issue Symantec certificates to computer and mobile devices, see the following Knowledge Base article:

Issuing Symantec Certificates to Computers and Mobile Devices in the JSS

Note: Inventory information for a user must be complete to properly issue a Symantec certificate to a computer or mobile device. Symantec certificates will not be issued or issued with missing attributes if there is incomplete data in inventory information for a user in the JSS.

Requirements

To integrate with Symantec as a CA, you need:

- Symantec Managed PKI service
- Web browser with Symantec PKI Client
- Administrator certificate from Symantec added to your local keychain

Configure Symantec as a PKI Provider

Adding Symantec as a PKI Provider allows you to add Symantec certificates in the JSS and issue them to computers and 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 **Global Management**.
4. Click **PKI Certificates** 🏅 .
5. Click the **Certificate Authority** tab, and then click **Configure New Certificate Authority**.
6. Select **Symantec**. Follow the onscreen instructions to configure Symantec as the PKI provider.

The newly configured CA is listed on the Certificate Authorities pane.

View or Refresh Symantec Certificates

You can view the following information for a certificate issued by Symantec:

- Subject name
- Serial number
- Device name associated with certificate
- Username associated with certificate
- CA Configuration name
- Date/time issued
- Expiration date/time
- Status
- Configuration profiles associated with the certificate

In the JSS, you can also refresh the status of a certificate issued by Symantec. Refreshing a certificate starts communication between the JSS and Symantec to display the current status of the 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**.

4. Click **PKI Certificates** 🏅 .

5. To view a list of Expiring, Active, Inactive or All certificates, click the number displayed in the corresponding column on the Certificate Authorities pane.
   A list of certificates issued by Symantec is displayed.

6. Click on the certificate subject of the certificate you want to view.
   Information about the certificate is displayed.

7. To refresh the certificate status, click **Refresh Certificate Status**.
   The status of the certificate is displayed as Active, Revoked or Expired.

8. Click **Done** to return to the list of certificates.

Export Symantec Certificates

The Symantec certificates displayed in PKI Certificates can be exported from the JSS to the following file formats:

- Comma-separated values file (.csv)
- Tab delimited text file (.txt)
- XML file

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**.

4. Click **PKI Certificates** 📜 .

5. To view a list of Expiring, Active, Inactive or All certificates, click the number displayed in the corresponding column on the Certificate Authorities pane.
A list of all certificates issued by Symantec is displayed.

6. Click **Export.**

7. Select the appropriate file format to use for the export and click **Next.**
The export begins immediately.

8. Once the certificates have been exported, click **Done**.

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 computers and mobile devices.

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.

Note: If you need to make changes to your organizational or third-party CA in the JSS, it is recommended that you contact Jamf Support. Changes to the PKI could lead to re-enrolling the mobile devices in your environment.

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**.

4. Click **PKI Certificates** 📜 .

5. Click the **Management Certificate Template** tab, and then click **External CA**.

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 computers and 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 computer and 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 Technical 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 computer and 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 computers and mobile devices so that a unique challenge password is used for each device. For more information, see [User-Initiated Enrollment for Computers](#) and [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**.

4. Click **PKI Certificates** .

5. Click the **Management Certificate Template** tab, and then click **External CA**.

6. At the bottom of the E xternal 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 Mac Computers
  Learn how the JSS uses certificate-based authentication to verify the identity of Mac 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.

Integrating with VPP

Integrating with Apple's Volume Purchase Program (VPP) is the first step to utilizing VPP-managed distribution. To integrate with VPP, you need to add one or more VPP accounts to the Jamf Software Server (JSS).

When you add a VPP account to the JSS, you upload the service token that you obtained from Apple, and specify the country associated with the VPP account. You can also specify other information about the account, such as the contact person and Apple ID.

In addition, you can specify that all content purchased with the VPP account is populated in the app and eBook catalogs.

After the JSS is integrated with VPP, you can use the JSS to distribute content via VPP-managed distribution by assigning content to users (user-based assignment), or directly to computers or mobile devices (device-based assignment). The following table outlines the VPP-managed distribution types.

VPP-Managed Distribution Type	Applies to	User Requirements	Basic Procedure
VPP-managed distribution for computers	Mac App Store apps	Computers with macOS 10.11 or later	VPP-managed distribution for computers involves the following steps: 1. Add a VPP account to the JSS. 2. Configure device assignments when distributing a Mac App Store app. (For information, see Mac App Store Apps.)
VPP-managed distribution for mobile devices	▪ App Store apps ▪ VPP store apps (including custom B2B apps)	Mobile Devices with iOS 9 or later	VPP-managed distribution for mobile devices involves the following steps: 1. Add a VPP account to the JSS. 2. Configure device assignments when distributing an App Store app or VPP store app. (For information, see App Store Apps.)
VPP-managed distribution for users	▪ App Store apps ▪ VPP store apps (including custom B2B apps for iOS devices) ▪ Mac App Store apps ▪ eBooks	▪ Mobile devices with iOS 7 or later ▪ Computers with macOS 10.9 or later ▪ Valid, personal Apple ID	VPP-managed distribution for users involves the following steps: 1. Add a VPP account to the JSS. 2. Invite users to register with VPP. (For information, see VPP User Registration.) 3.Create VPP user assignments in the JSS. (For information, see User-Based VPP Assignments.)

For more information on VPP and VPP-managed distribution, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Requirements

To add a VPP account to the JSS, you need a service token (.vpptoken) from Apple's VPP store.

Adding a VPP Account

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**.
4. Click **VPP Accounts** .
5. Click **New** .
6. Enter a display name for the account.
7. Click **Upload Service Token** and upload the service token (.vpptoken) for the account.
   Note: Each service token should only exist in one location at a time. If the service token you want to upload already exists in Apple's Profile Manager, delete the service token from Apple's Profile Manager before uploading it to the JSS.
8. Choose the country that is associated with the account.
9. (Optional) Select **Populate Purchased VPP Content** if you want content purchased with the VPP account to be populated in the app and eBook catalogs.
10. (Optional) Select **Notify users when an app is no longer assigned to them** if you want to send a notification to users when an app is revoked.
11. (Optional) If your environment integrates with Apple School Manager and you do not want the users that have Managed Apple IDs to receive a VPP invitation or get prompted to register with VPP, select **Automatically register with VPP if users have Managed Apple IDs**.
    Note: For users that have Managed Apple IDs to be automatically registered with VPP, you need to create a VPP invitation that includes the users in the scope and configure the invitation to automatically register the users. (For more information, see VPP User Registration.)
12. (Optional) Enter additional information about the account, including the contact person and Apple ID.
13. Click **Save**.

Related Information

For related information, see the following Knowledge Base article:

[Recently Purchased Content is not Displayed in VPP Assignment](#)
The Content tab displayed in the VPP Account setting can be used when content recently purchased from VPP fails to display in the JSS. The functionality available in that tab allows you to pull that content into the JSS.

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, configuration profiles, apps, and eBooks 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 and choose a priority for the category.
   Note: Priority is used for displaying the category in Self Service (e.g., A category with a priority of "1" is displayed before other categories).

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 **Global Management**.

4. Click **Categories** 📁 .

5. Click **New** ➕ .

6. Enter a display name and choose a priority for the category.
   Note: Priority is used for displaying the category in Self Service.

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 change the display name and/or priority as needed. Then click **OK**.

   - 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.

- Self Service Configuration Profiles for Computers
  Find out how to display or feature configuration profiles in one or more categories in Self Service.

- Mac App Store Apps
  Find out how to display or feature Mac App Store apps in one or more categories in Self Service.

- eBooks Available in the iBooks Store
  Find out how to display or feature eBooks that are available in the iBooks Store in one or more categories in Self Service.

- In-House eBooks
  Find out how to display or feature in-house eBooks in one or more categories in Self Service.

Event Logs

The Jamf Software Server (JSS) records events in the form of logs. You can view the status of these events using the Event Logs.

The Event Logs pane displays the following information:

- Date/time the status was last updated for an event
- Name of the device that is in the scope of an event
- Object type (such as "macOS Configuration Profile" or "Casper Imaging")
- Object name associated with an event (such as the name of a configuration profile or "Standard Imaging")
- Action of the event (such as "Install" or "Imaging")
- Status of the event (such as "Started" or "Completed")

Event logs can be viewed for macOS configuration profiles and iOS configuration profiles. As of the Casper Suite v9.7, event logs can also be viewed for imaging.

Depending on your system configuration:

- Some historical event logs data may not be available for macOS configuration profiles and iOS configuration profiles installed using v9.63 or earlier.
- Some historical event logs data may not be available for imaging performed using Casper Imaging v9.66 or earlier.

Requirements

To access Event Logs, a JSS user account or group must have the Administrator or Auditor privilege set. (For more information, see JSS User Accounts and Groups.)

Viewing Event Logs

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**.

4. Click **Event Logs** 📅ⓘ .
   The event logs are displayed on the pane.

   - "Standard Imaging" includes Target Mode Imaging (TMI) events.
     Note: All migrated imaging events will be displayed as "Standard Imaging".

   - "Autorun Imaging" represents events that include Autorun data.

   - "PreStage Imaging" represents events that include PreStage data.

5. Do one of the following:

   - To view details about a particular device, click a device in the Device Name column.

   - (Configuration profiles only) To view the object associated with an event, click an object in the Object Name column.

   - To view log details, click a status in the Status column.

Related Information

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

- Computer Configuration Profiles
  Learn about macOS configuration profiles, including how to view the status and the logs of a macOS configuration profile.

- Mobile Device Configuration Profiles
  Learn about iOS configuration profiles, including how to view the status and the logs of an iOS configuration profile.

- About Imaging
  Learn about imaging and the different imaging methods.

Webhooks

The Webhooks setting allows you to create outbound webhooks for any event in the Events API. In conjunction with the Events API, Webhooks allows you to use real-time events from the Jamf Software Server (JSS) to build custom workflows that occur on demand using the programming language of your choice. For example, you could configure a webhook to send an event to an instant message plug-in you have written that will notify a chatroom when a third-party macOS software title in the JSS has been updated.

For more information about webhooks, see the following website:
https://webhooks.pbworks.com/w/page/13385124/FrontPage

Configuring a Webhook

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**.

4. Click **Webhooks** 🔗 .

5. Click **New** ➕ .

6. Enter a display name for the webhook.

7. Enter a URL for the webhook to post to.

8. Choose either "XML" or "JSON" as the format for sending the webhook information.

9. Choose the event that will trigger the webhook.

10. Click **Save**.

AirPlay Permissions

AirPlay Permissions allow you to map one or more mobile devices to an AirPlay destination, such as an Apple TV, so that those mapped mobile devices can be automatically paired with the AirPlay destination. When a mobile device is mapped to an AirPlay destination via AirPlay Permissions, you can also choose to automatically give the mobile device the password for the AirPlay destination, or to make only the permitted AirPlay destinations available to that device.

Mobile Device Inventory Field Mapping

When configuring AirPlay Permissions, you must choose a mobile device inventory field to use to map devices to permitted AirPlay destinations. The inventory field you choose is automatically mapped to an AirPlay destination when the value in that field is the same for both the mobile device and the AirPlay destination device.

Requirements

To use AirPlay Permissions, you need:

- Mobile devices with iOS 8 or later
- Apple TV devices enrolled with the JSS

Creating an AirPlay Permission

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**.

4. Click **AirPlay Permissions** .

5. Click **New** ➕ .

6. Enter a display name for the AirPlay Permission.

7. Select the inventory field from the **Mapping Field** pop-up menu.

8. (Optional) Enable settings for restricting AirPlay destinations and automating passwords, as needed.

9. Click **Save**.

10. Repeat this process for each new AirPlay Permission you want to create.

   The mobile devices and AirPlay destinations that share the selected inventory field are mapped immediately.

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 content delivery networks (CDNs) to host files: - Rackspace Cloud Files - Amazon Web Services - Akamai - Jamf Cloud Distribution Service (JCDS)	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	Mac or Linux

	File Share Distribution Point	Cloud Distribution Point	JDS Instance
Protocol	AFP, SMB, HTTP, or HTTPS	HTTPS	HTTPS
Ports	- AFP: 548 - SMB: 139 - HTTP: 80 - HTTPS: 443	443	443

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 a cloud distribution point 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.

	File Share Distribution Point	Cloud Distribution Point	JDS Instance
Selective Replication	Not available when replicating to file share distribution points.	Available when replicating to a cloud distribution point if the master distribution point is a JDS instance or file share distribution point. The files for replication must be specified in the JSS and the replication initiated from Casper Admin.	Not available when replicating to root JDS instances. Available when replicating to non-root JDS instances. The files for replication must be specified in the JSS. The replication from non-root parent to child instances is initiated on check in with the JSS.

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 **Server Infrastructure**.

4. 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**.

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 content delivery network (CDN) to host packages, in-house apps, and in-house eBooks. The Jamf Software Server (JSS) supports the following content delivery services:

- Rackspace Cloud Files
- Amazon S3 or Amazon CloudFront
- Akamai NetStorage
- Jamf Cloud Distribution Service (JCDS)

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 if the master is a JDS instance or file share distribution point.

The JSS supports the use of signed URLs created with Amazon CloudFront. It also supports Akamai Remote Authentication. For more information about signed URLs created with CloudFront, see the following website:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

For more information about Akamai Remote Authentication, contact your Akamai Account Manager.

If your JSS is hosted in Jamf Cloud and you have the subscription-based option, you can use JCDS as your cloud distribution point. For more information about pricing, contact your Technical Account Manager.

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.)

Files that are uploaded to a cloud distribution point cannot have filenames that include the following characters:

/ : ? < > \ * | " [ ] @ ! % ^ #

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 **Server Infrastructure**.

4. Click **Cloud Distribution Point** ☁ .

5. Click **Edit**.

6. Choose a content delivery network from the **Content Delivery Network** 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 content delivery network.

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

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

3. Click **Server Infrastructure**.

4. 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 via Casper Admin. 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.

For related information, see the following Knowledge Base article:

Information Required to Configure a Cloud Distribution Point in the JSS
Learn about the information that must be obtained from your cloud services provider to configure the cloud distribution point in the JSS.

For more information about content delivery services, visit the following websites:

- Rackspace Cloud Files
  http://www.rackspace.com/cloud/files/

- Amazon S3
  http://aws.amazon.com/s3/

- Amazon CloudFront
  http://aws.amazon.com/cloudfront/

- Akamai NetStorage
  http://www.akamai.com/html/solutions/netstorage.html

- Jamf Cloud Distribution Service
  http://www.jamfsoftware.com/products/jamf-cloud/

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 Mac 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
- macOS 10.7 or later with macOS Server 1.4.3 or later installed

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) 6.4, 6.5, 6.6, or 7.0
  Note: To install a JDS instance on a Linux operating system that is running on a virtual machine, you need a virtualization platform that provides SMBIOS information.

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 Mac

1. Copy the JDS Installer for Mac (`JDS Installer.pkg`) to the server on which you plan to install a JDS instance.
   Note: To obtain the JDS Installer for Mac, log in to Jamf Nation and go to the following page: https://www.jamf.com/jamf-nation/my/products

2. Double-click the installer.

3. Follow the onscreen instructions to complete the installation.

Installing a JDS Instance on Linux

1. Copy the JDS Installer for Linux (`JDS Installer.run`) to the server on which you plan to install a JDS instance.
   Note: To obtain the JDS Installer for Linux, log in to Jamf Nation and go to the following page: https://www.jamf.com/jamf-nation/my/products

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 **Server Infrastructure**.

4. Click **JDS Instances** 🔧 .

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 replicated to child JDS instances from their non-root parent instances on check in with the JSS. 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 **Server Infrastructure**.

4. Click **JDS Instances** .

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 **Server Infrastructure**.

4. Click **JDS Instances** .

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 **Server Infrastructure**.
4. Click **Software Update Servers** 🌐 .
5. Click **New** ➕ .
6. Configure the settings on the pane.
7. Click **Save**.

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:

NetBoot/SUS Appliance
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 **Server Infrastructure**.
4. Click **NetBoot Servers** 🖥 .
5. Click **New** + .
6. Configure the settings on the pane.
7. Click **Save**.

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 articles:

- Creating a NetBoot Image and Setting Up a NetBoot Server
  Find out how to host a NetBoot server on a server with macOS Server installed.
- Booting macOS 10.11 or Later Computers to a NetBoot Image Using a Policy or Casper Remote
  Find out how to add a trusted NetBoot server so that you can boot a macOS 10.11 or later computer to a NetBoot image using a policy or Casper Remote.

For related information, see the following:

NetBoot/SUS Appliance
Find out how to host a NetBoot server on Linux.

Jamf Infrastructure Manager Instances

A Jamf Infrastructure Manager instance is a service that is managed by the Jamf Software Server (JSS). It can be used to host the following:

- **LDAP Proxy**—This allows traffic to pass securely between a JSS and an LDAP directory service. The Infrastructure Manager and the LDAP Proxy typically reside within the DMZ.
  The LDAP Proxy requires integration with an LDAP directory service.
  For more information, see LDAP Proxy.

- **Healthcare Listener**—This allows traffic to pass securely from a healthcare management system to a JSS.
  For more information, see Healthcare Listener.

When you install an instance of the Infrastructure Manager, the JSS allows you to enable the LDAP Proxy or the Healthcare Listener. Infrastructure Manager instances can be installed on Linux and Windows. For more information, see the *Jamf Infrastructure Manager Installation Guide*.

Viewing Inventory Information for a Jamf Infrastructure Manager Instance

The JSS displays the following inventory information for each Infrastructure Manager instance:

- Last Check-in

- IP Address at Last Check-in

- Operating System

- Operating System Version

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.**

4. In the "Computer Management–Server Infrastructure" section, click **Infrastructure Managers** 🔵 .
   A list of Infrastructure Manager instances is displayed along with the services that are installed on each instance.

5. Click the Infrastructure Manager instance you want to view inventory information for.

Further Considerations

- When editing an Infrastructure Manager instance, only the display name and recurring check-in frequency can be changed.
  Note: The default check-in frequency at which the Infrastructure Manager instance checks in with the JSS is 30 seconds.

- An Infrastructure Manager instance cannot be deleted if there are dependencies for the Infrastructure Manager. For example, an Infrastructure Manager cannot be deleted if there is an LDAP Proxy hosted on it. To delete the Infrastructure Manager, you must first disable the LDAP Proxy.

- If a Healthcare Listener is hosted on the Infrastructure Manager, the Healthcare Listener is deleted when the Infrastructure Manager is deleted.

Related Information

Email Notifications
Learn how to enable an email notification in the event that an Infrastructure Manager instance does not check in with the JSS.

Healthcare Listener

The Healthcare Listener is a service that receives ADT messages from a healthcare management system and allows traffic to pass securely from the healthcare management system to the Jamf Software Server (JSS). When the Healthcare Listener receives an ADT message, the JSS interprets the message to automatically send remote commands to mobile devices based on rules you configure. (For more information about the communication process of the Healthcare Listener, see the Healthcare Listener Communication Knowledge Base article.)

For example, you could configure a rule so that when the Healthcare Listener receives a "Patient Discharge" ADT message, the JSS sends a Wipe Device command to the device assigned to the patient room.

When you configure the Healthcare Listener, you must do the following:

- Specify IP addresses or a range of IP addresses to accept incoming messages from
  Note: The Healthcare Listener is compatible with IPv4 and IPv6 connection methods.

- Specify a port number
  Note: The default port value is 8080. This should be changed to the port number that the Healthcare Listener uses to receive healthcare management system communications.

- Add rules by configuring settings that enable the JSS to send commands to devices (For more information, see Healthcare Listener Rules.)
  You can also enable email notifications in the event that a command is not sent.

In addition, email notifications can be sent from the JSS when a remote command fails to send or remains in a pending state. (For more information, see Notifications.)

The Healthcare Listener is hosted by the Jamf Infrastructure Manager, a service that is managed by the JSS. After you install an instance of the Infrastructure Manager, the JSS allows you to enable the Healthcare Listener. For more information, see Jamf Infrastructure Manager Instances.

Healthcare Listener Rules

Configuring a rule enables the JSS to send remote commands to devices when the Healthcare Listener receives an ADT message. If you want to send more than one type of command or use more than one type of ADT message, you must configure a separate rule for each. You can configure as many rules as your organization requires.

The following table provides an overview of the settings you can configure for each rule:

Setting	Description

Remote Command	This setting allows you to specify which command you want sent from the JSS when the Healthcare Listener receives an ADT message. You can choose from the following commands:
	
	▪ Wipe Device
	  Note: If a mobile device has Activation Lock enabled, the Activation Lock is cleared when the device is wiped.
	▪ Lock Device
	▪ Clear Passcode
	▪ Enable Lost Mode
	  Choosing Enable Lost Mode requires you to configure custom messaging.
	▪ Disable Lost Mode
	
	For more information, see Remote Commands for Mobile Devices.

ADT Message	For the JSS to send commands to devices, the Healthcare Listener must receive an ADT message. You can choose from the following ADT message types: ▪ Admit/Visit Notification (ADT-A01) ▪ Patient Transfer (ADT-A02) ▪ Patient Discharge (ADT-A03) ▪ Cancel Admit/Visit Notification (ADT-A11) ▪ Cancel Transfer (ADT-A12) ▪ Cancel Discharge/End Visit (ADT-A13)
Mapping Fields	ADT messages contain multiple fields of information that the Healthcare Listener can extract. You can choose which ADT message field to extract, and then map that field to an attribute from user and location information in device inventory. For example, you can choose the field that returns "bed number" and map that field to the "Room" attribute in a device's inventory information. The command you specify is then sent to devices that match the inventory attribute you select. You can choose from the following ADT message fields: ▪ Patient Visit - Person Location - Bed (PV1-3-3) ▪ Patient Visit - Prior Person Location - Bed (PV1-3-6) In addition, you can create an extension attribute for a specific inventory attribute that fits your environment. After you create the extension attribute, it is available as an option. (For more information about creating an extension attribute for a mobile device, see Mobile Device Extension Attributes.)
Email Notifications	Email notifications can be sent from the JSS to specified users for the following events: ▪ A command fails to send. ▪ A command is in a pending state after a specified amount of time. To enable email notifications, you need an SMTP server set up in the JSS. (For more information, see Integrating with an SMTP Server.)

Requirements

To configure the Healthcare Listener and take full advantage of its latest features and enhancements, you must install the latest version of the Jamf Infrastructure Manager. (For more information, see the *Jamf Infrastructure Manager Installation Guide*.)
Note: To install the latest version of the Jamf Infrastructure Manager that hosts the Healthcare Listener, contact Jamf Support.

In addition, you need to ensure that your healthcare management system is compliant with Health Level Seven (HL7) messaging and that it communicates the version of HL7 protocol. For more information about HL7 messaging, see www.hl7.org.

Setting up the Healthcare Listener

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

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

3. Click **Server Infrastructure**.

4. Click **Infrastructure Manager Instances** 🔗 .
   A list of Infrastructure Manager instances is displayed along with the services that are installed on each instance.

5. Click the Infrastructure Manager instance with the Healthcare Listener that you want to configure.

6. Click **Edit**.

7. Select the **Enable Healthcare Listener** checkbox.

8. Enter a display name for the Healthcare Listener.
   This is the name that is displayed for the Healthcare Listener on the Infrastructure Manager. (For more information about viewing the services that are installed on an Infrastructure Manager instance, see Jamf Infrastructure Manager Instances.)

9. To specify the IP addresses to accept incoming ADT messages from, do one of the following:

   - Select **All IP addresses** to accept incoming messages from any IP address.

   - Select **Single IP address or Range of IP addresses** to specify the IP addresses to accept incoming ADT messages from, and do the following:

     a. To specify a single IP address, click the **(+) Add** button for Single, and enter the IP address.

     b. To specify a range of IP addresses, click the **(+) Add** button for Range, and enter the starting and ending IP addresses.

10. Enter the port number of your healthcare management system.

11. Click **Save**.

After the Healthcare Listener is set up, you can add rules. Adding a rule enables the JSS to send remote commands to devices.

Adding a Healthcare Listener Rule

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

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

3. Click **Server Infrastructure**.

4. Click **Infrastructure Manager Instances** .
   A list of Infrastructure Manager instances is displayed along with the services that are installed on each instance.

5. Click the Infrastructure Manager instance with the Healthcare Listener that you want to add a rule to.

6. Click **Edit**, and then click the **Add (+)** button.

7. Choose the remote command you want the JSS to send to devices when the Healthcare Listener receives an ADT message.

8. Choose which ADT message the Healthcare Listener can receive.

9. Use the **Field Mapping** options to map a field from the ADT message to an attribute of inventory information.

10. (Optional) To enable email notifications, click the **Notifications** tab, and do the following:

    a. Select the **Enable Email Notifications** checkbox.

    b. Enter an email address or multiple email addresses separated by a line break or a comma.

    c. Use the **Email Delay** pop-up menu to choose how many minutes to wait when a command is pending before sending an email to specified email addresses.

11. Click **Save**.

When the Healthcare Listener receives an ADT command, the JSS sends the specified command to devices that are mapped to the field in the ADT message.

Further Considerations

- If you edit or delete a rule that has a remote command in a pending state, the pending command is still sent to devices regardless of editing or deleting the rule.

- If the Healthcare Listener cannot communicate with the JSS (e.g., during a JSS upgrade), any ADT messages that the Healthcare Listener receives during that time are saved and then processed once communication is re-established.

Related Information

- Viewing Audit Logs for a Mobile Device
  Find out how you can view the date/time of the remote command that was sent to a specific mobile device in the device's inventory information.

- Change Management
  Find out how to view Healthcare Listener changes that happen in the JSS.

LDAP Proxy

The Jamf Software Server (JSS) allows you to enable an LDAP Proxy. Enabling an LDAP Proxy creates a secure tunnel to allow traffic to pass between a JSS and an LDAP directory service. For example, if your environment uses a firewall, an LDAP Proxy can be used to allow a directory service on an internal network to pass information securely between the directory service and the JSS.

The LDAP Proxy is hosted by the Infrastructure Manager, a service that is managed by the JSS. After you install an instance of the Infrastructure Manager, the JSS allows you to enable an LDAP Proxy if you have an LDAP server set up in the JSS. For more information, see Jamf Infrastructure Manager Instances.

Note: The LDAP Proxy that is hosted on the Infrastructure Manager is not the same service as the open source NetBoot/SUS/LP server. For more information about the open source NetBoot/SUS/LP server, see the following webpage:
https://github.com/jamf/NetSUS/tree/master/docs .

Network Communication

When using the LDAP Proxy, the Jamf Infrastructure Manager can be customized for incoming access by any available port 1024 or greater. The port used must be opened, inbound, on your firewall and also on the computer on which the Infrastructure Manager is installed. The recommended port is 8389 for communication between your JSS and the Infrastructure Manager.

For communication between the Infrastructure Manager and an LDAP directory service, your LDAP server's regular incoming port is used. This port is specified in the LDAP server's configuration in the JSS. The most common configurations are port 389 for LDAP and port 636 for LDAPS. This communication occurs between the Infrastructure Manager in the DMZ and an internal LDAP directory service only.

Note: The Infrastructure Manager does not support Network Address Translation (NAT).

When using the JSS hosted on Jamf Cloud, the necessary external IP addresses for Jamf Cloud must be allowed inbound to the Infrastructure Manager. For more information, see the Permitting Inbound /Outbound Traffic with Jamf Cloud Knowledge Base article.

Note: Internal domain addresses (for example, .local, .company, or .mybiz) are not supported at this time. The Infrastructure Manager must be resolvable to the external JSS server.

Requirements

To configure an LDAP Proxy, you need the following:

- An Infrastructure Manager instance installed and configured (For more information, see the *Jamf Infrastructure Manager Installation Guide*.)

- An LDAP server set up in the JSS (For more information, see [Integrating with LDAP Directory Services](#).)

Configuring the LDAP Proxy

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.**
4. Click **LDAP Servers** 📖 .
5. Click the LDAP Server to which you want to assign an LDAP Proxy.
6. Click **Edit**.
7. Select the **Enable LDAP Proxy** checkbox.
8. Select the proxy server to use and enter a port number.
9. Click **Save**.

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**.

4. Click **Buildings** 🏢 or **Departments** 🏢 .

5. Click **New** + .

6. Enter a display name for the building or department.

7. Click **Save**.

Related Information

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

- Viewing and Editing Inventory Information for a 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 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 multiple computers to a building or department.

- Mass Editing the Building or Department for Mobile Devices
  Find out how to use the mass edit function to add multiple mobile devices 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**.
4. Click **Network Segments** 🔵 .
5. Click **New** ➕ .
6. Configure the network segment using the settings on the pane.
7. Click **Save**.

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.

iBeacon Regions

The Jamf Software Server (JSS) allows you to utilize Apple's iBeacon technology to monitor when computers and mobile devices enter or exit an iBeacon region. This allows you to ensure that configuration profiles and policies are only installed on a device when the device is in the specified region.

You can use iBeacon regions as the basis for the following:

- The scope of a configuration profile
- The scope of a policy (This initiates the policy the first time that a computer checks in to the JSS while in the specified region.)
- A custom trigger for a policy (The event name for initiating a policy when an iBeacon region change occurs is "beaconStateChange". This initiates the policy immediately when a computer enters the specified region.)

For more information about iBeacon devices and iBeacon regions, see Apple's documentation at: https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf

If you have an iBeacon device in your environment, you can add that device to the JSS as an iBeacon region. The JSS can then detect when computers and mobile devices enter or exit the region.

Requirements

To monitor an iBeacon region for computers, you need:

- One or more iBeacon devices in your environment
- Computers that are Bluetooth Low Energy capable and have Bluetooth turned on
- The Computer Inventory Collection settings configured to monitor iBeacon regions (For more information, see Computer Inventory Collection Settings.)

To monitor an iBeacon region for mobile devices, you need:

- One or more iBeacon devices in your environment
- Mobile devices with:
  - iOS 7 or later
  - Bluetooth Low Energy capability
  - Bluetooth turned on
  - Self Service Mobile for iOS installed (For more information, see Installing Self Service on Mobile Devices.)
  - Location Services enabled for Self Service Mobile for iOS
- The Mobile Device Inventory Collection settings configured to monitor iBeacon regions (For more information, see Mobile Device Inventory Collection Settings.)

Note: iBeacon region monitoring is not available for personally owned devices.

Adding an iBeacon Region

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**.

4. Click **iBeacons** ◎ .

5. Click **New** ➕ .

6. Enter a display name for the iBeacon region.

7. Define the iBeacon region using the settings on the pane.

8. Click **Save**.

Related Information

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

- Scope
  Find out how to configure the scope of configuration profiles and policies based on iBeacon regions.
- Computer Inventory Collection Settings
  Find out how to configure the Computer Inventory Collection settings to monitor iBeacon regions.
- Mobile Device Inventory Collection Settings
  Find out how to configure the Mobile Device Inventory Collection settings to monitor iBeacon regions.

For related information, see the following Knowledge Base article:

Smart Group and Advanced Search Criteria for iBeacon Regions
Learn about the smart group and advanced search criteria available for iBeacon regions.

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**.

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**.

Adding Items to a Site

The following items can be added to a site:

- Computers
- Mobile devices
- Users
- 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
- Device Enrollment Program instances
- PreStage enrollments
- VPP accounts
- Network integration instances

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 the **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 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 the **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 Mobile Device.)

There are several ways to add users to a site:

- Add the user to a computer or mobile device that belongs to a site.

- Add a computer or mobile device with a user assigned to it to a site.

- Mass add users to a site for users in the JSS. (For more information, see Adding Multiple Users to a Site.)

- Manually add users to a site for individual users in the JSS. (For more information, see Viewing and Editing Inventory Information for a User.)

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.

Network Integration

The JSS can be integrated with a network access management service, such as Cisco Identity Services Engine (ISE). Network integration allows the service to communicate with the JSS to verify that the computers and mobile devices on your network are compliant with your organization's standards. With information from the JSS, the service can determine the level of network access to grant to a computer or mobile device, provide messaging to end users, and refer end users to enroll their computers and mobile devices to the JSS to become compliant.

Note: When the network access management service refers end users to enroll their computer or mobile device with the JSS, an enrollment URL is provided to the user in a webpage when they access the Internet. The end user can then access the enrollment URL to enroll with the JSS via user-initiated enrollment. (For more information, see User-Initiated Enrollment Settings.)

Network integration can also allow the network access management service to send remote commands to computers and mobile devices via the JSS, including passcode lock and wipe commands.

Creating a network integration instance in the JSS prepares the JSS to integrate with a network access management service. This allows you to do the following:

- When sites are defined in the JSS, select the site to add the network integration instance to.
- Select the saved advanced computer search and advanced mobile device search to be used by the network access management service to verify computers and mobile devices that are compliant with your organization's standards. Computers and mobile devices that appear in the search results are reported as compliant to the network access management service.
- Specify compliance verification failure and compliance remediation messaging that can be displayed to end users via the network access management service.
- Configure the passcode to be used when remotely locking or wiping computers via the network access management service.
- After saving the network integration instance, view the network integration URL to be used by the network access management service to communicate with the specific JSS network integration instance.

Important: When using network integration on a per-site basis in the JSS, ensure that any site-specific configuration profiles and policies in the JSS do not conflict with computer and mobile device compliance verification performed through network integration.

Requirements

For more information and requirements for configuring your network access management service to communicate with an MDM server, see your vendor's documentation.

To allow the network access management service to send remote commands via the JSS, your environment must meet the requirements for sending remote commands to computers and mobile devices. (For more information, see Remote Commands for Computers and Remote Commands for Mobile Devices.)

Adding a Network Integration Instance

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**.

4. Click **Network Integration** 🌐 .

5. Click **New** ＋ .
   Note: Only one network integration instance can be added per site in the JSS. If all sites already have a network integration instance, you will not be able to add a new one.

6. Configure the network integration instance using the settings on the pane, including the site, the advanced computer search and advanced mobile device search to be used for compliance verification, compliance messaging to be displayed to users, and the remote lock and wipe passcode setting for computers.
   Note: If you select the "Create Random Passcode" option for the passcode assignment method for computers, to identify the passcode used for a remote lock or wipe on a specific computer, you will need to view the management history for the computer in the JSS. (For information, see Viewing the History for a Computer.)

7. Click **Save**.
   After saving the network integration instance, a unique network integration URL appears at the bottom of the pane. This URL will be used by the network access management service to communicate with the specific JSS network integration instance.

Related Information

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

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

▪ Advanced Computer Searches
   Learn how to create and save an advanced computer search.

▪ Advanced Mobile Device Searches
   Learn how to create and save an advanced mobile device search.

Scope

Scope gives you granular control over which computers, mobile devices, and users 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:

- Individual computers, mobile devices, or users
- Computer, mobile device, or user groups
- Departments
- Buildings
- LDAP or local users
- LDAP user groups
- Network segments
- Classes
- iBeacon regions

The items available vary depending on the remote management task you are configuring the scope for. For example, only eBook scope can be based on classes.

Note: Scope cannot be based on personally owned mobile devices.
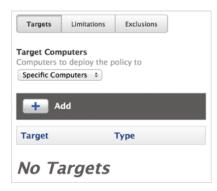
Configuring Scope

For most remote management tasks, configuring the scope involves adding targets, limitations, and exclusions. (The process varies depending on the remote management task you are configuring the scope for.)

Adding Targets

Targets make up the initial pool of computers, mobile devices, or users that receive the remote management task. You can add all computers, mobile devices, or users, or you can add a combination of specific items (e.g., computers, groups, buildings).

1. On the Targets pane, use the pop-up menu(s) to choose items to add to the scope.
   Note: All computers, mobile devices, and/or users selected from the pop-up menus will be added to the scope. One pop-up menu selection does not override another. For example, selecting "All Mobile Devices" and "Specific Users" as targets to the scope of an eBook will cause the eBook to be distributed to all mobile devices, as well as any computers or mobile devices that the chosen user or users are assigned to.

2. If you chose to add specific items:

   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 on the Targets pane.

Adding Limitations

Adding limitations to the scope of a remote management task allows you to do the following:

- **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.

- **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.

- **Limit policies and configuration profiles to devices in the target when the devices are in a specific iBeacon region.** For example, if you want to install a configuration profile on mobile devices when they are in a specific iBeacon region, you can add the iBeacon region as a limitation.

1. On the Limitations pane, click **Add** ⊞ .

2. On each tab, add items as needed.
   To add a network segment, click the **Network Segments** tab and then click **Add** for the network segment.

149

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

To add an LDAP user group, click the **LDAP 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.

3. Click **Done**.
   The items you added are displayed in a list on the Limitations pane.

Adding 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.

You can also add iBeacon regions as exclusions to the scope of policies and configuration profiles. For example, if you want to prevent a mobile device from having a configuration profile installed when it is in a specific iBeacon region, you can add the iBeacon region as an exclusion.

1. On the exclusions pane, click **Add** [+] .

2. On each tab, add items as needed.
   To add an LDAP or local user, click the **LDAP/Local Users** tab. Then enter the username in the search field and click **Add**.

   To add an LDAP user group, click the **LDAP 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.

3. Click **Done**.
   The items you added are displayed in a list on the Exclusions pane.

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**.

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**.
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**.
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.
- Configure SSL certificate verification.
- Specify the condition under which the checksum will be used to validate packages. If you choose to validate packages, the validation occurs after the package is downloaded.
- Specify a maximum clock skew between managed computers and the JSS host server.

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

Configuring SSL Certificate Verification

Configuring the SSL Certificate Verification setting in the JSS ensures that computers only communicate with a host server that has a valid SSL certificate. This prevents computers from communicating with an imposter server and protects against man-in-the-middle attacks.

Consider the following when configuring SSL certificate verification:

- If you are using the self-signed certificate from Apache Tomcat that is built into the JSS, you must select "Always except during enrollment".
- If you are using an SSL certificate from an internal CA or a trusted third-party vendor, select either "Always" or "Always except during enrollment". It is recommended that you use "Always" if computers in your environment are configured to trust the certificate before they are enrolled.

For more information, see the following Knowledge Base articles:

- Safely Configuring SSL Certificate Verification
- Change to the SSL Certificate Verification Setting in the Casper Suite v9.98 or Later

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**.

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 Mac computers can use to verify the identity of the JSS.
- Calculating a Checksum
  Learn about using the checksum to validate a package and how to manually calculate the value.
- PreStage Imaging
  Learn about using PreStage Imaging.
- Autorun Imaging
  Learn about using Autorun Imaging.

For related information, see the following Knowledge Base articles:

- Certificate-Based Authentication for Mac Computers
  Learn how the JSS uses certificate-based authentication to verify the identity of Mac computers.
- Safely Configuring SSL Certificate Verification
  Learn about why it is important to configure SSL Certificate Verification in the JSS and how to do so without putting your environment at risk.

Enrollment of Computers

About Computer Enrollment

Enrollment is the process of adding Mac computers to the Jamf Software Server (JSS). When computers are enrolled, inventory information for the computers is submitted to the JSS.

Enrolling 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 computers, you specify a local administrator account that you want to use to manage them (called the "management account").

Note: Enrolling computers with macOS 10.9 or earlier using a PreStage enrollment allows you to search and report on the computers as part of your inventory; however, this process alone does not make the computers managed by the JSS.

There are several ways to enroll computers with the JSS:

- **User-initiated enrollment**—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.
- **Use a QuickAdd package created with Recon**—You can use Recon to create a QuickAdd package that enrolls 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 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 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 computer that you want to enroll, you can run Recon locally on the computer.
- **Image computers**—You can enroll computers by imaging them with a configuration that is associated with a management account.
- **Use a PreStage enrollment**—A PreStage enrollment allows you to store enrollment and computer setup settings in the JSS and use them to enroll new computers with the JSS. In addition to reducing the amount of time and interaction it takes to prepare new computers for use, this enrollment method makes the computers MDM capable. Computers with macOS 10.10 or later can also be managed automatically when using a PreStage enrollment.
This enrollment method requires an Apple Deployment Programs account. For more information, see the Integrating with Apple's Device Enrollment Program (DEP) Knowledge Base article.

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 a computer by running Recon remotely.

- Local Enrollment Using Recon
  Find out how to enroll a 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.

- Computer PreStage Enrollments
  Find out how to enroll computers using a PreStage enrollment.

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 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 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. The enrollment URL is the full URL for the Jamf Software Server (JSS) followed by "/enroll". For example:

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

You can provide the enrollment URL to users by doing the following:

- **Provide the URL in the way that best fits your environment**
  Simply provide the URL to users in the way that best meets your needs. You can add a computer to a site when using this method.

- **Send an enrollment invitation to users via email**
  This allows you to create an email invitation in the JSS and send it to one or more users. It gives you more control over user access to the enrollment portal by allowing you do the following:

  - Set an expiration date for the invitation
  - Require users to log in to the portal
  - Allow multiple uses of the invitation
  - Add the computer to a site during enrollment
  - View the status of the invitation

Users can log in to the enrollment portal using an LDAP directory account or a JSS user account. When a user logs in with an LDAP directory account, user and location information is submitted to the JSS during enrollment. When a user logs in with a JSS user account, it allows an LDAP user to be assigned to the computer.

Requirements

To allow computers to be enrolled with user-initiated enrollment, you need:

- User-initiated enrollment enabled (For more information, see User-Initiated Enrollment Settings.)
- The user-initiated enrollment QuickAdd package configured in the JSS (For more information, see User-Initiated Enrollment Settings.)
  If the QuickAdd package is signed, target computers must have a Certification Authority (CA) 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

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.)

For users to log in to the enrollment portal with an 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

You can send an email invitation that contains the enrollment URL from the JSS. Users click the enrollment URL in the email message to access the enrollment portal.

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**.

4. Click **New** + .

5. Follow the onscreen instructions to send the enrollment invitation.

   An enrollment invitation is immediately sent to the 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**.

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.

Related Information

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

- User-Initiated Enrollment Settings
  Learn about the settings you can configure for user-initiated enrollment.

- User-Initiated Enrollment Experience for Computers
  Learn about the steps users take to enroll computers.

User-Initiated Enrollment Experience for Computers

When a user accesses the enrollment URL from their computer, they are guided through the following steps:

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 about enrollment invitations, see User-Initiated Enrollment for Mobile Devices.)

2. When prompted, the user must choose the site that they are associated with.
   If the user is associated with multiple sites, they must select the site that will assign the appropriate settings to the device.
   If the user signed in with a JSS user account, they can assign an LDAP user to the computer at this time.

3. If the user signed in with an LDAP directory account and the text for a End User License Agreement (EULA) was entered in the JSS, the user must accept the EULA to continue.

4. When prompted, the user must download the QuickAdd package.

5. After the QuickAdd package downloads, the user must double-click the QuickAdd package installer and follow the onscreen instructions to install the package.

6. When the installation is complete, an enrollment complete message is displayed in the enrollment portal.

   The computer is enrolled with the JSS.

Related Information

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

User-Initiated Enrollment Settings
Learn about the settings you can configure for user-initiated enrollment.

QuickAdd Packages Created Using Recon

You can use Recon to create a QuickAdd package that enrolls Mac 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:

- Specify that the management account password be randomly generated.
- Create the management account during enrollment and configure settings for the account.
- Ensure that SSH (Remote Login) gets enabled on computers that have it disabled.
- Ensure that computers launch Self Service after they are enrolled.
- Ensure that computers that already belong to a site will retain existing site membership.
- 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:

- macOS 10.7 or later
- An installer certificate (.p12) from Apple in the System keychain in Keychain Access (For more information, see the Obtaining an Installer Certificate from Apple 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.
   To randomly generate a management account password, choose "Randomly generate password" from the Method for Setting Password pop-up menu.
   The randomly generated password will contain eight characters by default.
   Note: If you choose to randomly generate passwords and create the management account during enrollment, the **Hide management account** and **Allow SSH for management account only** checkboxes are not available by default. To make these options available, you need to first select the **Create management account if it does not exist** checkbox, and then select the **Randomly generate password** method for setting the management account password.

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. To add the computers to a site, choose a site from the **Site** pop-up menu.

9. To ensure that computers that already belong to a site will retain their existing site membership, select the **Use existing site membership, if applicable** checkbox.

10. 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 Mac 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.

- 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.

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.

   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.

Remote Enrollment Using Recon

If you know the IP address of the Mac 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.

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. This assigns the user to the computer during enrollment. (For more information on setting up an LDAP server, see Integrating with LDAP Directory Services.)
   If you specified a username that matches an existing username in the JSS, the user is assigned to the computer during enrollment. If you specified a username that does not match an existing username in the JSS, the user is created and assigned to the computer during enrollment.

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 Mac 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.

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. This assigns the user to the computer during enrollment. (For more information on setting up an LDAP server, see Integrating with LDAP Directory Services.)
   If you specified a username that matches an existing username in the JSS, the user is assigned to the computer during enrollment. If you specified a username that does not match an existing username in the JSS, the user is created and assigned to the computer during enrollment.

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**.

Computer PreStage Enrollments

A PreStage enrollment allows you to store enrollment and Mac computer setup settings in the Jamf Software Server (JSS) and use them to enroll new Mac computers with the JSS. This reduces the amount of time and interaction it takes to prepare Mac computers for use.

Before you can use a PreStage enrollment, you need to integrate the JSS with the Device Enrollment Program (DEP). This creates an instance of DEP in the JSS. (For more information, see Integrating with the Device Enrollment Program.) Only computers associated with a DEP instance can be enrolled with the JSS using a PreStage enrollment.

After creating a DEP instance, you need to create a PreStage enrollment in the JSS for the computers you want to enroll. Creating a PreStage enrollment allows you to configure the enrollment settings and customize the user experience of the Setup Assistant. You can also specify the computers that should be enrolled using the PreStage enrollment. In addition, you can specify that computers newly associated with the DEP instance be automatically added to the PreStage enrollment.

You can require users to authenticate during computer setup using an LDAP directory account or a JSS user account. If users authenticate with an LDAP directory account, user and location information is submitted during enrollment.

When computers with macOS 10.10 or later are enrolled using a PreStage enrollment, they are also automatically managed if user-initiated enrollment is enabled for macOS in the JSS. When enabled, User-Initiated Enrollment settings apply to computer PreStage enrollments, including management account and QuickAdd package settings, and whether to automatically launch Self Service. (For more information, see User-Initiated Enrollment Settings and Installing Self Service on Computers.)

Computers with macOS 10.9 or earlier (and computers with macOS 10.10 or later if user-initiated enrollment is not enabled) can be managed using one of the following methods after they are enrolled with the JSS using a PreStage enrollment:

- Remote Enrollment Using Recon
- QuickAdd Packages Created Using Recon
- User-Initiated Enrollment for Computers

Requirements

To enroll a computer using a PreStage enrollment, the computer must be connected to the Internet during the Setup Assistant.

To require LDAP users or JSS users to authenticate during setup, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

Configuring a Computer PreStage Enrollment

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

2. Click **Computers** at the top of the page.

3. Click **PreStage Enrollments**.

4. Click **New** .

5. Use the General payload to configure basic settings for the PreStage enrollment and customize the user experience of the Setup Assistant.
To customize the user experience of the Setup Assistant, select which steps you want to skip in the Setup Assistant. If you choose to skip steps, the user can enable these settings after the computer is configured unless otherwise restricted.

6. (Optional) Use the Account Settings payload to specify the accounts to create for computers with macOS 10.10 or later if they are enrolled via a PreStage enrollment and user-initiated enrollment for macOS is enabled in the JSS.
Note: If a computer is not bound to a directory service, only the management account and the first local administrator account created for that computer can log in to the computer.

7. (Optional) Use the User and Location payload to specify user and location information for the computers.
This information is stored in the JSS for each computer enrolled using a PreStage enrollment.
Note: The User and Location Information payload is only displayed if the **Require Authentication** checkbox is not selected.

8. (Optional) Use the Passcode payload to specify passcode requirements for the computers.

9. (Optional) Use the Purchasing payload to specify purchasing information for the computers.
This information is stored in the JSS for each computer enrolled using a PreStage enrollment.

10. (Optional) Use the Attachments payload to upload attachments to store for computers.
This information is stored in the JSS for each computer enrolled using a PreStage enrollment.

11. If the SSL certificate you are using is signed by an external CA (your organization's CA or a trusted third-party CA), use the Certificates payload to upload a certificate for the CA that you want computers to trust at enrollment.
Note: The anchor certificate is only displayed if the SSL certificate you are using is signed by the JSS's built-in CA.

12. (Optional) Use the Directory payload to choose a directory server for the computers.

13. Click the **Scope** tab and configure the scope of the PreStage enrollment by selecting the checkbox next to each computer you want to add to the scope.
The computers listed on the **Scope** tab are the computers that are associated with the Device Enrollment Program (DEP) via the server token file (.p7m) you downloaded from the Apple Deployment Programs website.
Note: If you want to add computers to the scope automatically as they become associated with the DEP instance, select the **Automatically assign new devices** checkbox in the General payload.

14. Click **Save**.

Refreshing PreStage Enrollment Information

The JSS allows you to manually refresh information about the computers in the PreStage enrollment as needed.

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

2. Click **Computers** at the top of the page.

3. Click **PreStage Enrollments**.

4. Click the PreStage enrollment you want to refresh.

5. Click **Refresh**.

   If there is updated information about the computers in DEP, this information is displayed in the JSS.

Further Considerations

When cloning a PreStage enrollment, computers in the scope of the original PreStage enrollment are not included in the scope of the cloned PreStage enrollment.

Related Information

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

Integrating with the Device Enrollment Program
Find out how to configure an instance of DEP.

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**.

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.

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 macOS 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** .
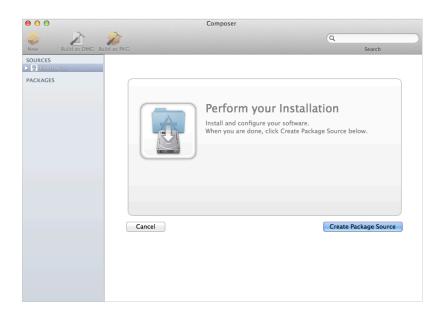
3. Under the Monitor Installation heading in the sidebar, select **Snapshot**.

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

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

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

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**.

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**.

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/
```
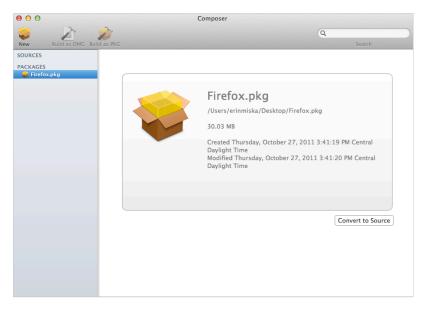
- Any other items are copied to their current location.

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**.

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

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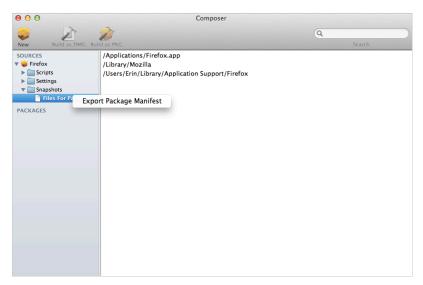
Package manifests are .composer files that can be used to create package sources from the software installed on your computer. They can also be used to capture settings configured on your computer, such as Dashboard, Display, and Global Preference settings.

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**.

5. Enter a name for the package manifest.

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

7. Select the checkbox next to each file that must be present on a computer for the package manifest to appear under the Pre-Installed Software heading or the User Environment heading in Composer.

8. If desired, select the **Custom Icon** checkbox and choose an icon for the package manifest.
   The icon is displayed when viewing the package manifest in Composer.

9. If you want to upload the package manifest to Jamf Nation:

   a. Click **Upload to Jamf Nation**.

   b. Enter the username and password for your Jamf Nation account.

   c. Choose a third-party product to associate the package manifest with. For example, if you are creating a package manifest for Adobe Reader 10, associate it with the "Adobe Reader" third-party product.

   d. Click **Upload**.

10. Click **Save As**.

11. Choose a location to save the package manifest and click **Save**.

Updating Package Manifests

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

Composer downloads the latest package manifests from Jamf Nation and any new package manifests that Jamf 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.
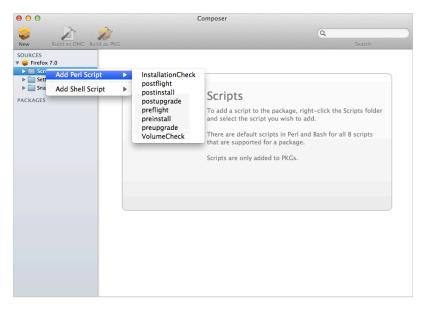
Adding a postflight script to a package source allows you to remove deprecated or unneeded files from computers as they install the package.

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.

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.
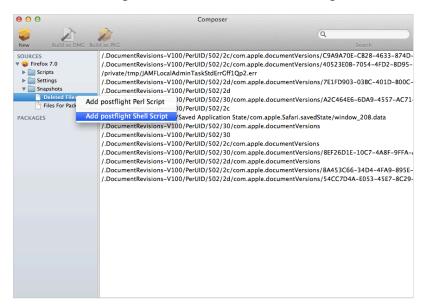
Adding a Postflight Script that Removes Deleted Files from Computers

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**.

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.

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.

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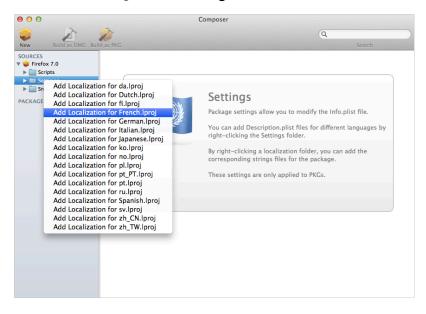
Composer includes defaults for the following localizations supported by the PKG format:

- `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.
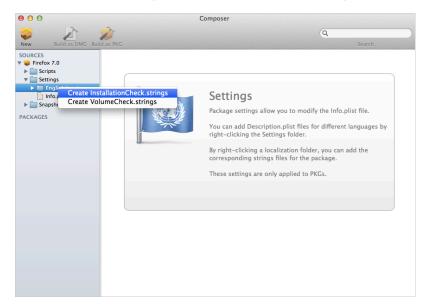
Adding and Editing Files for a Localization

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

4. 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**.

5. 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 re-created 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.

Delete MCX Records in the Local Directory Service
This option removes the `/var/db/dslocal/nodes/Default/computers/localhost.plist` file before building an OS package.

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

Cancel   Previous   Next

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

Related Information

For related information, see the following Knowledge Base article:

How Composer Displays Partitions when Building OS Packages
Find out how Composer v9.7 or later displays partitions when building OS packages.

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.

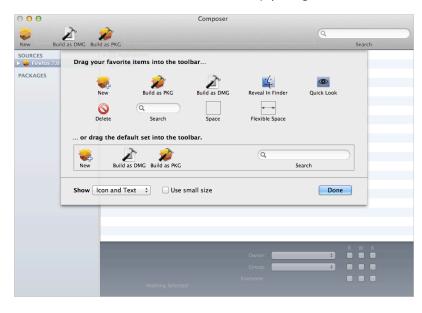This section provides a detailed explanation of Composer preferences.

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.

Package Preferences

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

This pane includes the following preference settings:

Build flat PKGs
By default, Composer builds flat PKGs. Flat PKGs consist of a single file and allow for easier and more reliable deployment than non-flat PKGs. You cannot view or 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. 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 macOS 10.7 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, see the following Knowledge Base article:

Obtaining an Installer Certificate from Apple

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.
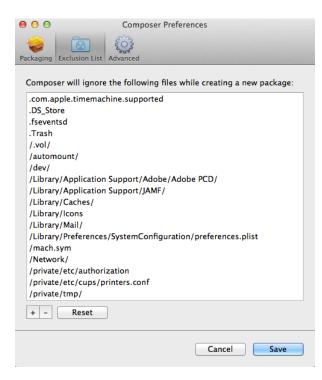
Exclusion List

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.

Advanced Preferences

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

This pane includes the following preference settings:

Work Directory
When Composer creates a package source, it copies files to a work directory. This work directory must have 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 for Computers

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

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 Computer. You can also use the Computer Inventory Collection settings to do the following:

- Specify custom search paths to use when collecting applications, fonts, and plug-ins.
- Monitor iBeacon regions so that computers submit information to the JSS when they enter or exit a region

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.**

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:

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

- [Viewing the Application Usage Logs for a Computer](#)
  Find out how to view Application Usage logs for a computer.

- [iBeacon Regions](#)
  Learn what iBeacon regions can be used for and how you can add them to the JSS.

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 Computer 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 Mac 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 Mac 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**.
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**.

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 a 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://www.jamf.com/jamf-nation/third-party-products/files/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**.

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**.

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 Computer
  You can view the extension attributes collected from a 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 each JSS user 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**.

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:

- Assign the peripheral to a computer and populate information about the user assigned to the computer
- Assign a user to the peripheral and populate information about the user. (For information on assigning a user to a peripheral or removing a user assignment, see User Assignments.)
- 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**.

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**.

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. Use the General payload to specify basic information about the peripheral.

8. (Optional) Use the User and Location payload to assign the peripheral to a computer or assign a user to the peripheral by specifying user and location information. (For information on assigning a user to a peripheral or removing a user assignment, see User Assignments.)
   This information is stored in the JSS for each peripheral.

9. (Optional) Use the Purchasing payload to specify purchasing information for the peripheral.
   This information is stored in the JSS for each peripheral.

10. (Optional) Use the Attachments payload to upload attachments to store for the peripheral.
    Attachments are stored in the JSS for each peripheral.

11. Click **Save**.

Further Considerations

Peripherals assigned to a computer automatically receive user and location information from the computer they are assigned to. To make changes to user and location information for a peripheral assigned to a computer, you must make changes to the computer's user and location information.

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 Computer
  You can view the peripherals associated with a computer.

- User Assignments
  Learn how to assign users to periperhals and remove user assignments from peripherals.

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

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all results

In general, searches are not case-sensitive.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains". (For more information, see Configuring Account Preferences.)

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

Usage	Example
Use an asterisk after a search term to return all results with attributes that begin with that term.	Perform an application search for "Adobe*" to return all applications that begin with "Adobe".
Use an asterisk before a search term to return all results with attributes that end with that term.	Perform a computer search for "*@mycompany.com" to return all computers with email addresses that end with "@mycompany.com".
Use an asterisk before and after a search term to return all results that include that term.	Perform an application search for "*Word*" to return all applications that include "Word".
Use an asterisk without any other terms to return all results for the item you are searching.	Perform a peripheral search for "*" to return all peripherals.

Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform an application search for "Adobe*, *.app" to return all applications that begin with "Adobe" and end with ".app".

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a printer search for "abc*, -*West" to return all printers that begin with "abc" except for those that end with "West".

Returning All Results

There are two ways to return all results: use an asterisk (*) without any other characters or terms, or perform a blank search.

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**.

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 Computer
  Find out how to view and edit inventory information for a 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
  Find out how to create and save an advanced computer search.

- Computer Inventory Display Settings
  Find out 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**.
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 **Show Advanced 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.

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**.

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**.

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 Computer
  Find out how to view and edit inventory information for a 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
- Certificate name

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.
- Send remote commands.

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.
   Note: When computers are added to a site, any users assigned to those computers are also added to that 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: You can only perform mass actions from a simple computer search if you searched by 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 **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.

Mass Sending Remote Commands to Computers

You can mass send the Lock Device and Update OS Version remote command to computers.

The remote commands available for a particular computer vary depending on the computer's OS version. For more information, see the following sections in this guide:

- Remote Commands for Computers
  Learn about remote command requirements.

- Computer Management Capabilities
  Learn about remote command availability on 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 **Send Remote Commands**.

6. Select the remote command to send to computers.

7. Follow the onscreen instructions to send the remote command.

Related Information

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

- Viewing and Editing Inventory Information for a 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 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 Computer

The Jamf Software Server (JSS) stores detailed inventory information for each computer. You can view and edit this information from the JSS.

The following table lists the information that you can view and edit for each computer.

Note: Extension attributes are displayed in computer inventory information in the category in which they are configured to display.

Field	Editable	Notes
General Category		
Computer Name	✓	
Site	✓	
Last Inventory Update		
Last Check-in		
IP Address	✓	
Reported IP Address		
jamf binary Version		
Platform		
Managed		
Enrollment Method		
Last Enrollment		
MDM Capability		
JSS Computer ID		
Asset Tag	✓	
Bar Code 1	✓	
Bar Code 2	✓	

Bluetooth Low Energy Capability		
Logged in to iTunes Store		This value will be reported as "Active" when a user-level configuration profile is installed from Self Service using MDM-enabled credentials
Management Account Username	✓	
Management Account Password	✓	
Hardware Category		
Make		
Model		
Model Identifier		
UDID	✓	
Serial Number		
Processor Speed		
Number of Processors		
Number of Cores		
Processor Type		
Architecture Type		
Bus Speed		
Cache Size		
Primary MAC Address	✓	
Secondary MAC Address	✓	
Total RAM		
Available RAM Slots		

Field	Editable	Notes
Battery Capacity		
SMC Version		
NIC Speed		
Optical Drive		
Boot ROM		
Operating System Category		
Operating System		
Operating System Version		
Operating System Build		
Active Directory Status		
Master Password Set		
FileVault Users		
Service Pack		
User and Location Category		
Username	✓	
Full Name	You can assign a user to the computer and populate user information from the **Users** tab. (For more information, see User Assignments .)	
Email Address		
Phone Number		
Position		
Department		
Building		
Room		

Field	Editable	Notes
Security Category		
System Integrity Protection	N/A For more information, see the Working with Apple's macOS Security Features in Jamf Pro Knowledge Base article.	Displays whether System Integrity Protection is enabled for a computer (collected for macOS 10.11 or later only).
Gatekeeper		Displays whether Gatekeeper is enabled for a computer (collected for macOS 10.9 or later only).
XProtect Definitions Version		Displays the current version of XProtect Definitions installed on a computer (collected for macOS 10.9 or later only).
Purchasing Category		
Purchased or Leased	✓ You can 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.)	
PO Number		
PO Date		
Vendor		
Warranty Expiration		
AppleCare ID		
Lease Expiration		
Purchase Price		
Life Expectancy		
Purchasing Account		
Purchasing Contact		
Extension Attributes Category		
	✓ Non-script extension attributes only	Displays a list of custom data fields collected using extension attributes.
Storage Category		
Model		
Revision		
Serial Number		
Drive Capacity		

Field	Editable	Notes
S.M.A.R.T. Status		
Number of Partitions		
Name		Displays the name of the partition
Size		Displays the size of the partition
% Used		Displays the % used of the partition
Available		Displays space available for Boot Partition.
FileVault 2 State		Displays the FileVault 2 State of the partition This value will be reported as "Unknown" when: - Inventory has not been updated since the last JSS upgrade - The JSS is unable to detect encryption status due to an error
Core Storage Partition Scheme		Displays the core storage partition scheme of the partition
Disk Encryption Category		
Last Inventory Update		
FileVault 2 Partition Encryption State		This value will be reported as "Unknown" when: - Inventory has not been updated since the last JSS upgrade - The JSS is unable to detect encryption status due to an error
Individual Recovery Key Validation		Displays whether the individual recovery key on a computer matches the individual recovery key stored for that computer in the JSS This value will be reported as "Unknown" when: - macOS version is 10.8 or earlier - No recovery key in the JSS to validate against - Inventory has not been updated since the last JSS upgrade
Institutional Recovery Key		
Disk Encryption Configuration		
FileVault 2 Enabled Users		Displays the usernames of FileVault 2-enabled users on the computer

Field	Editable	Notes
Peripherals Category		
		Displays a list of peripherals associated with the computer
Licensed Software Category		
		Displays a list of licensed software titles installed on the computer
Applications Category		
		Displays a list of applications installed on the computer
Fonts Category		
		Displays a list of fonts installed on the computer
Plug-ins Category		
		Displays a list of plug-ins installed on the computer
Profiles Category		
		Displays a list of profiles installed on the computer
iBeacon Regions Category		
		Displays a list of iBeacon regions that the computer is currently in. (This category is only displayed if the Computer Inventory Collection settings are configured to monitor iBeacon regions. For more information, see Computer Inventory Collection Settings.)
Certificates Category		
		Displays a list of certificates installed on the computer
Package Receipts Category		
		Displays a list of packages installed by Installer.app or Software Update, and a list of packages installed or cached by the Casper Suite
Software Updates Category		
		Displays a list of software updates available for the computer
Local User Accounts Category		
		Displays a list of local user accounts and information about them
Printers Category		
		Displays a list of printers mapped to the computer and information about those printers
Services Category		

Field	Editable	Notes
		Displays a list of active services
Attachments Category		
		Displays a list of files attached to the inventory record
		Upload and delete attachments

Viewing Inventory Information for a 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 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 purchasing information, you can click **Search** 🔍 to look up and populate information from Apple's Global Service Exchange (GSX).
   Note: This button is only displayed if you have a GSX connection set up in the JSS.
   If you are editing user and location information, the changes are applied in the Users tab. This specified information is also applied in the inventory information for mobile devices, peripherals, and other computers that the user is assigned to. (For information on assigning a user to a computer or removing a user assignment, see User Assignments.)

7. Click **Save**.

Viewing Management Information for a Computer

The Jamf Software Server (JSS) allows you to view the following management information for each computer:

- Pending management commands
- Policies
- eBooks
- Mac App Store apps
- Computer configuration profiles
- Managed Preferences
- Restricted software
- FileVault 2 recovery key(s)
- Group memberships
- Patch reporting software titles

Requirements

To view pending management commands for a computer, the computer and the JSS must meet the requirements for sending a remote command or installing a computer configuration profile. (For more information, see Remote Commands for Computers or Computer Configuration Profiles.)

Viewing the Pending Management Commands for a Computer

When viewing management information for a computer, you can view a list of pending management commands for the computer. The list includes all pending actions related to sending a remote command and installing or removing a computer 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 Computer

When viewing management information for a 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 eBooks for a Computer

When viewing management information for a computer, you can view a list of eBooks that have the computer in the scope. You can also view a list of eBooks 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 eBooks 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 **eBooks** category.
   A list of eBooks for the computer is displayed.

6. To view eBooks for a specific user, enter the username in the **Username** field and click **Update**.

   A list of eBooks for the user is displayed.

Viewing Mac App Store Apps for a Computer

When viewing management information for a computer, you can view a list of Mac App Store apps that have the computer in the scope. You can also view a list of Mac App Store apps 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 apps 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 **Mac App Store Apps** category.
   A list of apps for the computer is displayed.

6. To view apps for a specific user, enter the username in the **Username** field and click **Update**.
   A list of apps for the user is displayed.

Viewing Configuration Profiles for a Computer

When viewing management information for a computer, you can view a list of computer 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.
   Note: This list of profiles does not take into account users assigned to the computer or user actions taken on the computer.

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 Computer

When viewing management information for a 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 Computer

When viewing management information for a 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 Computer

When viewing management information for a 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 Computer

When viewing management information for a 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.

Viewing Patch Reporting Software Titles for a Computer

When viewing management information for a computer, you can view patch reporting software titles for the computer. Patch reporting software titles in the JSS are third-party macOS software titles that can be used for patch reporting and patch notifications. (For information on patch management for third-party updates, see About Patch Management.)

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 patch reporting software titles 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 **Patch Reporting Software Titles** category.
   A list of software titles is displayed.

6. To view the software titles that are on the latest version, click **Latest Version**.
   A list of software titles on the latest version is displayed.

7. To view the software titles that are on a version other than the latest, click **Another Version**.
   A list of software titles on a version other than the latest 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 Computer

The Jamf Software Server (JSS) allows you to view the history for each computer. The information you can view includes:

- Application Usage logs
- Computer Usage logs
- Audit 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
- Completed, pending, and failed Mac App Store app installations

You can also flush policy logs for a computer.

Viewing Application Usage Logs for a Computer

The Application Usage logs for a 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 Computer

The Computer Usage logs for a 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 Audit Logs for a Computer

The audit logs allow you to view a list of the following events that occurred for a computer:

- The computer's FileVault encryption key has been viewed.
- The Wipe Computer remote command has been sent to the computer.

The date/time that the event occurred and the username of the administrator who initiated the event are included in the log.

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 audit 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 **Audit Logs** category.
   Audit logs for the computer are displayed.

Viewing and Flushing Policy Logs for a Computer

The policy logs for a 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 Computer

The Casper Remote logs for a 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 Computer

The screen sharing logs for a 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 Computer

The Casper Imaging logs for a 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 Casper Imaging 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 Computer

The management history for a computer allows you to view lists of completed, pending, and failed management commands for the computer. The lists include all actions related to sending a remote command and installing or removing a computer 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 Computer

The hardware/software history for a 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 Computer

The user and location history for a 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.

Viewing Mac App Store App Installations for a Computer

You can view the completed, pending, and failed Mac App Store app installations for a computer. You can also cancel pending Mac App Store app installations.

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 app installation 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.

5. Click the **History** tab, and then click the **Mac App Store Apps** category.
   A list of apps installed on the computer 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.**

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 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 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**.

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**.

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 **Show Advanced 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.
      Note: Creating a smart computer group with no criteria will cause all managed computers to be included in the group's membership.

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.

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**.

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**.

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**.
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**.

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**.
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**.

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**.

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**.
   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**.

4. Click **Grid View** 🔲 at the top of the list.

Viewing and Flushing Logs for a Policy

The logs for a 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

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

2. Click **Computers** at the top of the page.

3. Click **Policies**.

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 bottom of the pane.

Related Information

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

- [Viewing and Flushing Policy Logs for a 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 macOS 10.8 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 macOS 10.9 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 macOS 10.9 or later.

This payload also allows you to disable an existing local account for FileVault 2 on computers with macOS 10.9 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 macOS 10.9 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.
- Perform an authenticated restart on computers with macOS 10.8.2 or later that are FileVault 2 enabled.
  Note: For this to work on computers with FileVault 2 activated, the enabled FileVault 2 user must log in after the policy runs for the first time and the computer has restarted.

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

For more information on authenticated restart, see the following Apple Knowledge Base article:
http://support.apple.com/en-us/HT202918

Maintenance Payload

This payload allows you to perform the following maintenance tasks:

- Update inventory.
- Reset computer names.
- Install all cached packages.
- Fix disk permissions (macOS 10.11 or earlier).
- 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.

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 macOS 10.8 or later, most User Interaction messages are displayed in 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 for Computers

About Self Service for Computers

The Self Service application allows users to browse and run policies, install configuration profiles, Mac App Store apps and eBooks, 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, user authentication, and the items available to users. In addition, you can configure notifications to be displayed to users as new items are added to Self Service.

You can make any policy, configuration profile, Mac App Store app, or eBook available in Self Service and customize how it is displayed to users. This includes displaying an icon and description, featuring the item on the main page, displaying it in relevant categories, and displaying item-specific notifications. You can also specify which computers display the item 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 on Computers
  Find out how to install Self Service on managed computers.

- Self Service User Login Setting
  Find out how to require users to log in to Self Service using their LDAP directory accounts.

- Self Service Notifications Setting
  Find out how to display notifications to users when new items are added to Self Service.

- Self Service Policies
  Find out how to make policies available in Self Service.

- Self Service Configuration Profiles for Computers
  Find out how to make macOS configuration profiles available in Self Service.

- Self Service Plug-ins
  Find out how to add plug-ins to Self Service.

- Self Service User Experience on Computers
  Learn how users log in to Self Service, run policies, install configuration profiles, Mac App Store apps, and eBooks, use plug-ins, and view notifications.

- **Mac App Store Apps**
  Find out how to distribute Mac App Store apps.

- **eBooks Available in the iBooks Store**
  Find out how to make iBooks Store eBooks available in Self Service.

- **In-House eBooks**
  Find out how to distribute in-house eBooks.

Installing Self Service on Computers

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**.

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

Self Service User Login Setting

The User Login setting for Self Service allows you to configure the method for logging in to Self Service.

Requirements

To require or allow users to log in to Self Service with an LDAP directory account, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

To require or allow a user to log in using a JSS user account, you must first create an account for that user. (For more information, see JSS User Accounts and Groups.)

Configuring the User Login Setting 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**.

4. In the "Computer Management–Management Framework" section, click **Self Service** .

5. Click **Edit**.

6. Click the **Login** tab.

7. Configure the User Login setting.

8. Click **Save**.

   The change is applied the next time computers check in with the JSS.

Self Service Notifications Setting

The Self Service Notifications setting allows you to configure whether or not users receive notifications when new items are added to Self Service.

When Self Service notifications are enabled:

- A "Notifications" page is available in Self Service that allows the user to view a list of notifications for items that have been added to Self Service. The user can click to install any item in the list.
- When the Self Service icon is in the Dock, the icon displays a red badge with a number to indicate how many new items have been added to Self Service since the user last viewed the "Notifications" page.
- Optional, item-specific notification settings are available in the JSS when adding or editing items that are made available in Self Service. These settings allow you to add a notification for the item to Notification Center (including in banners or alerts), and to specify subject and/or message text to display in Self Service and Notification Center.

For more information, see Self Service User Experience on Computers.

Requirements

To use Self Service notifications, you need:

- To display badges on the Self Service icon in the Dock, computers with macOS 10.7 or later
- To display notifications in Notification Center, computers with macOS 10.8 or later

Configuring the Notifications Setting 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**.
4. In the "Computer Management–Management Framework" section, click **Self Service** .
5. Click **Edit**.
6. Click the **Notifications** tab.
7. Configure the Notifications setting.
8. Click **Save**.

The change is 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**.
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. You can customize the text displayed in the description for the policy in Self Service by using Markdown in the Description field.
    For information about Markdown, see the following Knowledge Base article:
    Using Markdown to Format Text
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:

- Running Policies from Self Service
  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 Configuration Profiles for Computers

You can make any computer configuration profile available in Self Service, but it is up to you to determine which profiles are appropriate.

When you make a configuration profile 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 configuration profiles are displayed to users by doing the following:

- Entering a description
- Uploading an icon
- Featuring the configuration profile on the main page
- Displaying or featuring the configuration profile in one or more categories

Creating a Self Service 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**.
4. Do one of the following:
   - To use the JSS to manually create a new configuration profile, click **New** + .
   - To upload a configuration profile (.mobileconfig) that was created using Apple's Profile Manager, click **Upload** ↑ .

   For more information about configuration profiles, see Computer Configuration Profiles.
5. Use the General payload to set the distribution method to "Make Available in Self Service" and to configure basic settings.
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 configuration profile.
   For more information, see Scope.
8. Click the **Self Service** tab and configure how the configuration profile is displayed in Self Service using the settings on the pane. You can customize the text displayed in the description for the configuration profile in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text
9. Click **Save**.

   Computer-level and user-level profile settings are applied when the user installs the profile from Self Service.

Related Information

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

- Self Service User Experience on Computers
  Learn how users log in to Self Service, run policies, install configuration profiles, Mac App Store apps, and eBooks, use plug-ins, and view notifications.

- Computer Configuration Profiles
  Learn about computer configuration profiles, including requirements, payload variables, and how to manually create and upload a configuration profile.

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**.
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.

Related Information

For more information on the Self Service API, download the Casper Suite SDK from:
https://www.jamf.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 on Computers

This section provides an overview about what users do to log in to Self Service, run policies, install configuration profiles, Mac App Store apps, and eBooks, use plug-ins, and view notifications 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 Login setting for Self Service is configured to require or allow login. (For more information, see Self Service User Login Setting.)

Running Policies from Self Service

Users can browse policies from the "Featured" section or the list of categories in Self Service. Policies are only displayed in the "Featured" page 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. Users can view the status of the policy installation in the status area at the top of Self Service.

Installing Configuration Profiles from Self Service

Users can browse and install computer-level and user-level configuration profiles from the "Featured" page or list of categories in Self Service. Users can view configuration profile installation status in the status area at the top of Self Service.

Note: Self Service must be configured to require or allow user log in, and users must be logged in to Self Service to see user-level configuration profiles.

If you have configured a configuration profile to allow it, users can also remove a configuration profile using Self Service. (For more information, see Self Service Configuration Profiles for Computers.)

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. (For more information, see Self Service Plug-ins.)

Installing Mac App Store Apps from Self Service

Users can browse and install Mac App Store apps from the "Featured" page or list of categories on the main page. (For more information, see Mac App Store Apps.)

To install an app, users click the button next to it. Users can view the status of the app installation in the status area at the top of Self Service.

Note: Mac App Store apps installed from Self Service are not managed by the JSS. Users can update apps using the Mac App Store or uninstall apps from their computers.

Installing eBooks from Self Service

Users can browse in-house eBooks and eBooks available from the iBooks Store in the "Featured" section or the list of categories on the main page. eBooks are only displayed in the "Featured" section if you configured the eBook to do so. (For more information, see eBooks Available in the iBooks Store or In-House eBooks.)

To install an eBook, users click the button next to it. Users can see the status of the eBook installation in the status area at the top of Self Service.

Viewing Self Service Notifications

If enabled in the Jamf Software Server (JSS), notifications are displayed to users when new items are added to Self Service. (For more information, see Self Service Notifications Setting.)

Self Service notifications are displayed to the user in the following ways:

- A "Notifications" page allows the user to view a list of notifications for new items added to Self Service. The user can click to install any item in the list.

- When the Self Service icon is in the Dock, the icon displays a red badge with a number to indicate how many new items have been added to Self Service since the user last viewed the "Notifications" page.

- (Optional) When configured in the JSS for an item, notifications also display in Notification Center and as banners or alerts in macOS (requires macOS 10.8 or later). Users can click any notification to go to the item in Self Service.
- (Optional) When configured in the JSS for an item, notification subject and/or message text for the item is displayed in the "Notifications" page of Self Service, in Notification Center, and in banners or alerts in macOS. If subject and message text is not specified, the item name is displayed in the notification by default.

VPP Content Distribution for Computers

VPP-Managed Distribution for Computers

You can distribute Mac App Store apps and eBooks purchased through Apple's Volume Purchase Program (VPP) to computers and users via VPP-managed distribution.

For more information about VPP, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Note: As an alternative to VPP-managed distribution, the JSS also supports distributing Mac App Store apps and eBooks to computers by associating redeemable VPP codes with apps and eBooks. For more information, see VPP Code Distribution for Computers.

VPP-Managed Distribution for Computers

The JSS allows you to distribute Mac App Store apps directly to computers for VPP-managed distribution. Because VPP-managed distribution for computers is device-based, VPP user registration is not required and users do not need to provide an Apple ID. Anyone using the computer can access apps distributed to the computer.

With VPP-managed distribution for computers, the JSS has full control of your Mac App Store apps. The JSS can be used to automatically update apps in the JSS and on computers on a schedule, and app updates can be forced at any time. Apps distributed directly to computers do not appear in the user's own Mac App Store purchase history and the apps cannot be updated by users.

VPP-managed distribution for computers requires computers with macOS 10.11 or later. To distribute Mac App Store apps to computers using VPP-managed distribution, you need a VPP account set up in the JSS. For more information, see Integrating with VPP.

To distribute a Mac App Store app directly to a computer, when configuring the app distribution settings, choose the VPP account that purchased the app for VPP-managed distribution. For more information, see Mac App Store Apps.

Note: If you have apps that were distributed with user-based VPP assignments and the apps are device-assignable, you can move to device-based VPP-managed distribution for the apps. For more information, see the Moving from User- to Device-based VPP Assignments Knowledge Base article.

VPP-Managed Distribution for Users

The JSS also allows you to distribute Mac App Store apps and eBooks to users for VPP-managed distribution. Because VPP-managed distribution for users is user-based, it involves VPP user registration and VPP user assignments. For more information, see VPP User Registration and User-Based VPP Assignments.

VPP-managed distribution for users requires computers with macOS 10.9 or later.

Related Information

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

- Simple VPP Content Searches for Computers
  Find out how to search the VPP content in the JSS.

- VPP-Managed Distribution for Mobile Devices
  Learn about assigning content to mobile devices with VPP-managed distribution.

VPP Code Distribution for Computers

The Jamf Software Server (JSS) allows you to distribute Mac App Store apps and eBooks purchased through Apple's Volume Purchase Program (VPP) to computers by distributing redeemable VPP codes. When you distribute Mac App Store apps and eBooks, and associate VPP codes with the app or eBook, you can track VPP code redemption.

To distribute an app or eBook to computers using VPP codes, you need an Excel spreadsheet (.xls) that contains VPP codes for the app or eBook.

For more information on VPP, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Note: As an alternative to VPP code distribution, The JSS also supports device-based VPP-managed distribution for computers and user-based VPP-managed distribution for users. For more information, see VPP-Managed Distribution for Computers and User-Based VPP Assignments.

For information on distributing Mac App Store apps to computers using redeemable VPP codes, see Mac App Store Apps.

For information on distributing eBooks to computers using redeemable VPP codes, see eBooks Available in the iBooks Store.

Simple VPP Content Searches for Computers

A simple VPP content search functions like a search engine, allowing you to quickly search the Mac App Store apps and eBooks in the Jamf Software Server (JSS) for a general range of results.

VPP content searches are based on the name of the app or eBook you are searching for.

Simple VPP content search results display the following information:

- Name of the app or eBook
- VPP account used to purchase the content
- Type of content
- Total content that has been purchased with the VPP account
- Number of apps or eBooks assigned to computers, mobile devices, or users
- Number of VPP assignments that the content is associated with

Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all content

In general, searches are not case-sensitive.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains". (For more information about configuring account preferences, see JSS User Accounts and Groups.)

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

Usage	Example
Use an asterisk after a search term to return all results with attributes that begin with that term.	Perform a search for "key*" to return all content with names that begin with "key".
Use an asterisk before a search term to return all results with attributes that end with that term.	Perform a search for "*note" to return all content with names that end with "note".
Use an asterisk before and after a search term to return all results that include that term.	Perform a search for "*ABC*" to return all content that includes "ABC".
Use an asterisk without any other terms to return all results for the item you are searching.	Perform a search for "*" to return all content.

Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform a user search for "key*, *note" to return all content that begins with "key" and ends with "note".

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a user search for "ABC*, -*note" to return all content with names that begin with "ABC" except for those that end with "note".

Returning All Content

There are two ways to return all content: use an asterisk (*) without any other characters or terms, or perform a blank search.

Performing a Simple VPP Content Search

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

2. Click **Computers** at the top of the page.

3. Click **Search VPP Content**.

4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see Search Syntax.

5. Press the Enter key.
   The list of search results is displayed.

Viewing the Computers that Content is Assigned To

You can view the computers that content is assigned to.

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

2. Click **Computers** at the top of the page.

3. Click **Search VPP Content**.

4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see Search Syntax.

5. Press the Enter key.
   A list of content is displayed.

6. To view the computers that the content is associated with, click the number displayed in the In Use column.
The computers that have the content assigned to them are listed on the Computers pane.

Viewing the VPP Assignments that Content is Associated With

You can view the VPP assignments that content is associated with.

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

2. Click **Computers** at the top of the page.

3. Click **Search VPP Content**.

4. Enter one or more search terms in the field provided.
For information on the syntax to use to refine your search, see Search Syntax.

5. Press the Enter key.
A list of content is displayed.

6. To view the VPP assignments that the content is assigned to, click the number displayed in the VPP Assignments column.

Related Information

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

- Advanced VPP Content Searches for Computers
  Find out how to create and save an advanced VPP content search.

- VPP Content Reports for Computers
  Find out how to export the data in your search results to different file formats.

- Mac App Store Apps
  Find out how to assign apps to computers for VPP-managed distribution.

- User-Based VPP Assignments
  Find out how to assign content to users for VPP-managed distribution.

Advanced VPP Content Searches for Computers

Advanced VPP content searches allow you to use detailed search criteria to search Mac App Store apps and eBooks 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 VPP Content Search

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search VPP Content**.
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.
   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.

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 content is modified and meets or fails to meet the specified search criteria.

    To view the search results, click **View**.

Viewing Advanced VPP Content Search Results

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search VPP Content**.
4. Click the advanced VPP content 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:

- Simple VPP Content Searches for Computers
  Learn how to quickly search VPP content for a general range of results.

- VPP Content Reports for Computers
  Find out how to export the data in your search results to different file formats.

VPP Content Reports for Computers

The data displayed in VPP content 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

Creating VPP Content Reports

1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Search VPP Content**.
4. View simple or advanced VPP content search results. (For more information, see Simple VPP Content Searches for Computers or Advanced VPP Content Searches for Computers.)
5. At the bottom of the list, click **Export**.
6. Follow the onscreen instructions to export the data.

   The report downloads immediately.

Software Distribution

Mac App Store Apps

The Jamf Software Server (JSS) allows you to distribute Mac App Store apps to computers and users. You can also use the JSS to update Mac App Store apps that have been installed by the JSS.

The JSS provides two Mac App Store app distribution methods: make the app available in Self Service, or install the app automatically/prompt users to install the app. When you distribute a Mac App Store app, you add it to the JSS and configure settings for the app, including the distribution method. Then, you specify the users and computers that should receive it (called "scope").

Mac App Store apps purchased through Apple's Volume Purchase Program (VPP) can be distributed to computers or users with VPP-managed distribution. For more information, see VPP-Managed Distribution for Computers and User-Based VPP Assignments.

As an alternative to VPP-Managed distribution, the JSS also supports distributing Mac App Store apps to computers using redeemable VPP codes. For more information, see VPP Code Distribution for Computers.

Mac App Store apps distributed with user-based VPP assignments or with VPP codes are not managed by the JSS. Users can update apps using the Mac App Store or uninstall the apps from their computers.

Requirements

To allow users to install Mac App Store apps from Self Service via MDM, or to allow Mac App Store apps to be installed automatically you need:

- A push certificate in the JSS (For information, see Push Certificates.)
- The **Enable certificate-based authentication** and **Enable push notifications** settings configured in the JSS (For information, see Security Settings.)
- Computers that are bound to a directory service or local user accounts that have been MDM-enabled (For information, see Binding to Directory Services and the Enabling MDM for Local User Accounts Knowledge Base article.)
  Note: If a Mac App Store app is configured to be installed automatically and the user has a local user account that is not MDM-enabled (and there are no other MDM-enabled local user accounts on the computer), the user is prompted to enter local administrator credentials to enable MDM for their account. After the account becomes MDM-enabled, the app is installed and subsequent apps can be installed automatically.
- Apps assigned to computers or users via VPP-managed distribution
  - For device-based assignments, you need:
    - Computers with macOS 10.11 or later

- For user-based assignments, you need:

  - Computers with macOS 10.9 or later
    Note: If a computer does not have macOS 10.9 or later and the "Install Automatically/Prompt Users to Install" distribution method is selected, the app will instead be made available in Self Service.

  - Users registered with VPP and the apps assigned to them using VPP assignments (For information, see VPP User Registration and User-Based VPP Assignments.)

  - Users must be logged in to iTunes or the Mac App Store with the Apple ID used during VPP registration
    Note: If the scope for a Mac App Store app is configured to include a computer and the user is not assigned to that computer in the JSS, the app will instead be made available in Self Service.

To allow users to install apps from the Mac App Store (linked from Self Service), you need:

- Computers with macOS 10.7 or later

- Computers that are bound to a directory service or local user accounts that have been MDM-enabled (For information, see Binding to Directory Services and the Enabling MDM for Local User Accounts Knowledge Base article.)

- Users may be prompted to enter an Apple ID

Distributing a Mac App Store App

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

2. Click **Computers** at the top of the page.

3. Click **Mac App Store Apps**.

4. Click **New** ⊞ .

5. 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**.

6. Use the General pane to configure settings for the app, including the distribution method. For apps distributed using VPP-managed distribution, you can also enable automatic app updates.

7. Click the **Scope** tab and configure the scope of the app.
   For more information, see Scope.

8. (Optional) Click the **Self Service** tab and configure the way the app is displayed in Self Service. You can customize the text displayed in the description for the app in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text
   Note: The **Self Service** tab is only displayed if "Make Available in Self Service" is chosen in the **Distribution Method** pop-up menu.

9. (Optional) If you want to distribute the app directly to computers via VPP-managed distribution, do the following:

   a. Click the **VPP** tab, and then click the **Device Assignments** tab.

   b. Select the **Assign VPP Content** checkbox.

   c. Choose the VPP account that has purchased the app to distribute to computers.

10. (Optional) If you want to associate VPP codes with the app and have not already uploaded a VPP code spreadsheet, do the following:

    a. Click the **VPP** tab, and then click the **VPP Codes** tab.

    b. Upload the Excel spreadsheet (.xls) that contains VPP codes for the app.

11. Click **Save**.

   If users were added as targets to the scope, the app is distributed to the computers those users are assigned to the next time the computers check in with the JSS.

Updating a Mac App Store App

The JSS allows you to update an individual Mac App Store app in the following ways:

- **Enable automatic Mac App Store app updates**–This automatically updates the app description, icon, and version in the JSS and on computers. This update happens once a day depending on the time of day you specify.

- **Force a Mac App Store app to update**–You can force an app to update immediately on computers if there are updates available in the JSS. This applies only to apps distributed using VPP-managed distribution for computers.

- **Distribute a Mac App Store app update**–You can distribute an update for a Mac App Store app by manually updating the version number and URL for the app in the JSS. The update is distributed to computers the next time they contact the JSS.

Note: The JSS also allows you to enable automatic updates for all Mac App Store apps, or force all Mac App Store apps to update immediately. For more information, see Mac App Store App Update Settings.

Enabling Automatic App Updates

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

2. Click **Computers** at the top of the page.

3. Click **Mac App Store Apps**.

4. Click the app for which you want to enable automatic app updates.

5. Click **Edit**.

6. Select **Automatically update app**.

7. To select a country or region to use for syncing apps with iTunes, choose an option from the **iTunes Country or Region** pop-up menu.

8. To specify a time of day to sync apps with iTunes, set the time using the **iTunes Sync Time** pop-up menus.

9. Click **Save**.

   The app is updated in the JSS and on computers in the scope based on the time you configure the app to sync with iTunes.

Forcing an App Update

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

2. Click **Computers** at the top of the page.

3. Click **Mac App Store Apps**.

4. Click the app you want to update.

5. Click **Edit**.

6. Click **Force Update**.

7. Click **Save**.

   The app is updated immediately on computers in the scope if there is an update available in the JSS.

Distributing an App Update

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

2. Click **Computers** at the top of the page.

3. Click **Mac App Store Apps**.

4. Click the app you want to update.

5. Click **Edit**.

6. 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.

7. Click **Save**.

   The update is distributed the next time computers in the scope contact the JSS.

Related Information

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

- [Viewing and Editing Inventory Information for a Computer](#)
  Find out how to view and edit inventory information for a computer.

- [Viewing Mac App Store Apps for a Computer](#)
  Find out how to view the Mac App Store apps in the scope of a computer.

- [Viewing the History for a Computer](#)
  Find out how to view and cancel pending Mac App Store app installations for a computer.

- [Self Service User Experience on Computers](#)
  Learn how users log in to Self Service and install Mac App Store apps made available in Self Service.

Mac App Store App Update Settings

The Jamf Software Server (JSS) allows you to configure settings to update all Mac App Store apps in the JSS and on computers that were distributed using VPP-managed distribution. You can use the App Updates settings in the JSS to do the following:

- **Enable automatic app updates**–You can enable automatic app updates for all Mac App Store apps. This automatically updates app descriptions, icons, and versions in the JSS and on computers. This update happens once a day depending on the time of day you specify.

- **Force apps to update**–You can force all Mac App Store apps to update immediately on computers if there are updates available in the JSS.

Note: The JSS also allows you to enable an automatic app update and force an update for an individual Mac App Store app. For more information, see Mac App Store Apps.

Enabling Automatic 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 **Computer Management**.

4. Click **App Updates** .

5. Click **Edit**.

6. Select **Automatically update all Mac App Store apps**.

7. To select a country or region to use for syncing apps with iTunes, choose an option from the **iTunes Country or Region** pop-up menu.

8. To specify a time of day to sync apps with iTunes, use the **iTunes Sync Time** pop-up menus.

9. Click **Save**.

   Mac App Store apps are updated in the JSS and on computers based on the time you configure apps to sync with iTunes.

Forcing 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 **Computer Management**.

4. Click **App Updates** .

5. Click **Edit**.

6. Click **Force Updates**.

7. Click **Save**.

Mac App Store apps are updated immediately on computers if there are updates available in the JSS.

Managing Packages

Packages in the following formats can be administered using the Casper Suite:

- DMG
- PKG
- MPKG

Note: There are special instructions for managing macOS Installers, and Adobe Updaters and Installers for CS3 or CS4. For more information, see Managing macOS 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.

In addition, you can validate packages using the checksum. (For more information, see Calculating a Checksum.)

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.

5. Click the **Options** tab and configure additional settings for the package, including the priority, and operating system and architecture type requirements.
   Note: Package Limitations options do not apply when installing a package during imaging.

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**.

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**.

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.

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**.

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.

Calculating a Checksum

The checksum is calculated when a package is uploaded to the JSS. The checksum ensures authenticity when the package is downloaded.

The checksum can also be calculated manually using Casper Admin:

1. Open Casper Admin and authenticate to the JSS.

2. In the main repository, select the package you want to calculate checksum for.

3. Control-click (or right-click) and select **Calculate Selected Package Checksum(s)**.

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 macOS Installers

Adding a macOS Installer to Casper Admin is the first step to installing a clean copy of macOS on computers.

Requirements

To manage macOS Installers, you need a distribution point set up in the Jamf Software Server (JSS). (For more information, see About Distribution Points.)

To add a macOS Installer to Casper Admin, the installer must be a .app file from the Mac App Store or a DMG.

Adding a .app File for macOS to Casper Admin

Adding a .app file for macOS 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 from the .app file and then analyzes the contents of the `InstallESD.dmg` file.

The `InstallESD.dmg` file 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 choose a category for the package.

5. Click **OK.**

Adding a DMG of a macOS Installer to Casper Admin

Adding a DMG of a macOS 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.

5. When prompted, click **OK** to continue.
   Casper Admin analyzes the contents of the DMG.

6. When the Options pane appears, choose a default language for the installation from the **Language** pop-up menu.

7. 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.

5. When prompted, click **OK** to continue.
Casper Admin analyzes the contents of the DMG.

6. When the Options pane appears, click **OK**.

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.

4. On the General pane, configure basic settings for the installation, including the display name and category.

5. Click the **Options** tab and configure additional settings for the installation, including the priority and installation language.

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**.

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.

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the package you want to install.

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.

9. Click the **Restart** tab and configure settings for restarting computers.

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**.

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.

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the package you want to cache.

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.

9. Click the **Restart** tab and configure settings for restarting computers.

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**.
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.

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the cached package you want to install.

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.

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**.

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.

4. Click the **Packages** tab.

5. Select the **Install All Cached Packages** checkbox.

6. Click the **Restart** tab and configure settings for restarting computers.

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**.
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.

4. Click the **Packages** tab.

5. In the list of packages, select the checkbox for the package you want to uninstall.

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.

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

About Patch Management

In the Jamf Software Server (JSS), the patch management process is different for Apple Updates than for third-party macOS software title updates.

Patch management for Apple Updates consists of running Software Update on computers via policies. This process installs all updates available from Apple. To customize the process, you can use NetSUS to control which computers get which updates, or deploy macOS manually.

Patch management for third-party macOS software titles consists of:

- Taking inventory of the software titles and versions in your environment

  - If the third-party macOS software title is in the JSS, you can configure patch reporting
  - If the software title is not in the JSS, you can use advanced computer searches and smart computer groups to identify computers that need to be updated

- Determining when vendors release new updates

  - If the third-party macOS software title is in the JSS, you can configure patch notifications
  - If the software title is not in the JSS, use the Internet to search for updates

- Creating a package when an update becomes available
- Uploading the package to a distribution point
- Deploying the package using smart groups and a policy
  To configure the scope of the policy, smart computer groups that use the "greater than" and "less than" operators can be used.

Related Information

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

- Composer
  Learn how to use Composer to build packages of software, applications, preference files, or documents.
- Managing Packages
  You can add packages to a category.
- Installing Packages
  Find out how to install a QuickAdd package using a policy or Casper Remote.
- Patch Reporting
  Learn how to create a patch report for a macOS software title.
- Patch Reporting Software Titles
  Learn about the third-party macOS software titles in the JSS that can be used for patch reporting and patch notifications.

- Patch Notifications
  Learn how to configure patch notifications of third-party macOS software title updates that have been added to the JSS.

For related information, see the following:
NetBoot/SUS Appliance
Find out how to host an internal software update server on Linux.

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.

Patch Reporting Software Titles

The Jamf Software Server (JSS) includes more than 30 third-party macOS software titles that can be used for patch reporting and patch notifications. These third-party software titles represent software that is not available in the App Store. (For the list of software titles provided in the JSS, see the Patch Reporting Software Titles Knowledge Base article.)

When you configure a patch reporting software title, you are able to receive a notification when a third-party macOS software title update has been released by the vendor and added to the JSS, as well as generate reports for the third-party macOS software titles in your environment which allows you to identify the software titles that need to be patched.

Different software titles have different requirements for updating them. For example, some software titles must have additional apps installed for the title to be updated. Because these requirements are in the JSS, you save time by not having to track down the required information.

Requirements

- To configure third-party macOS software titles and enable them to automatically update, the JSS must have outbound access to port 443 to access the patch server and the software title definitions which are hosted on Amazon CloudFront.

- To configure a software title that requires an extension attribute, you must use a JSS user account that has full access. A JSS user account with site access only will not be able to configure a software title that requires an extension attribute.

Configuring a Patch Reporting Software Title

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

2. Click **Computers** at the top of the page.

3. Click **Patch Reporting**.

4. Click **New** $\boxed{+}$.

5. Choose a software title.

6. Use the General pane to configure basic settings for the software title, including whether to receive a JSS notification or email when an updated software title is available.
   Note: This setting is applied for all users who configure their personal notification preferences. (For more information, see Patch Notifications.)

7. If you are configuring a software title that uses an extension attribute, you must click the **Extension Attributes** tab and accept the terms.
   Note: You cannot configure a patch reporting software title if it uses an extension attribute that has the same name as an existing extension attribute. You must first rename the existing extension attribute so that you can save the new one.

8. (Optional) Click the **Definition** tab to review information about the supported software title versions and attributes about each version.

9. Click **Save**.

Related Information

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

- About Patch Management
  Learn about patch management for Apple Updates and for third-party updates.
- Patch Reporting
  Learn how to create a patch report for a macOS software title.

For related information, see the following Knowledge Base article:

Jamf Process for Updating Patch Reporting Software Titles
Learn about the contents of a software definition file in the JSS and the process used by Jamf to add software title updates to the JSS.

Patch Notifications

Patch notifications provide an easy method for being informed of a third-party macOS software title update that has been released by the vendor and added to the Jamf Software Server (JSS). Each JSS user can choose to be notified of available software title updates via email or a JSS Web notification, or both. The JSS Web notification option displays a pop-up dialog to the user in the JSS when a new software title update is available.

Requirements

To configure third-party macOS software titles and enable them to automatically update, the JSS must have outbound access to port 443 to access the patch server and the software title definitions which are hosted on Amazon CloudFront.

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.)

Configuring Patch 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 **Notifications**.
3. For the "An updated patch reporting software title is available" option, select the checkbox for **Email**, **JSS Web**, or both.
4. Click **Save**.

Notifications will be sent or displayed to the JSS user when an update is available for a third-party macOS software title if corresponding notification settings have been enabled for the individual software title. (For information on configuring notifications for a specific software title, see Patch Reporting Software Titles.)

Related Information

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

- About Patch Management
  Learn about patch management for Apple Updates and for third-party updates.
- Patch Reporting
  Learn how to create a patch report for a macOS software title.

Patch Reporting

The patch reporting area of the Jamf Software Server (JSS) can be used to easily configure third-party macOS software titles used in your environment. This provides you with a process to:

- Generate reports for third-party macOS software titles that you have configured in your environment
- Identify which third-party macOS software titles in your environment need to be patched
- Determine which computers need patches

You can use the patch reporting features alone, or combine them with the following additional searching and reporting features in the JSS based on your needs:

- **Advanced computer searches**—There are several benefits to using advanced computer searches to produce a list of computers in the JSS:

  - The ability to display all application titles; the list is not limited to the third-party macOS software titles provided in the patch reporting area.
  - The ability to combine patch-related criteria with other criteria. Patch-related criteria includes features to report on Apple operating systems and third-party macOS software titles. When creating an advanced computer search and selecting Patch Reporting Software Title, you can use "greater than" and "less than" operators, and "Latest Version" as a value to ensure the search will remain current as new versions are released. For example, this criteria can be used to create a general compliance report that includes encryption, or whether computers are on a specific version of an operating system, etc.
    For more information on how to create and save an advanced computer search, see Advanced Computer Searches.

- **Smart computer groups**—Smart computer groups offer the same patch reporting functionality as advanced computer searches. In addition, you can view the status of smart groups on the JSS Dashboard. You can also get notifications when the membership of a smart group changes.
  For more information on how to create computer groups that are based on criteria and have dynamic memberships, see Smart Computer Groups.

Patch Reports

For each software title, you can view the latest version number as well as the percentage of computers in your environment that are on the latest version. In addition, you can view the number of computers that are on the latest version and the number that are on another version.

From the report, you can view when each computer last checked in and the version of the software title installed on the computer.

The data displayed in a patch report can be exported from the JSS to the following file formats:

- Comma-separated values file (.csv)
- Tab delimited text file (.txt)

Requirements

To configure third-party macOS software titles and enable them to automatically update, the JSS must have outbound access to port 443 to access the patch server and the software title definitions which are hosted on Amazon CloudFront.

Creating a Patch Report for a macOS Software Title

For each macOS software title, you can view the number of computers on the latest version of the software title or on a different version of the software title.

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

2. Click **Computers** at the top of the page.

3. Click **Patch Reporting**.

4. A list of configured macOS software titles is displayed.

   - To view a list of computers that are on the latest version of a particular software title, click the number displayed in the On Latest Version column.

   - To view a list of computers that are on another version of a particular software title, click the number displayed in the On Other Version column.
     A report that shows additional details is displayed.
     Note: You can also access the report by choosing a specific software title and clicking the **Report** button.

5. At the bottom of the report, click **Export** and choose "Comma-Separated Values file (.csv)" or "Tab Delimited Text file (.txt)".
    Note: The data will be exported as it is currently filtered.

Related Information

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

- About Patch Management
  Learn about patch management for Apple Updates and for third-party updates.

- Patch Reporting Software Titles
  Learn about the third-party macOS software titles in the JSS that can be used for patch reporting and patch notifications.

- Patch Notifications
  Learn how to configure patch notifications for third-party macOS software title updates that have been added to the JSS.

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**.

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.

4. Click the **Packages** tab.

5. Select the **Install all updates** checkbox.

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.

7. Click the **Restart** tab and configure 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 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 macOS.

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. In addition, if the target computer has macOS 10.10 or later, Screen Sharing must also be enabled on the 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.

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" (macOS 10.8 or later) or "Ask to share the display" (macOS 10.7).

   - To hide the screen sharing session, choose "Log In" (macOS 10.8 or later) or "Connect to a virtual display" (macOS 10.7).

   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 macOS 10.7 or later, 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
Microsoft's Active Directory	Compatible	Compatible	Compatible
Apple's 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**.

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.

Related Information

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

Viewing Managed Preferences for a Computer
Find out how to view managed preferences for a computer or user.

Computer Configuration Profiles

Computer configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for Mac computers and users.

You can use the Jamf Software Server (JSS) to manually create a computer 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 a computer 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. There are two different ways to distribute a computer configuration profile: install it automatically (requires no interaction from the user) or make it available in Self Service. You can also specify the computers and users to which the profile should be applied (called "scope").

Payload Variables for Computer Configuration Profiles

There are several payload variables that you can use to populate settings in a computer 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 or $DEVICENAME	Computer Name
$SITENAME	Site Name
$SITEID	Site ID
$UDID	UDID
$SERIALNUMBER	Serial Number

Variable	Computer Information
`$USERNAME`	Username associated with the computer in the JSS (computer-level profiles only)
	Username of the user logging in to the computer (user-level profiles only)
`$FULLNAME` or `$REALNAME`	Full Name
`$EMAIL`	Email Address
`$PHONE`	Phone Number
`$POSITION`	Position
`$DEPARTMENTNAME`	Department Name
`$DEPARTMENTID`	Department ID
`$BUILDINGNAME`	Building Name
`$BUILDINGID`	Building ID
`$ROOM`	Room
`$MACADDRESS`	MAC Address
`$JSSID`	JSS ID
`$PROFILEJSSID`	JSS ID of the Configuration Profile
`$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 a computer configuration profile, you need:

- 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.)
- Computers with macOS 10.7 or later
- (User-level profiles only) Computers that are bound to a directory service or local user accounts that have been MDM-enabled (For information, see Binding to Directory Services and the Enabling MDM for Local User Accounts Knowledge Base article.)

Manually Creating a Computer 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**.

4. Click **New** ⊞ .

5. Use the General payload to configure basic settings, including the level at which to apply the profile and the distribution method.
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. (Optional) If you chose to distribute the profile in Self Service, click the **Self Service** tab to configure Self Service settings for the profile.
For more information, see Self Service Configuration Profiles for Computers.

9. Click **Save**.

Uploading a Computer Configuration Profile

You can create a computer 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**.

4. Click **Upload** ⬆ and upload the configuration profile (.mobileconfig).

5. Use the General payload to change or configure basic settings for the profile, including a distribution method.

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. (Optional) If you chose to distribute the profile in Self Service, click the **Self Service** tab to configure Self Service settings for the profile.
For more information, see Self Service Configuration Profiles for Computers.

9. Click **Save**.

Downloading a Computer Configuration Profile

If you want to view the contents of a computer 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**.

4. Click the configuration profile you want to download.

5. Click **Download**.

   The profile downloads immediately.

Viewing the Status of a Computer Configuration Profile

For each computer configuration profile, you can view the number of computers for which the profile installation has a status of Completed, Remaining, or Failed.

Note: Depending on your system configuration, some historical status data may not be available for profiles installed using the Casper Suite v9.63 or earlier.

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

2. Click **Computers** at the top of the page.

3. Click **Configuration Profiles**.
   A list of computer configuration profiles is displayed.
   For each profile, you can view the number of computers for which the profile installation has a Completed, Remaining, or Failed status.
   Note: If a computer becomes unmanaged after a profile is successfully distributed to it, the profile will continue to be displayed in the Completed column.

4. To view a list of computers for which the profile installation has a Completed, Remaining, or Failed status, click the number displayed in the corresponding column. Then click **Done**.

Viewing Logs for a Computer Configuration Profile

The logs for a computer configuration profile include a list of computers that are in the scope of the profile, as well as the username of the user who installed the profile, the date/time that the status was last updated, and the status of the profile for each computer.

Note: Depending on your system configuration, some historical log data may not be available for profiles installed using v9.63 or earlier.

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

2. Click **Computers** at the top of the page.

3. Click **Configuration Profiles**.
   A list of computer configuration profiles is displayed.

4. Click **View** next to the configuration profile you want to view logs for.
   A list of computers that are in the scope of the configuration profile is displayed.

5. To view logs for a different date range, specify the starting and ending dates using the **Date Range** pop-up calendars.

6. Click **Done**.

Related Information

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

- Viewing the Pending Management Commands for a Computer
  Find out how to view and cancel pending computer configuration profile installations and removals for a computer.

- Viewing Management History for a Computer
  Find out how to view all completed, pending, and failed computer configuration profile installations and removals for a computer.

- Viewing Configuration Profiles for a Computer
  Find out how to view the computer configuration profiles in the scope for a computer.

- Self Service Configuration Profiles for Computers
  Find out how to make computer configuration profiles available in Self Service.

Remote Commands for Computers

The remote commands available in the Jamf Software Server (JSS) allow you to remotely perform the following tasks on a Mac computer:

You can send a remote command to a single computer. Some commands can also be sent to multiple computers at once using mass actions. For more information, see Performing Mass Actions for Computers.

Note: The remote commands available for a particular computer vary depending on the computer's OS version. For more information, see Computer Management Capabilities.

The following table describes the remote commands that you can send from the JSS:

Remote Command	Description	Requirements
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 macOS 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)	--

Remote Command	Description	Requirements
Update OS version and built-in apps	Updates the OS version and built-in apps on the computer You can choose to download the update for users to install, or to download and install the update and restart computers after installation.	macOS 10.11 or later Enrolled via a PreStage enrollment

Requirements

To manage remote commands, you need:

- Computers with macOS 10.7 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 a 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 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 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 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 a 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 a 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.

5. Click the **Options** tab and configure additional settings for the script, including the priority and parameter labels.

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**.

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.

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**.

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** ![site icon] 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.

4. Click the **Scripts** tab.

5. In the list of scripts, select the checkbox for the script you want to run.

6. Configure the settings for the script.

7. Click the **Restart** tab and configure 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 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.

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.

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.

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**.

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.

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
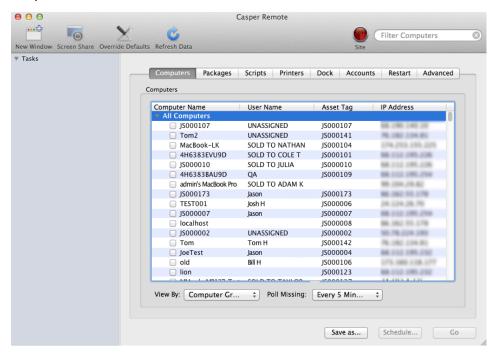
1. Log in to the JSS with a web browser.
2. Click **Computers** at the top of the page.
3. Click **Policies**.
4. Click **New** ⊞ .
5. Use the General payload to configure basic settings for the policy, including the trigger and execution frequency.
   For an overview of the settings in the General payload, 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
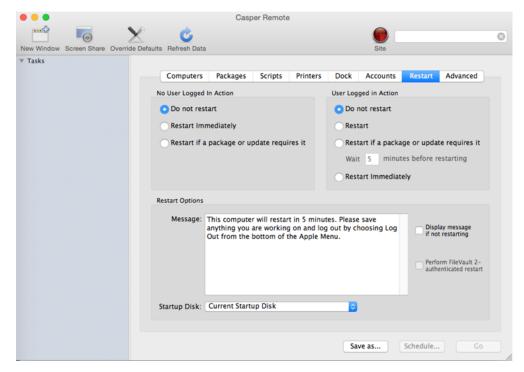
1. Open Casper Remote and authenticate to the JSS.

2. Click **Site** [icon] 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.

4. Click the **Printers** tab.

5. In the list of printers, select the checkbox for the printer you want to map or unmap.

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.

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.

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.**
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.

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**.

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** ![Site icon] 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.

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.

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.

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 macOS 10.9 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 macOS 10.9 or later.

When you delete an existing account, you can permanently delete the home directory or specify an archive location.

Requirements

To enable a new account for FileVault 2, the computer must have macOS 10.9 or later and have an existing, valid individual recovery key that matches the recovery key stored in the JSS.

To disable an existing account for FileVault 2, the computer must have macOS 10.9 or later.

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**.
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.

4. Click the **Accounts** tab.

5. Click **Create**, **Reset Password**, or **Delete**.

6. Configure the action using the options in the window that appears.

7. Click the **Restart** tab and configure 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:

- 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 change or reset the management account password, and enable or disable the management account for FileVault 2.

Administering the Management Account

You can use a policy or Casper Remote to administer the management account.

Using a policy to administer the management account allows you to do the following:

- **Change the account password**—This option changes the management account's password, as well as the account's login keychain password and FileVault 2 password. It is recommended that you use this option if the management account's login keychain password matches the account password stored in the JSS.

- **Reset the account password**—This option only changes the management account's password. This option does not change the management account's login keychain password or FileVault 2 password.
  Note: If the management account's login keychain password does not match the account password stored in the JSS, you must use the **Reset Account Password** option when administering the management account using a policy or the policy will fail.

- **Enable the user for FileVault 2**

- **Disable the user for FileVault 2**

Using Casper Remote to administer the management account allows you to reset the management account's password.

Requirements

To enable the management account for FileVault 2, the computer must have macOS 10.9 or later and have an existing, valid individual recovery key that matches the recovery key stored in the JSS.

To disable the management account for FileVault 2, the computer must have macOS 10.9 or later.

Administering the Management Account Using a Policy

You can change or reset the management account password using a policy. You can also enable or disable the management account for FileVault 2.

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

2. Click the **Computers** tab at the top of the page.

3. Click **Policies**.

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 select an action using the options on the pane.

7. Use the Restart Options payload to configure settings for restarting computers.

8. 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.

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.

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.

6. Click the **Restart** tab and configure settings for restarting computers.

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 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:

- Microsoft's Active Directory
- Apple's 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**.

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**.

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**.

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.

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.

6. Click the **Restart** tab and configure settings for restarting computers.

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 macOS 10.8 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.
    Note: If you make the management account the enabled FileVault 2 user on computers with macOS 10.9 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.)
  - **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.

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**.

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**.

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 macOS 10.8 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. In addition, if you are deploying a disk encryption configuration using a policy, you can configure the policy to defer FileVault 2 enablement until after multiple user logins have occurred.

Requirements

To activate FileVault 2 on a computer, the computer must be running macOS 10.8 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**.

4. Click **New** $\boxed{+}$.

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 "Apply Disk Encryption Configuration" from the **Action** pop-up menu.

8. 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.

9. Choose an event from the **Require FileVault 2** pop-up menu to specify when users must enable disk encryption.

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**.

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.

4. Click the Restart tab and configure settings for restarting computers.
   If you want to perform an authenticated restart on computers enabled with FileVault 2, select
   Perform FileVault 2-authenticated restart. This is applicable to computers with macOS 10.8.2 or later.

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.

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 Computer
  Find out how to view the FileVault 2 recovery key(s) for a 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.

For related information, see the following Apple Knowledge Base article:

http://support.apple.com/en-us/HT202918
Find out how Mac computers can be used with authenticated restart.

Issuing a New FileVault 2 Recovery Key

You can issue a new FileVault 2 recovery key to computers with macOS 10.9 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 File Vault

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:

- macOS 10.9 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:

- macOS 10.9 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**.
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 Computer
  Find out how to view the FileVault 2 recovery key(s) for a 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

The "setregproptool" binary must be present on each computer and any alternate boot volume(s) used to set firmware. For models "Late 2010" or later with macOS 10.9.x or earlier, the binary must be obtained and placed on the computer. (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**.

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.

4. Click the **Accounts** tab.

5. Select the **Set Open Firmware/EFI Password** checkbox.

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.

7. Click the **Restart** tab and configure 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.

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 Air computers 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.
- Event Logs
  Find out how to view event logs for Casper Imaging events.

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 that include a macOS Installer must be compiled on a computer with the same OS version as the installer.

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.

4. (Optional) Click the **Management** tab and set or create a management account.
   This ensures that computers imaged with the configuration are managed.

5. (Optional) Click the **Homepage** tab and enter a homepage URL.

6. (Optional) Click the **Partitions** tab and click **Add (+)** to set up a partition.

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**.

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.

Configurations that include a macOS Installer must be compiled on a computer with the same OS version as the installer.

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.

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 Imaging PreStage.
- 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**.
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.

Booting 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.

4. Click the **Restart** tab.

5. Choose "NetBoot" from the **Startup Disk** pop-up menu.

6. If you want to change the NetBoot server that computers use, click **Override Defaults** and choose a NetBoot server.

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.

For related information, see the following Knowledge Base article:

Booting macOS 10.11 or Later Computers to a NetBoot Image Using a Policy or Casper Remote
Find out how to add a trusted NetBoot server so that you can boot a macOS 10.11 or later computer to a NetBoot image using a policy or Casper Remote.

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.

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 <u>Autorun Imaging</u>.

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](#).

13. Click **Image**.

Related Information

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

- [Viewing Casper Imaging Logs for a Computer](#)
  Find out how to view Casper Imaging logs for a computer.

- [Event Logs](#)
  Find out how to view event logs for Casper Imaging events.

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 an Imaging PreStage in the JSS and then run Casper Imaging on target computers to image them. Creating an Imaging PreStage allows you to configure the imaging settings and specify the computers that should be imaged with the Imaging PreStage (called "scope"). When you open Casper Imaging on a computer in the scope, Casper Imaging is populated with the settings in the Imaging PreStage.

You can configure an Imaging 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 Imaging PreStage.

Requirements

To create an Imaging 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 an Imaging PreStage, you need a startup disk other than the target drive that has Casper Imaging installed. (For more information, see About Imaging.)

Creating an Imaging PreStage

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

2. Click **Computers** at the top of the page.

3. Click **PreStage Imaging**.

4. Click **New** + .

5. Use the General payload to configure basic settings for the Imaging 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 Imaging 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 Imaging 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 Imaging PreStage.

14. Click **Save**.

Imaging a Computer Using an Imaging PreStage

If you configured the Imaging 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 Imaging PreStage to start the imaging process automatically, complete the following instructions:

1. On a computer that is in the scope of the Imaging 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.

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.

6. Click **Image**.

Bypassing PreStage Imaging

To bypass PreStage imaging, hold down the Shift key when opening Casper Imaging.

Viewing Imaging PreStage Logs

Each Imaging PreStage log includes a list of computers that were imaged using the Imaging 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**.
4. Click the Imaging PreStage you want to view logs for.
5. Click **Logs**.
   A list of computers imaged using the Imaging PreStage is displayed.
6. To view the list of actions that were performed when a computer was imaged, click **Show** for the computer.

Related Information

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

Event Logs
Find out how to view event logs for Casper Imaging events.

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**.

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 an Imaging 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**.

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.

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.

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.

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.

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**.

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.

- [Event Logs](#)
  Find out how to view event logs for Casper Imaging events.

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 Air computers 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.

5. To erase each target drive before it is imaged, select the **Erase drives connected to this computer** checkbox.

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.

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 sections in this guide:

- Viewing Casper Imaging Logs for a Computer
  Find out how to view Casper Imaging logs for a computer.

- Event Logs
  Find out how to view event logs for Casper Imaging events.

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 an Imaging 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 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 an Imaging 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 (macOS 10.11 or earlier)
  - Show 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**.

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.**

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 Adobe Illustrator and Adobe CS 5.5 Design Standard, both of which contain 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**.

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**.

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://www.jamf.com/jamf-nation/third-party-products/files/licensed-software-templates

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

2. Click **Computers** at the top of the page.

3. Click **Licensed Software**.

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**.

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**.

   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**.

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 of 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 Computer
  You can view the licensed software in use on a 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 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**.
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 computer or 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 Computer

The Application Usage logs for a 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 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**.

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 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**.

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.

Related Information

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

Viewing Restricted Software for a Computer
Find out how to view the restricted software for a 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 of Mobile Devices

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 several ways to enroll mobile devices with the JSS:

- **User-initiated enrollment**—You can allow users to enroll 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.
  Personally owned devices can only be enrolled via user-initiated enrollment, and require an enabled personal device profile assigned to the site that the user has access to (or to the full JSS if sites have not been added to the JSS). For more information, see Personal Device Profiles.
- **Enroll mobile devices using an enrollment profile**—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).
  For Apple TV devices, you must install the enrollment profile using Apple Configurator.
- **Enroll mobile devices using a PreStage enrollment**—A PreStage enrollment allows you to store enrollment and mobile device setup settings in the JSS and use them to enroll iOS and tvOS devices with the JSS. This reduces the amount of time and interaction it takes to prepare new mobile devices for use.
  You can also use Apple Configurator 2 and a PreStage enrollment to enroll devices with the JSS, supervise them, and configure device setup.
  This enrollment method requires an Apple Deployment Programs account. For more information, see the Integrating with Apple's Device Enrollment Program (DEP) Knowledge Base article.
- **Apple Configurator enrollment**—You can enroll mobile devices with the JSS by connecting them to a computer via USB and using an enrollment URL with Apple Configurator 2.

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 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.
- Mobile Device PreStage Enrollments
  Find out how to enroll mobile devices using a PreStage enrollment.

- [Apple Configurator Enrollment Settings](#)
  Find out how to enable Apple Configurator enrollment so you can enroll mobile devices using Apple Configurator and an enrollment URL.

For related information, see the following Knowledge Base article:

[Components Installed on Mobile Devices](#)
Learn about the components installed on mobile devices during enrollment.

For related information, see the following technical paper:

[Deploying iOS Devices Using Apple Configurator 2 and the Casper Suite](#)
Get step-by-step instructions on how to deploy iOS devices using Apple Configurator 2.

User-Initiated Enrollment for Mobile Devices

You can allow users to enroll 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. The enrollment URL is the full URL for the Jamf Software Server (JSS) followed by "/enroll". For example:

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

You can provide the enrollment URL to users by doing the following:

- **Provide the URL in the way that best fits your environment**
  Simply provide the URL to users in the way that best fits your needs. You can add a mobile device to a site when using this method.

- **Send an enrollment invitation to users via email or SMS**
  This allows you create an email or SMS invitation in the JSS and send it to one or more users. It gives you more control over user access to the enrollment portal by allowing you to do the following:

  - Set an expiration date for the invitation

  - Require users to log in to the portal

  - Allow multiple uses of the invitation

  - Add the mobile device to a site during enrollment

  - View the status of the invitation

  Note: Mobile device enrollment invitations cannot be sent to personally owned devices. You must provide the enrollment URL to those users by some other means.

Users can log in to the enrollment portal using an LDAP directory account or a JSS user account. When a user logs in with an LDAP directory account, user and location information is submitted to the JSS during enrollment. When a user logs in with a JSS user account, it allows an LDAP user to be assigned to the mobile device.

Requirements

To allow mobile devices to be enrolled with user-initiated enrollment, you need:

- A push certificate in the JSS (For more information, see Push Certificates.)

- User-initiated enrollment enabled (For more information, see User-Initiated Enrollment Settings.)

Note: For mobile devices with iOS 10.3 or later, Apple has enabled an important security enhancement that requires untrusted root certificates installed manually on unsupervised iOS devices to be manually trusted in Certificate Trust Settings during user-initiated enrollment, or installation of the MDM profile will fail. For more information, see the following Knowledge Base article:
Changes in User-Initiated Enrollment with Untrusted Certificate Authority (CA) Signed SSL Certificates in iOS 10.3 and Later .

To send a mobile device enrollment invitation via email or SMS, you need an SMTP server set up in the JSS. (For more information, see Integrating with an SMTP Server.)

For users to log in to the enrollment portal with an 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 for User-Initiated Enrollment

You can send an email or SMS invitation that contains the enrollment URL from the JSS. Users click the enrollment URL in the email or SMS message to access the enrollment portal.

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**.
4. Click **New** + .
5. Select **User-Initiated Enrollment** as the enrollment method.
6. Follow the onscreen instructions to send the enrollment invitation.

   An enrollment invitation is immediately sent to the 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 specific 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**.
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.

Related Information

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

- User-Initiated Enrollment Settings
  Learn about the settings you can configure for user-initiated enrollment.

- User-Initiated Enrollment Experience for Mobile Devices
  Learn about the steps users take to enroll mobile devices.

For related information, see the following Knowledge Base article:

Components Installed on Mobile Devices
Learn about the components installed on mobile devices during enrollment.

User-Initiated Enrollment Experience for Mobile Devices
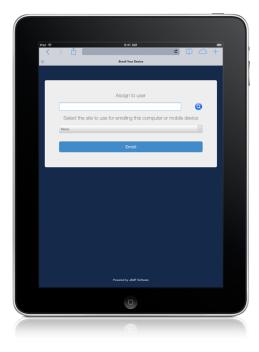
When a user accesses the enrollment URL from a mobile device, they are guided through a series of steps to enroll the device. The steps vary depending on the platform of the device being enrolled—iOS or Android.

User-Initiated Enrollment Experience for iOS Devices

iOS devices can be enrolled as institutionally owned or personally owned devices.

Note: Apple has enabled an important security enhancement beginning with iOS 10.3. This security enhancement requires untrusted root certificates installed manually on unsupervised iOS devices to be manually trusted in Certificate Trust Settings during user-initiated enrollment, or installation of the MDM profile will fail. For more information, see the following Knowledge Base article: Changes in User-Initiated Enrollment with Untrusted Certificate Authority (CA) Signed SSL Certificates in iOS 10.3 and Later .

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 Log in.
   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 about enrollment invitations, see User-Initiated Enrollment for Mobile Devices.)

If notified that the device cannot verify the identity of the JSS, the user must tap **Continue** to log in to the enrollment portal.
This notification only appears if the SSL certificate is not natively trusted by the device.

2. The user is prompted to enroll the device as a personally owned device or an institutionally owned device.
This is only displayed if both institutionally owned device enrollment and personally owned device enrollment are enabled in the JSS.

You can display a description to users who enroll a personally owned device. (For more information, see [User-Initiated Enrollment Settings](#).)
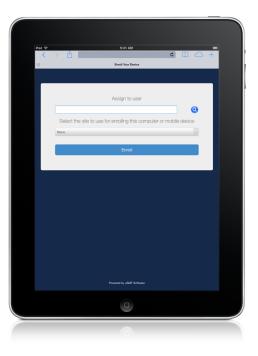
You can display a description to users who enroll an institutionally owned device.

3. When prompted, the user must choose the site that they are associated with.
   If the user is associated with multiple sites, they must select the site that will assign the appropriate settings to the device.
   If the user signed in with a JSS user account, they can assign an LDAP user to the computer at this time.

4. The user is prompted to continue to the CA certificate installation.

Note: For mobile devices with iOS 11, a pop-up window will appear notifying users, "This website is trying to open Settings to show you a configuration profile. Do you want to allow this?" The user must tap **Allow**.

5. The user must tap **Install** to continue.

6. When notified that the profile will change settings on the device, the user must tap **Install**. If the device has a passcode, the user must enter the passcode.

7. To complete the installation, the user must tap **Done**.

8. The user is prompted to continue to the MDM profile installation.
Information about enrollment can be accessed by tapping the **Information** icon.

Note: For mobile devices with iOS 11, a pop-up window will appear notifying users, "This website is trying to open Settings to show you a configuration profile. Do you want to allow this?" The user must tap **Allow**.

9. The user must tap **Install** to continue.

10. 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.
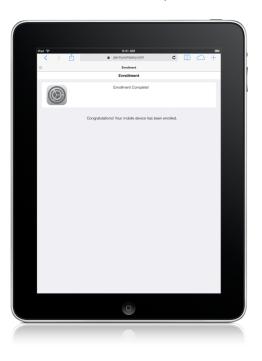
11. When notified that installing the profile will allow an administrator to remotely manage the device, the user must tap **Install**.

12. To complete the enrollment process, the user must tap **Done**.

When the enrollment is complete, the device is enrolled with the JSS.

If you chose to install Self Service Mobile, users are prompted to install the app from the App Store. (For more information, see Self Service Mobile.)

User-Initiated Enrollment Experience for Android Devices

Android devices can only be enrolled as personally owned devices.
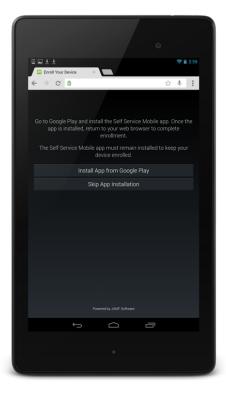
During user-initiated enrollment of an Android device, the user is required to install Self Service Mobile from Google Play. Self Service Mobile must remain installed on an enrolled Android device to keep the device managed by the JSS.

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 **Log In**.

2. If prompted, the user must choose the site that they are associated with.
   If the user is associated with multiple sites, they must select the site that will assign the appropriate settings to the device.

3. The user is prompted to go to Google Play to install Self Service Mobile, and then return to the enrollment portal.
   Note: If the user already has Self Service Mobile installed, they can skip the app installation step.

4. If the user goes to Google Play to install Self Service Mobile, they must tap **Install** to start the app installation process.

5. The user must then tap **Accept** to install Self Service Mobile.

6. When the Self Service Mobile installation is complete, the user must return to the enrollment portal in their web browser.
Note: If the user taps **Open** in Google Play to open Self Service Mobile, a welcome page directs the user to return to their web browser to continue enrollment. If the user knows the JSS URL to use for enrollment, they can tap **Manually Enroll Using JSS URL** and complete enrollment in Self Service Mobile.

7. The user is prompted to continue to the MDM profile installation.
The user can access information about enrollment by tapping the **Information** icon.

If notified that the device cannot verify the server's identity, the user must tap **Yes** to log in to the enrollment portal.
This notification only appears if the SSL certificate is not natively trusted by the device.

The Self Service Mobile enrollment progress page is displayed.

8. When prompted to activate Self Service Mobile as a device administrator, the user must tap **Activate**.

When enrollment is complete, the device is enrolled with the JSS.

9. (Optional) The user can tap **Continue** to install third-party apps if appropriate for their environment.

The user can then install apps for configuring email, calendar, and contacts, and for configuring a VPN connection.

Apple Configurator Enrollment Settings

The Apple Configurator Enrollment settings allow you to enroll mobile devices with the Jamf Software Server (JSS) using Apple Configurator 2 and an enrollment URL. This involves enabling Apple Configurator enrollment in the JSS, and then connecting devices to a computer via USB to enroll them using Apple Configurator 2 and an enrollment URL.

You can enable one or both of the following types of Apple Configurator enrollment URL:

- **Static URL –** Using a static URL allows you to manually provide the URL to the person that operates the Apple Configurator workstation in the way that best fits your environment. The static URL cannot expire and does not allow you to enroll devices into sites as a part of the enrollment process. The static enrollment URL for the JSS is the URL for the JSS followed by "/configuratorenroll". For example:
  https://jss.mycompany.com:8443/configuratorenroll

- **Dynamic URL –** Using a dynamic URL allows you to view a randomly generated enrollment URL in the JSS or send that URL to the person that operates the Apple Configurator workstation via an enrollment invitation, allowing for a more secure enrollment experience. When you view or send a dynamic URL via an enrollment invitation, you can set the expiration date for the URL and choose a site to add devices to during enrollment.

Requirements

Apple Configurator enrollment only applies to mobile devices with iOS 9 or later. In addition, you need Apple Configurator 2.0 or 2.1.

Enabling Apple Configurator Enrollment via Static URL

Before you can enroll mobile devices using Apple Configurator and a static URL, you must enable Apple Configurator enrollment 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 **Mobile Device Management**.

4. Click **Apple Configurator Enrollment** 📱 .

5. Click the **Enrollment** tab, and then click Edit.

6. Select **Enable Apple Configurator Enrollment via Static URL**.

7. Click **Save**.

You can now use the static URL with your Apple Configurator workstation.

Enabling Apple Configurator Enrollment via Dynamic URL

Before you can enroll mobile devices using Apple Configurator and a dynamic URL, you must enable Apple Configurator enrollment 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 **Mobile Device Management**.

4. Click **Apple Configurator Enrollment** ⬚ .

5. Click the **Enrollment** tab, and then click **Edit**.

6. Select **Enable Apple Configurator Enrollment via Dynamic URL** .

7. Click **Save**.

   Dynamic URLs can now be viewed in the JSS or sent to the person that operates the Apple Configurator workstation via an enrollment invitation.

   Viewing or Sending a Dynamic Apple Configurator Enrollment URL via a Mobile Device Enrollment Invitation

   You can view the dynamic Apple Configurator enrollment URL or send an email or SMS invitation that contains the URL from the JSS to the person that operates the Apple Configurator workstation. The enrollment URL is used with Apple Configurator to enroll mobile devices with the JSS.

   Before you configure the invitation, make sure you have the email address or phone number of the person 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**.

4. Click **New** ＋ .

5. Select **Apple Configurator Enrollment** as the enrollment method.

6. Follow the onscreen instructions to view or send the enrollment invitation.

   If you chose to view the enrollment URL, it is displayed in the JSS. If you chose to send the enrollment URL, an enrollment invitation containing the dynamic URL is sent to the 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 specific 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**.

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.

Related Information

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

Supervision Identities
Find out how to create, upload, and download a supervision identity for use with Apple Configurator 2.

For related information, see the following Knowledge Base article:

Components Installed on Mobile Devices
Learn about the components installed on mobile devices during enrollment.

For related information, see the following technical paper:

Deploying iOS Devices Using Apple Configurator 2 and the Casper Suite
Get step-by-step instructions on how to deploy iOS devices using Apple Configurator 2 and an enrollment URL.

Supervision Identities

If you plan to supervise devices and deploy them using Apple Configurator 2 and the Casper Suite, you can use a supervision identity to pair supervised devices with multiple Apple Configurator 2 workstations that have the same supervision identity. A supervision identity can be applied to a device by pairing the device with an Apple Configurator 2 workstation or by enrolling the device with the JSS using a PreStage enrollment configured with a DEP instance that has a supervision identity.

A supervision identity certificate (.p12 file) can be created in the JSS or created in Apple Configurator 2 and then uploaded to the JSS. The identity can then be stored in the JSS until you need to download it and add it to other Apple Configurator 2 workstations, or add it to a DEP instance for use with a PreStage enrollment.

Note: To ensure devices are paired securely with each Apple Configurator 2 workstation, the workstations you are using must have matching supervision identities. If the wrong identity is applied to a device, the device must be wiped, re-supervised, and re-enrolled to change the identity.

For more information about supervision identities, see Apple's Configurator 2 Help documentation at:

http://help.apple.com/configurator/mac

For step-by-step instructions on how to use supervision identities while deploying mobile devices using Apple Configurator 2, see the following technical paper:

Deploying iOS Devices with Apple Configurator 2 and the Casper Suite

Requirements

To use supervision identities, you need:

- Supervised devices with iOS 9 or later, or tvOS 10.2 or later
- Apple Configurator 2.0 or 2.1

Creating a Supervision Identity

You can create a supervision identity in the JSS for use with Apple Configurator 2.

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**.
4. Click **Apple Configurator Enrollment** 📱 .
5. Click the **Supervision Identities** tab, and then click **Edit**.
6. Click **New**.

7. Configure the supervision identity using the fields on the pane.

8. Click **Save**.

Uploading a Supervision Identity

If you created a supervision identity using Apple Configurator 2, you can upload that identity to the JSS so it can be accessed from other Apple Configurator 2 workstations or added to a DEP instance.

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**.

4. Click **Apple Configurator Enrollment** 📱 .

5. Click the **Supervision Identities** tab, and then click **Edit**.

6. Click **Upload**.

7. Click **Upload Supervision Identity** and upload the supervision identity (.p12).

8. Configure the supervision identity using the fields on the pane.

9. Click **Save**.

Downloading a Supervision Identity

You can download a supervision identity from the JSS and add it to the Apple Configurator 2 workstations that you want your devices with the same supervision identity to trust.

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**.

4. Click **Apple Configurator Enrollment** 📱 .

5. Click the **Supervision Identities** tab.

6. Click **View** next to the supervision identity you want to download.

7. Click **Download**.

8. Click **Done**.

Adding a Supervision Identity to a DEP Instance

When you add a supervision identity to a DEP instance, that identity is applied to all devices enrolled using a PreStage enrollment that is configured with the DEP instance.

Note: Devices that are already enrolled with the JSS and associated with a DEP instance need to be re-enrolled to become associated with the supervision identity for that DEP instance.

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**.

4. Click **Device Enrollment Program** .

5. Click the DEP instance you want to add a supervision identity to.

6. Click **Edit**.

7. Select the supervision identity you want to add from the **Supervision Identity for Use with Apple Configurator** pop-up menu.

8. Click **Save**.

Related Information

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

- [Integrating with the Device Enrollment Program](#)
  Find out how to configure an instance of DEP.

- [Mobile Device PreStage Enrollments](#)
  Find out how to enroll mobile devices using a PreStage Enrollment.

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**.

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. (Optional) Click the **Attachments** tab and click **Upload** to upload an attachment.

9. 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**.

4. Click **New** ➕ .

5. Use the General pane to configure basic settings for the enrollment profile.

6. 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.

7. (Optional) Click the **User and Location Information** tab and specify user and location information for the devices.

8. (Optional) Click the **Purchasing Information** tab and specify purchasing information for the devices.

9. (Optional) Click the **Attachments** tab and click **Upload** to upload an attachment.

10. Click **Save**.

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**.

4. Click the enrollment profile you want to download.

5. Click **Download**.
   On macOS 10.7 or later, you may be prompted to install the profile. Click **Cancel** to decline.

   The enrollment profile downloads immediately as a .mobileconfig file.

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**.

4. Click the enrollment profile for which you want to download a Trust Profile.

5. Click **Trust Profile**.
   On macOS 10.7 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`.

   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 Knowledge Base article:

Components Installed on Mobile Devices
Learn about the components installed on mobile devices during enrollment.

For related information, see the following technical paper:

Deploying iOS Devices Using Apple Configurator 2 and the Casper Suite
Get step-by-step instructions on how to deploy iOS devices using Apple Configurator 2 and an enrollment profile.

Mobile Device PreStage Enrollments

A PreStage enrollment allows you to store enrollment and mobile device setup settings in the Jamf Software Server (JSS) and use them to enroll new iOS and tvOS devices with the JSS. This reduces the amount of time and interaction it takes to prepare mobile devices for use. For tvOS devices, this includes supervising devices, requiring users to apply the MDM profile for enrollment, and auto advancing through the Setup Assistant with optional settings to skip selected items during enrollment.

Before you can use a PreStage enrollment, you need to integrate the JSS with the Device Enrollment Program (DEP). This creates an instance of DEP in the JSS. (For more information, see Integrating with the Device Enrollment Program.) Only devices associated with a DEP instance can be enrolled with the JSS using a PreStage enrollment.

After creating a DEP instance, you need to create a PreStage enrollment in the JSS for the mobile devices you want to enroll. Creating a PreStage enrollment allows you to configure the enrollment settings and customize the user experience of the Setup Assistant. You can also specify the mobile devices that should be enrolled using the PreStage enrollment. In addition, you can specify that devices newly associated with the DEP instance be automatically added to the PreStage enrollment.

You can require users to authenticate during mobile device setup using an LDAP directory account or a JSS user account. If users authenticate with an LDAP directory account, user and location information is submitted during enrollment.

Requirements

To require LDAP users or JSS users to authenticate during mobile device setup, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.) In addition, authentication requires mobile devices with iOS 7.1 or later, or Apple TV devices with tvOS 10.2 or later.

To enable Shared iPad, you need the following:

- Supervised iPads with iOS 9.3 or later
- Apple Education Support enabled in the JSS. (For more information, see Apple Education Support Settings.)
- The user's Managed Apple ID entered in the Roster category of user inventory information. (For more information, see Viewing and Editing Inventory Information for a User.)

For more information on Shared iPad, see the following technical paper:
Supporting Apple's Classroom App and Shared iPad Using the Casper Suite

Configuring a Mobile Device PreStage Enrollment

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

2. Click **Mobile Devices** at the top of the page.

3. Click **PreStage Enrollments**.

4. Click **New** + .

5. Use the General payload to configure basic settings for the PreStage enrollment.
To enable Shared iPad during enrollment, select **Supervise Devices** and then select **Enable Shared iPad**. You must also select the maximum number of user accounts that can be stored with Shared iPad using the **Number of users** pop-up menu. This limits the number of user accounts that can be stored locally on the iPad.
To customize the user experience of the Setup Assistant, select which steps you want to skip in the Setup Assistant. If you choose to skip steps, the user can enable these settings after the device is configured unless otherwise restricted. For Apple TV devices, Ethernet connection is required.

6. (Optional) Use the Mobile Device Names payload to choose a method for assigning names to mobile devices.
This information is stored in the JSS for each mobile device enrolled using a PreStage enrollment.
The Mobile Device Names payload is only displayed if the **Supervise Devices** checkbox is selected.
The List of Names naming method requires mobile devices with iOS 8 or later.

7. (Optional) Use the User and Location payload to specify user and location information for the mobile devices.
This information is stored in the JSS for each mobile device enrolled using a PreStage enrollment.
The User and Location Information payload is only displayed if the **Require Authentication** checkbox is not selected.

8. (Optional) Use the Purchasing payload to specify purchasing information for the mobile devices.
This information is stored in the JSS for each mobile device enrolled using a PreStage enrollment.

9. (Optional) Use the Attachments payload to upload attachments to store for mobile devices.
This information is stored in the JSS for each mobile device enrolled using a PreStage enrollment.

10. If the SSL certificate you are using is signed by an external CA (your organization's CA or a trusted third-party CA), use the Certificates payload to upload a certificate for the CA that you want mobile devices to trust at enrollment.
The anchor certificate is only displayed if the SSL certificate you are using is signed by the JSS's built-in CA.

11. Click the **Scope** tab and configure the scope of the PreStage enrollment by selecting the checkbox next to each mobile device you want to add to the scope.
The mobile devices listed on the **Scope** tab are the mobile devices that are associated with the Device Enrollment Program (DEP) via the server token file (.p7m) you downloaded from the Apple Deployment Programs website.
Note: If you want to add mobile devices to the scope automatically as the devices become associated with the DEP instance, select the **Automatically assign new devices** checkbox in the General payload.

12. Click **Save**.

Refreshing PreStage Enrollment Information

The JSS allows you to manually refresh information about the mobile devices in the PreStage enrollment as needed.

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

2. Click **Mobile Devices** at the top of the page.

3. Click **PreStage Enrollments**.

4. Click the PreStage enrollment you want to refresh.

5. Click **Refresh**.

If there is updated information about the mobile devices in DEP, this information is displayed in the JSS.

Further Considerations

When cloning a PreStage enrollment, mobile devices in the scope of the original PreStage enrollment are not included in the scope of the cloned PreStage enrollment.

Related Information

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

- Integrating with the Device Enrollment Program
  Find out how to configure an instance of DEP.
- User-Initiated Enrollment for Mobile Devices
  Find out how to allow users to enroll mobile devices by having them log in to an enrollment portal.

For related information, see the following Knowledge Base article:

Components Installed on Mobile Devices
Learn about the components installed on mobile devices during enrollment.

For related information, see the following technical paper:

Deploying iOS Devices Using Apple Configurator 2 and the Casper Suite
Get step-by-step instructions on how to deploy iOS devices using Apple Configurator 2 and a PreStage enrollment.

Inventory for Mobile Devices

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 (does not apply to personally owned devices).
- Collect user and location from an LDAP directory service (only available if an LDAP server is set up in the JSS).
- Monitor iBeacon regions so that mobile devices with Self Service Mobile for iOS installed submit information to the JSS when they enter or exit a region.

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**.
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
  Learn how to create and save an advanced mobile device search.
- Viewing and Editing Inventory Information for a Mobile Device
  Find out how to view and edit inventory information for a mobile device.
- iBeacon Regions
  Learn what iBeacon regions can be used for and how you can add them to the JSS.

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.

Note: Mobile device extension attributes do not apply to personally owned mobile devices.

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 Mobile Device 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**.

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.

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 Mobile Device
  You can view the extension attributes collected from a 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 each JSS user 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**.

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

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all results

In general, searches are not case-sensitive.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains". (For more information, see Configuring Account Preferences.)

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

Usage	Example
Use an asterisk after a search term to return all results with attributes that begin with that term.	Perform an app search for "Adobe*" to return all apps that begin with "Adobe".
Use an asterisk before a search term to return all results with attributes that end with that term.	Perform a mobile device search for "*@mycompany.com" to return all mobile devices with email addresses that end with "@mycompany.com".
Use an asterisk before and after a search term to return all results that include that term.	Perform an app search for "*pro*" to return all apps that include "pro".
Use an asterisk without any other terms to return all results for the item you are searching.	Perform a mobile device search for "*" to return all mobile devices.

Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform an app search for "news*, *pro" to return all applications that begin with "news" and end with "pro".

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a mobile device search for "*@mycompany.com, -555*" to return all mobile devices with email addresses that end with "@mycompany.com" except for those with phone numbers that begin with "555".

Returning All Results

There are two ways to return all results: use an asterisk (*) without any other characters or terms, or perform a blank search.

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**.
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 Mobile Device
  Find out how to view and edit inventory information for a 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
  Find out how to create and save an advanced mobile device search.

- Mobile Device Inventory Display Settings
  Find out 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**.
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 **Show Advanced 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.

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**.

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**.

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 Mobile Device
  Find out how to view and edit inventory information for a 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 of 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 building or department.
- Edit the site.
- Look up and populate purchasing information from Apple's Global Service Exchange (GSX).
- Send a mass email to users.
- Send a mass notification to mobile devices with Self Service Mobile for iOS installed.
- Delete the mobile devices from the JSS.
- Send remote commands.
- Cancel management commands.

Mass actions can be performed on static or smart group membership lists or mobile device search results.

Mass Editing the Building or Department for Mobile Devices

Mass editing the building or department for mobile devices allows you to add the mobile devices 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 **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 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 and department.

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.

Note: Changing the site that personally owned devices belong to automatically changes the personal device profile that is used to perform management tasks on those devices. For more information, see Personal Device Profiles.

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.
   Note: When mobile devices are added to a site, any users assigned to those mobile devices are also added to that 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.

Sending a Mass Notification to Mobile Devices

You can send a mass notification to mobile devices.

This requires mobile devices with Self Service Mobile for iOS installed. (For more information, see Installing Self Service on Mobile Devices.)

Notifications are displayed to users in the following ways:

- The Self Service Mobile icon displays a badge with the number of notifications that have not been viewed by the user.

- In Self Service Mobile, the **Notifications** browse button displays a badge with the number of notifications that have not been viewed by the user. Items are listed in the "Notifications" area of the app as they are added.

- (Optional) Each notification can be configured to also display an alert and appear in Notification Center. This requires a proxy server token in the JSS. (For more information, see Jamf Push Proxy.)

For more information about how notifications are displayed, see Self Service User Experience on Mobile Devices.

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 a Notification to Mobile Devices with Self Service Mobile Installed**.

6. Follow the onscreen instructions to send the notification.

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.

Mass Sending Remote Commands to Mobile Devices

You can mass send the following remote commands to mobile devices:

- Update iOS version
- Clear passcode
- Lock device
- Update inventory
- Wipe device
- Unmanage Institutionally Owned Device
- Set wallpaper
- Enable/Disable diagnostic and usage reporting and app analytics
- Shut down device
- Restart device
- Update passcode lock grace period

The remote commands available for a particular device vary depending on the device ownership type, device platform, device type, and OS version. For more information, see the following sections in this guide:

- Remote Commands for Mobile Devices
  Learn about remote command requirements.
- Mobile Device Management Capabilities
  Learn about remote command availability on institutionally and personally owned devices.

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 Remote Commands**.

6. Select the remote command to send to mobile devices.

7. Follow the onscreen instructions to send the remote command.

Mass Canceling Management Commands on Mobile Devices

You can mass cancel all pending or all failed management commands on 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 **Cancel Management Commands**.

6. Follow the onscreen instructions to cancel all pending or all failed management commands on the mobile devices.

Related Information

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

Viewing and Editing Inventory Information for a Mobile Device
Find out how to view and edit inventory information for a single mobile device.

Viewing and Editing Inventory Information for a Mobile Device

The Jamf Software Server (JSS) stores detailed inventory information for each managed mobile device. You can view and edit this information from the JSS.

Note: The inventory information displayed for a particular device varies depending on the device ownership type, device platform, device type, and OS version. For more information, see Mobile Device Management Capabilities.

The following table lists the information that you can view and edit for each mobile device.

Note: Extension attributes are displayed in mobile device inventory information in the category in which they are configured to display.

Field	Editable	Notes	Personally Owned Device Support	
General Category			iOS	Android
Mobile Device Name	✓ Editable for supervised devices with iOS 8 or later when Enforce Mobile Device Name is configured		✓	✓
JSS Mobile Device ID			✓	
Asset Tag	✓			
Site	✓		✓	✓
Last Inventory Update			✓	✓
iOS Version		For Apple TV devices prior to tvOS 10.2, the iOS version is equivalent to the OS build version on which the Apple TV software is based. The Apple TV software version is not collected. For Apple TV devices with tvOS 10.2 or later, the tvOS version is displayed.	✓	

Field	Editable	Notes	Personally Owned Device Support	
iOS Build			✓	
Android Version Name				✓
Android Version				✓
Android API Level				✓
IP Address			✓	✓
Managed			✓	✓
Supervised				
Shared iPad		Displays whether Shared iPad has been enabled on the iPad. (This only displays for supervised iPads with iOS 9.3 or later.)		
Maximum Shared iPad Users Stored		Displays the maximum number of user accounts that can be stored with Shared iPad		
Device Ownership Type			✓	✓
Enrollment Method			✓	
Last Enrollment			✓	✓
Device Locator Service Enabled		Displays whether Find my iPhone/iPad has been enabled on the mobile device		
Do Not Disturb Enabled				
iCloud Backup				
Last iCloud Backup				

Field	Editable	Notes	Personally Owned Device Support	
Bluetooth Low Energy Capability		To detect Bluetooth Low Energy capability, the mobile device must have Self Service Mobile for iOS installed. If Self Service Mobile has never been launched on the device, this value will be reported as "Not Capable/Unknown".	✓	
Location Services For Self Service Mobile		Displays whether Location Services has been enabled on the mobile device for the Self Service Mobile app To detect if Location Services has been enabled for Self Service Mobile, the device must have Self Service Mobile for iOS installed. If Self Service Mobile has never been launched on the device, or if Self Service Mobile has not been launched since the initial iBeacon region was added to the JSS, this value will be reported as "Not Enabled /Unknown".	✓	
Logged in to iTunes Store			✓	
AirPlay Password	✓	Apple TV only		
Locales		Apple TV only		
Languages		Apple TV only		
Hardware Category			iOS	Android
Capacity			✓	
Available Space			✓	
Used Space			✓	
Internal Capacity				✓
Internal Available Space				✓

Field	Editable	Notes	Personally Owned Device Support	
Internal Used Space				✓
External Capacity				✓
External Available Space				✓
External Used Space				✓
Battery Level			✓	✓
Serial Number			✓	✓
UDID			✓	✓
Wi-Fi MAC Address			✓	✓
Bluetooth MAC Address			✓	✓
Modem Firmware Version			✓	✓
Model			✓	✓
Model Identifier			✓	
Model Number			✓	
Manufacturer				✓
User and Location Category			iOS	Android
Username	✓		✓	✓
Full Name	You can assign a user to the mobile device and populate user information from the **Users** tab. (For more information, see User Assignments.)			
Email Address				
Phone Number				
Position				
Department				

Field	Editable	Notes	Personally Owned Device Support	
Building				
Room				
Shared iPad Users Category			iOS	Android
	✓ You can remove users from Shared iPad. The status of user removal is displayed in the list of pending management commands. (For more information, see Viewing the Pending Management Commands for a Mobile Device.)	Displays a list of the Managed Apple IDs of the users that logged in to the iPad. (This category is only displayed for iPads that have Shared iPad enabled. For more information, see Mobile Device PreStage Enrollments.)		

Field	Editable	Notes	Personally Owned Device Support	
Purchasing Category			iOS	Android
Purchased or Leased	✓ You can 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](#).)			
PO Number				
PO Date				
Vendor				
Warranty Expiration				
AppleCare ID				
Lease Expiration				
Purchase Price				
Life Expectancy				
Purchasing Account				
Purchasing Contact				
Extension Attributes Category			iOS	Android
	✓	Displays a list of custom data fields collected using extension attributes		
Security Category			iOS	Android
Data Protection			✓	✓
Hardware Encryption			✓	
Passcode Status			✓	
Block Encryption Capability			✓	✓

Field	Editable	Notes	Personally Owned Device Support	
File Encryption Capability			✓	✓
Passcode Compliance			✓	✓
Passcode Compliance with Config Profile			✓	✓
Activation Lock			✓	
Jailbreak Detected		To detect jailbreak status, the mobile device must have Self Service Mobile for iOS installed. The JSS will receive an updated Jailbreak Detected value each time Self Service Mobile is launched. If Self Service Mobile has never been launched on the device, this value will be reported as "Not Reported".	✓	
Lost Mode (supervised only)		Displays whether Lost Mode is enabled on the device You can play a sound on the device when Lost Mode is enabled by clicking the **Play Sound** button.		
Always enforce Lost Mode		Displays whether the **Always enforce Lost Mode** setting is enabled on the device.		
Lost Mode Message				
Lost Mode Phone Number				
Lost Mode Footnote				
Last Location Update		Displays the last time Global Positioning System (GPS) data was collected for the device when Lost Mode is enabled		

Field	Editable	Notes	Personally Owned Device Support	
Approximate Location	You can collect updated location data for the device by clicking the **Update Location** button.	Displays coordinates for the approximate location of the device when Lost Mode is enabled To collect GPS data for a device, the device must have a network connection.		
Horizontal Accuracy				
Vertical Accuracy				
Altitude				
Speed				
Course				
Timestamp				
Personal Device Profile Status		Displays whether the most up-to-date profile has been installed on the mobile device	✓	✓
Apps Category			iOS	Android
		Displays a list of apps installed on the mobile device	✓ **Note:** Only managed apps are collected.	
Managed eBooks Category			iOS	Android
		Displays a list of managed eBooks installed on the mobile device		
Network Category			iOS	Android
Home Carrier Network				
Current Carrier Network				
Carrier Settings Version				

Field	Editable	Notes	Personally Owned Device Support	
Cellular Technology				
Phone Number				
IMEI				
MEID				
ICCID				
Current Mobile Country Code				
Current Mobile Network Code				
Home Mobile Country Code				
Home Mobile Network Code				
Voice Roaming				
Data Roaming Status				
Roaming Status				

Field	Editable	Notes	Personally Owned Device Support	
iBeacon Regions Category			iOS	Android
		Displays a list of iBeacon regions that the mobile device is currently in. (This category is only displayed if the Mobile Device Inventory Collection settings are configured to monitor iBeacon regions. For more information, see Mobile Device Inventory Collection Settings.)		
Certificates Category			iOS	Android
		Displays a list of certificates installed on the mobile device	✓	
Profiles Category			iOS	Android
		Displays a list of profiles installed on the mobile device		
Provisioning Profiles Category			iOS	Android
		Displays a list of provisioning profiles installed on the mobile device	✓	
Attachments Category			iOS	Android
	✓ You can upload and delete attachments.	Displays a list of files attached to the inventory record		

Viewing Inventory Information for a 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 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 purchasing information, you can click Search 🔍 to look up and populate information from Apple's Global Service Exchange (GSX).
   Note: This button is only displayed if you have a GSX connection set up in the JSS.
   If you are editing user and location information, the changes are applied in the Users tab. This specified information is also applied in the inventory information for computers, peripherals, and other mobile devices that the user is assigned to. For information on assigning a user to a mobile device or removing a user assignment, see User Assignments.)

7. Click **Save**.

Viewing Management Information for a Mobile Device

The Jamf Software Server (JSS) allows you to view the following management information for each mobile device:

- Pending management commands
- iOS configuration profiles
- Activation Lock bypass code
- Apps
- eBooks
- Group memberships

Note: The management information available for a particular device varies depending on the device ownership type, device platform, device type, and iOS version. For more information, see Mobile Device Management Capabilities.

Viewing the Pending Management Commands for a Mobile Device

When viewing management information for a 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 remote commands
- Installing or removing iOS configuration profiles
- Installing or removing apps
- Installing or removing managed eBooks
- Installing or removing provisioning profiles
- Updating inventory
- Performing other actions that are based on MDM commands (for example, removing a user from Shared iPad or updating location information for Lost Mode)
- Remote commands that are being sent to a mobile device automatically if your environment uses the Healthcare Listener

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.

   Note: If your environment uses the Healthcare Listener, "Healthcare Listener" is displayed as the value in the Username column for the remote command that is automatically sent to the mobile device. For more information about the Healthcare Listener, see Healthcare Listener.

Viewing Configuration Profiles for a Mobile Device

When viewing management information for a 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 the Activation Lock Bypass Code for a Mobile Device

When viewing management information for a mobile device, you can view the Activation Lock bypass code for the mobile device.

For information about what the Activation Lock bypass code can be used for, see the Leveraging Apple's Activation Lock Feature with the Casper Suite Knowledge Base article.

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 the Activation Lock bypass code 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 **Activation Lock Bypass** category.

6. Click **Get Activation Lock Bypass Code**.
   The Activation Lock bypass code is displayed on the pane.

Viewing Apps for a Mobile Device

When viewing management information for a 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 Mobile Device

When viewing management information for a 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 Mobile Device

When viewing management information for a 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 Mobile Device

The Jamf Software Server (JSS) allows you to view the history for each mobile device. The information you can view includes:

- Management history (completed, pending, and failed management commands)
- Audit logs
- User and location history
- Completed, pending, and failed app installations
- Completed, pending, and failed managed eBook installations

Note: The management history available for a particular device varies depending on the device ownership type, device platform, device type, and iOS version. For more information, see Mobile Device Management Capabilities.

Viewing Management History for a Mobile Device

The management history for a 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 managed eBooks
- 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 Audit Logs for a Mobile Device

The audit logs allow you to view a list of the following events that occurred for a mobile device:

- The mobile device's Activation Lock bypass code has been viewed. (For more information, see [Viewing the Activation Lock Bypass Code for a Mobile Device](#).)
- The following remote commands have been sent to the mobile device:
  - Wipe device
  - Unmanage device
  - Clear passcode
- Remote commands have been sent to an iPad automatically (only available if your environment uses the Healthcare Listener).

The date/time that the event occurred and the username of the administrator who initiated the event are included in the log.

Note: If your environment uses the Healthcare Listener, "Healthcare Listener" is displayed as the value in the Username column for the remote command that is automatically sent to the mobile device. For more information, see [Healthcare Listener](#).

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 audit logs 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 **Audit Logs** category.
   Audit logs for the mobile device are displayed.

Viewing User and Location History for a Mobile Device

The user and location history for a 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 Mobile Device

You can view the completed, pending, and failed app installations for a mobile device. You can also cancel pending app installations.

Note: For a personally owned iOS device, you can only view managed 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**.

Viewing Managed eBook Installations for a Mobile Device

You can view the completed, pending, and failed managed eBook installations for a mobile device. You can also cancel pending managed eBook 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 managed eBook 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 **Managed eBooks** category.
   A list of managed eBooks installed on the mobile device is displayed.

6. To view a list of managed eBooks that are pending installation, click **Pending eBooks**.
   You can cancel a pending installation by clicking **Cancel** for the eBook.

7. To view a list of managed eBooks that failed to install, click **Failed eBooks**.
   You can cancel a failed installation by clicking **Cancel** for the eBook.

Deleting a 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 Remote Commands for Mobile Devices.)

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

2. Click **Mobile Devices** at the top of the page.

3. Click **Search Inventory**.

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.

Note: Personally owned mobile devices cannot be included in mobile device group memberships.

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).

You can configure a smart mobile device group to send remote commands to mobile devices when the devices become members of that group. For example, the Set Wallpaper remote command can be configured to automatically set the wallpaper on devices when they become members of the smart group.

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**.
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 **Show Advanced 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.
      Note: Creating a smart mobile device group with no criteria will cause all managed mobile devices to be included in the group's membership.
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.

9. (Optional) Click the **Automated Management** tab and configure remote commands to send to devices that are members of the group.

10. 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**.

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**.

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**.
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.

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**.
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

Mobile Device Configuration Profiles

Mobile device configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for mobile devices.

The Casper Suite can be used to deploy mobile device configuration profiles to the following types of mobile devices:

- iPads, iPhones, or iPod touches with iOS 4 or later
- Apple TV devices with Apple TV software based on iOS 7 or later, or Apple TV devices with tvOS 10.2 or later

A configuration profile will deploy containing both the iOS and tvOS selected options to all devices in scope. Devices will ignore the options that do not pertain to their device type.

For detailed information on payload capabilities for iOS and tvOS devices, see Payload Capabilities for Mobile Device Configuration Profiles.

You can use the Jamf Software Server (JSS) to manually create a mobile device 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 a configuration profile to an iOS device—install it automatically (requires no interaction from the user) or make it available in Self Service. For tvOS devices, configuration profiles must be distributed by installing automatically. You can also specify the mobile devices and users to which the profile should be applied (called "scope").

Note: Mobile device configuration profiles cannot be distributed to personally owned mobile devices.

Payload Variables for Mobile Device Configuration Profiles

There are several payload variables that you can use to populate settings in a mobile device 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
$ASSET_TAG	Asset Tag
$SITENAME	Site Name
$SITEID	Site ID
$SERIALNUMBER	Serial Number
$UDID	UDID
$USERNAME	Username
$FULLNAME or $REALNAME	Full Name
$EMAIL	Email Address
$PHONE	Phone Number
$ROOM	Room
$POSITION	Position
$DEPARTMENTNAME	Department Name
$DEPARTMENTID	Department ID
$BUILDINGNAME	Building Name
$BUILDINGID	Building ID
$MACADDRESS	MAC Address
$JSSID	JSS ID
$PROFILEJSSID	JSS ID of the Configuration Profile

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 a Mobile Device 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**.

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 Self Service, do the following:

   a. Choose a **Security** setting.

   b. Click the **Self Service** tab, and specify an icon to display in Self Service.

   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.
   Note: For limitations or exclusions to be based on LDAP users or LDAP user groups, the Username field must be populated in the mobile device's inventory.

9. Click **Save**.

   The profile is distributed to mobile devices in the scope the next time they contact the JSS.

Uploading a Mobile Device Configuration Profile

You can create a mobile device 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**.

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 Self Service, do the following:

   a. Choose a **Security** setting.

   b. Click the **Self Service** tab, and specify an icon to display in Self Service.

   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.
   Note: For limitations or exclusions to be based on LDAP users or LDAP user groups, the Username field must be populated in the mobile device's inventory.

9. Click **Save**.

   The profile is distributed to mobile devices in the scope the next time they contact the JSS.

Downloading a Mobile Device Configuration Profile

If you want to view the contents of a mobile device 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**.
4. Click the configuration profile you want to download.
5. Click **Download**.

   The profile downloads immediately.

Viewing the Status of a Mobile Device Configuration Profile

For each mobile device configuration profile, you can view the number of mobile devices for which the profile installation has a status of Completed, Remaining, or Failed.

Note: Depending on your system configuration, some historical status data may not be available for profiles installed using the Casper Suite v9.63 or earlier.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
   A list of mobile device configuration profiles is displayed.
   For each profile, you can view the number of mobile devices for which the profile installation has a Completed, Remaining, or Failed status.
   Note: If a device becomes unmanaged after a profile is successfully distributed to it, the profile will continue to be displayed in the Completed column.
4. To view a list of mobile devices for which the profile installation has a Completed, Remaining, or Failed status, click the number displayed in the corresponding column. Then click **Done**.

Viewing Logs for a Mobile Device Configuration Profile

The logs for a mobile device configuration profile include a list of mobile devices that are in the scope of the configuration profile, as well as the date/time the status was last updated and the status of the profile for each mobile device.

Note: Depending on your system configuration, some historical log data may not be available for profiles installed using v9.63 or earlier.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.

3. Click **Configuration Profiles**.
   A list of mobile device configuration profiles is displayed.

4. Click **View** next to the configuration profile you want to view logs for.
   A list of mobile devices that are in the scope of the configuration profile is displayed.

5. To view logs for a different date range, specify the starting and ending dates using the **Date Range** pop-up calendars.

6. Click **Done**.

Related Information

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

- Payload Capabilities for Mobile Device Configuration Profiles
  Learn about the payload capabilities of each iOS and tvOS version.

- Viewing the Pending Management Commands for a Mobile Device
  Find out how to view and cancel pending mobile device configuration profile installations and removals for a mobile device.

- Viewing Configuration Profiles for a Mobile Device
  Find out how to view the mobile device configuration profiles in the scope for a mobile device.

- Viewing Management History for a Mobile Device
  Find out how to view all completed, pending, and failed mobile device configuration profile installations and removals for a mobile device.

For related information, see the following Knowledge Base article:

Distributing Apps to Mobile Devices with App Store Restrictions After Upgrading to the JSS v9.5 or Later
Learn about the steps necessary to redistribute mobile device configuration profiles that contain App Store restrictions so that you can distribute apps to mobile devices with restrictions after upgrading from the JSS v9.4 or earlier.

Payload Capabilities for Mobile Device Configuration Profiles

The Casper Suite can be used to deploy mobile device configuration profiles to the following types of mobile devices:

- iPads, iPhones, or iPod touches with iOS 4 or later
- Apple TV devices with Apple TV software based on iOS 7 or later, or devices with tvOS 10.2 or later

The following table provides an overview of the payload capabilities by OS version and does not account for version-specific settings that are added to an existing payload. For detailed information on the iOS requirements for specific settings within each payload, see Apple's Configuration Profile Key Reference.

Payload	iOS 4	iOS 5	iOS 6	iOS 7	iOS 8	iOS 9	iOS 10	Apple TV with iOS 7–9[1]	tvOS 10.2
General	✓	✓	✓	✓	✓	✓	✓		✓
Passcode	✓	✓	✓	✓	✓	✓	✓		
Restrictions	✓	✓	✓	✓	✓	✓	✓		✓
Wi-Fi	✓	✓	✓	✓	✓	✓	✓	✓	✓
VPN	✓	✓	✓	✓	✓	✓	✓		
Mail	✓	✓	✓	✓	✓	✓	✓		
Exchange ActiveSync	✓	✓	✓	✓	✓	✓	✓		
Google Account						✓	✓		
LDAP	✓	✓	✓	✓	✓	✓	✓		
Calendar	✓	✓	✓	✓	✓	✓	✓		
Contacts	✓	✓	✓	✓	✓	✓	✓		
Subscribed Calendars	✓	✓	✓	✓	✓	✓	✓		
Web Clips	✓	✓	✓	✓	✓	✓	✓		
macOS Server Accounts						✓	✓		
Home Screen Layout						✓	✓		

Payload	iOS 4	iOS 5	iOS 6	iOS 7	iOS 8	iOS 9	iOS 10	Apple TV with iOS 7–9[1]	tvOS 10.2
Domains						✓	✓		
Certificate	✓	✓	✓	✓	✓	✓	✓	✓	✓
SCEP	✓	✓	✓	✓	✓	✓	✓	✓	✓
APN	✓	✓							
Cellular				✓	✓	✓	✓		
Single App Mode		✓	✓	✓	✓	✓			✓
Global HTTP Proxy				✓	✓	✓	✓	✓	✓
Single Sign-On				✓	✓	✓	✓		
Font				✓	✓	✓	✓		
AirPlay				✓	✓	✓	✓		
AirPrint				✓	✓	✓	✓		
Content Filter				✓	✓	✓	✓		
Lock Screen Message						✓	✓		
Notifications						✓	✓		
Network Usage Rules						✓	✓		
Conference Room Display[2]									✓

Notes:
1. The iOS verison is equivalent to the OS build version on which the Apple TV software is based.
2. Requires supervision.

Related Information

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

Mobile Device Configuration Profiles
Learn about mobile device configuration profiles and how to create them.

Personal Device Profiles

Personal device profiles are used to enroll personally owned iOS and Android devices with the Jamf Software Server (JSS) via user-initiated enrollment. Personal device profiles are also used to perform management tasks on personally owned devices, including defining settings and distributing managed apps to personal iOS devices.

You can create one personal device profile for each site in the JSS, and one profile for the full JSS. A personal device profile is only used to enroll and manage devices if the profile is enabled in the General payload.

The personal device profile used to enroll and manage a device is based on the site that the mobile device user has access to. Site access is determined by the LDAP directory account or JSS user account credentials entered during user-initiated enrollment. (For information on specifying the sites that LDAP user groups have access to during enrollment, see User-Initiated Enrollment Settings.)

If a profile has been enabled for the site, that profile is used to enroll the device and add the device to the site. If a profile has not been enabled for the site, or if sites have not been added to the JSS, the profile for the full JSS is used if it is enabled.

Note: Changing the site that a personal device belongs to automatically changes the profile that is used to perform management tasks on the device. If a profile has not been enabled for the new site, the device will continue to be managed by the JSS, but all settings and apps that were previously defined by the old profile are removed.

Personal Device Profile Payloads

The payloads and settings that you can configure using a personal device profile represent a subset of the iOS configuration profile payloads and settings available for institutionally owned mobile devices.

Before creating a personal device 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 personal device profile settings are unique to the JSS. For more information on these settings, see the following Knowledge Base article:

Personal Device Profile Settings Reference

Managed App Distribution to Personal iOS Devices

When creating or editing a personal device profile, you can specify managed in-house apps and App Store apps to distribute to personal iOS devices. Available apps include all managed apps that have been added to the site that the profile is assigned to, and all managed apps that have been added to the full JSS.

When a managed app is distributed to personal iOS devices, the personal device profile automatically applies settings to do the following:

- Distribute the app using the Install Automatically/Prompt Users to Install distribution method
- Remove the app when the MDM profile is removed
- Prevent backup of app data
- Prevent opening documents from managed apps in unmanaged apps

When selecting managed apps to distribute, you have the option to clone an unmanaged app and make it managed. This adds a managed version of the app to the JSS and leaves the original app unmanaged.

Note: Not all apps can be managed by the JSS. For information on the factors that determine whether an app can be managed, see Understanding Managed Apps.

Requirements

To create personal device profiles, the User-Initiated Enrollment settings must be configured to allow user-initiated enrollment for personally owned devices on the iOS or Android platform. (For more information, see User-Initiated Enrollment Settings.)

To enroll and manage personal iOS devices, you need:

- Mobile devices with iOS 4 or later (iOS 7 or later is recommended)
- A push certificate in the JSS (For more information, see Push Certificates.)

Note: To distribute managed apps to personal iOS devices, the devices must have iOS 5 or later and an MDM profile that supports managed apps. (For more information, see Managed App Requirements.)

To enroll and manage personal Android devices, you need:

- Mobile devices with Android 4.0.3 or later
- A proxy server token in the JSS (For more information, see Jamf Push Proxy.)

In addition, as part of user-initiated enrollment for personal Android devices, users need to install the Self Service Mobile app from Google Play. After enrollment, Self Service Mobile must remain installed on an enrolled Android device to keep the device managed by the JSS. (For more information, see User-Initiated Enrollment Experience for Mobile Devices.)

Note: Although not required, it is recommended that you configure the Mobile Device Inventory Collection settings to collect user and location information from LDAP. This is recommended because the mobile device name displayed in inventory for an Android device is often cryptic, making it difficult to identify a specific device. By collecting user and location information, you can search for and identify a specific Android device based on the Username field in the mobile device's inventory information.

Creating a Personal Device Profile

You can only create a personal device profile if there is an available site (or the full JSS) that does not have a profile assigned to it.

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

2. Click **Mobile Devices** at the top of the page.

3. Click **Personal Device Profiles**.

4. Click **New** ➕ .
   Note: Only one personal device profile can be created per site in the JSS. If all sites (or the full JSS) already have an assigned personal device profile, you will not be able to create a new one.

5. Use the General payload to configure basic settings for the profile, including the display name and the site to assign the profile to.
   Note: If you have site access only, the profile is assigned to the applicable site automatically and the **Site** pop-up menu is not displayed.
   To enable this personal device profile, select the **Enable personal device profile** checkbox.

6. (Optional) Use the Passcode payload to configure passcode policies.
   Note: On Android devices, the user is allowed to cancel when prompted to change their passcode to meet the configured settings. If the device passcode does not meet the configured Passcode payload settings, the **Passcode Compliance** status will be reported as Not Compliant in inventory information for the device.

7. (Optional) Use the Wi-Fi payload to configure how devices connect to your wireless network, including the necessary authentication information.

8. (Optional) Use the VPN payload to configure how devices connect to your wireless network via VPN, including the necessary authentication information.

9. (Optional) Use the Exchange ActiveSync (iOS only) payload to define settings for connecting to your Exchange server.

10. (Optional) Use the Mail (iOS only) payload to define settings for connecting to POP or IMAP accounts.

11. (Optional) Use the Calendar (iOS only) payload to define settings for configuration access to CalDAV servers.

12. (Optional) Use the Contacts (iOS only) payload to define settings for configuration access to CardDAV servers.

13. (Optional) Use the Subscribed Calendars (iOS only) payload to define settings for calendar subscriptions.

14. (Optional) Use the Certificate payload to specify the X.509 certificates (.cer, .p12, etc.) you want to install on devices to authenticate the device access to your network.

15. (Optional) Use the Security (Android only) payload to require encryption on Android devices.
    Warning: Android encryption is irreversible on most devices, and a factory reset must be performed to remove encryption from a device. In addition, failure to follow all onscreen instructions during the encryption process could lead to permanent loss of data.

16. (Optional) Select the Apps (iOS only) payload and then do any of the following:

    - To distribute a managed app to personal iOS devices added to the site (or the full JSS) that the profile is assigned to, click **Install** next to the app name. (To distribute all managed apps, click **Install All**.)

    - To remove a previously distributed managed app from devices, click **Remove** next to the app name. (To remove all managed apps previously distributed with this profile, click **Remove All**.)

- To clone an unmanaged app to add a managed version of the app to the JSS, click the unmanaged app name and then click **Clone App and Make Managed**. A managed version of the app is added to the JSS and is made available for installation.

17. (Optional) To add messaging that displays during user-initiated enrollment if the user belongs to multiple LDAP user groups with access to multiple sites, do the following:

   a. Click the **Messaging** tab, and then click **Add** + .

   b. Choose a language from the **Language** pop-up menu.

   c. Use the settings on the pane to specify the site/profile display name, as well as the text to describe the settings included with the profile. In the description for iOS devices, you can also list any managed apps that will be included with the profile.

   d. Click **Done**.

   e. Repeat this process as needed for other languages.

18. Click **Save**.

   If the profile is enabled in the General payload, it will be used to enroll personal devices with the JSS when users enter credentials for an LDAP directory account or a JSS user account that has access to the site (or to the full JSS).

Cloning, Editing, or Deleting a Personal Device Profile

Consider the following when cloning, editing, or deleting a personal device profile:

- **Cloning**—You can only clone a personal device profile if there is an available site (or the full JSS) that does not have a profile assigned to it.

- **Editing**—When a personal device profile is edited and saved, it is automatically redistributed to personal devices belonging to the site (or the full JSS) that the profile is assigned to.
  When editing an enabled profile, if you deselect the Enable personal device profile checkbox in the profile's General payload, all personal devices belonging to the site that the profile is assigned to will continue to be managed by the JSS, but all settings and apps that were previously defined by the profile are removed.

- **Deleting**—When a personal device profile is deleted, all personal devices belonging to the site that the profile is assigned to will automatically be changed to use the profile assigned to the full JSS if a profile for the full JSS is enabled. If an enabled profile for the full JSS does not exist, or if you are deleting the profile assigned to the full JSS, then the applicable devices will continue to be managed by the JSS, but all settings and apps that were previously defined by the profile are removed.
  Note: A personal device profile is automatically deleted if the site it is assigned to is deleted from the JSS.

Related Information

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

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

- User-Initiated Enrollment Settings
  Learn about the settings you can configure for user-initiated enrollment.

- User-Initiated Enrollment for Mobile Devices
  Find out how to allow users to enroll 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 mobile devices.

- Mobile Device Management Capabilities
  Learn about the management capabilities available for personally owned mobile devices.

Security Management

Remote Commands for Mobile Devices

The remote commands available in the Jamf Software Server (JSS) allow you to remotely perform tasks on a mobile device.

You can send a remote command to a single mobile device. Some commands can also be sent to multiple devices at once using mass actions. For more information, see Performing Mass Actions for Mobile Devices.

Note: The remote commands available for a particular device vary depending on the device ownership type, device platform, device type, and OS version. For more information, see Mobile Device Management Capabilities.

The following table describes the remote commands that you can send from the JSS:

Remote Command	Description	iOS Device Requirements	Personally Owned Device Support
Update Inventory	Prompts the mobile device to contact the JSS and update its inventory	--	iOS and Android
Lock Device	Locks the mobile device If the mobile device has a passcode, the user must enter it to unlock the 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.	--	iOS and Android **Note:** The lock message and phone number display options are not available on Android devices.
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.	--	N/A

Remote Command	Description	iOS Device Requirements	Personally Owned Device Support
Clear Restrictions	Removes restrictions and the restrictions passcode from a supervised mobile device	▪ iOS 8 or later ▪ Supervised	iOS
Update Passcode Lock Grace Period	Sets the amount of time that a device's screen can be locked before requiring a passcode to unlock it.	▪ iOS 9.3 or later ▪ Enrolled via a PreStage enrollment with Shared iPad enabled	N/A
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 ▪ 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 will no longer submit inventory, its inventory record remains in the JSS.	--	N/A
Wipe Device	Permanently erases all data on the device and deactivates the device. This command is available for both iOS and Apple TV devices (tvOS 10.2 or later). (Optional) Clears Activation Lock on 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.	--	N/A

Remote Command	Description	iOS Device Requirements	Personally Owned Device Support
Restart Device	Restarts a device. This command is available for both iOS and Apple TV devices (tvOS 10.2 or later). (Optional) Clears the passcode on the device. If this option is chosen, the Clear Passcode command is sent to the device before the device is restarted.	▪ iOS 10.3 or later ▪ Supervised	N/A
Send Blank Push	Sends a blank push notification, prompting the device to check in with Apple Push Notification service (APNs)	--	iOS and Android **Note:** On Android, the device checks in with Google Cloud Messaging.
Set Wallpaper	Sets an image or photo as wallpaper for the Lock screen, Home screen, or both screens on a supervised device You can upload an image file or choose an existing image file.	▪ iOS 7 or later ▪ Supervised	N/A
Enable /Disable Voice Roaming **Enable /Disable Data Roaming**	Enables/disables voice or data roaming on the device **Note:** Disabling voice roaming automatically disables data roaming.	▪ iOS 5 or later ▪ Cellular capability	N/A
Update iOS Version	Updates the iOS version on the mobile devices You can choose to download the update for users to install, or to download and install the update and restart devices after installation. **Note:** This command is only available as a mass action. For more information, see [Performing Mass Actions for Mobile Devices](#).	▪ iOS 9 or later ▪ Supervised ▪ Enrolled via a PreStage enrollment	N/A

Remote Command	Description	iOS Device Requirements	Personally Owned Device Support
Log Out User	Logs out the currently logged in user for Shared iPad only	▪ iOS 9.3 or later ▪ Supervised ▪ Enrolled via a PreStage enrollment with Shared iPad enabled	N/A
Enable /Disable Lost Mode	Enables/disables Lost Mode on the device Lost Mode locks the device and displays your custom messaging on the device's Lock screen. Global Positioning System (GPS) coordinates for the device's approximate location are also displayed in the inventory information for the device.	▪ iOS 9.3 or later ▪ Supervised	N/A
	(Optional) Always enforces Lost Mode on the device. This option ensures Lost Mode is enabled after an enrollment event has completed. When selected, Lost Mode can be only disabled in the JSS. (Optional) Plays a sound on the lost device.	▪ iOS 10.3 or later ▪ Supervised ▪ Lost Mode enabled	N/A
Update Location	Updates the GPS coordinates collected for a mobile device in Lost Mode	▪ iOS 9.3 or later ▪ Supervised ▪ Lost Mode enabled	N/A
Enable /Disable Diagnostic and Usage Reporting Enable /Disable App Analytics	Enables/disables the sending of diagnostic and usage data to Apple Enables/disables the sending of app analytics data to Apple **Note:** Disabling diagnostic and usage reporting automatically disables app analytics.	▪ iOS 9.3 or later ▪ Supervised ▪ Enrolled via a PreStage enrollment with Shared iPad enabled	N/A
Shut Down Device	Shuts down the device (Optional) Clears the passcode on the device. If this option is chosen, the Clear Passcode command is sent to the device before the device is shutdown.	▪ iOS 10.3 or later ▪ Supervised	N/A

Remote Command	Description	iOS Device Requirements	Personally Owned Device Support
Personally Owned Devices Only			
Wipe Institutional Data	Permanently erases institutional data and settings on the device On a personal iOS device, the following items are removed: - MDM profile - Personal device profile, including any institutional settings and managed apps - Device certificate On a personal Android device, the following items are removed: - MDM profile - Personal device profile, including any institutional settings **Note:** On an Android device, the Self Service Mobile app is also deactivated as a device administrator. On personal iOS and Android devices, the Wipe Institutional Data command makes the device unmanaged. This stops communication between the device and the JSS, which means you can no longer perform management tasks on the device. **Note:** Although an unmanaged device will no longer submit inventory, its inventory record remains in the JSS.	--	iOS and Android

Sending a 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 you want to send the 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.

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 Device command, enter a lock message and phone number if desired, and then click **Lock Mobile Device**.

- If you are sending a Wipe Device command, you can choose to clear the Activation Lock on the device.

- If you are sending an Enable Lost Mode command, enter the information to display on the device's Lock screen, and then click **Enable Lost Mode**.

The remote command runs on the mobile device the next time the device contacts the JSS.

Viewing the Status of 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 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 a 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 a 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 for Mobile Devices

About Self Service for Mobile Devices

Self Service allows users to browse and install iOS configuration profiles, apps, and eBooks on managed mobile devices. Users can point and tap their way through Self Service using an interface similar to the App Store.

The Jamf Software Server (JSS) allows you to manage every aspect of Self Service, including its installation, authentication, and the items available to users.

There are two kinds of Self Service for mobile devices:

- **Self Service Mobile for iOS**—You can use the JSS to group configuration profiles, apps, and eBooks in categories, which makes those items easier to locate in Self Service Mobile. (For more information, see Categories.) You can also send notifications to mobile devices with Self Service Mobile installed.
  By default, Self Service Mobile is installed on all managed mobile devices with iOS 7 or later except Apple TV devices and personally owned devices.
  Self Service Mobile is available for free from the App Store.
- **Self Service web clip**—In addition to configuration profiles, apps, and eBooks, you can use the Self Service web clip to distribute updated MDM profiles to mobile devices for users to install.

Note: If you have upgraded from the Casper Suite v9.3x or earlier, the Self Service web clip remains installed on all managed mobile devices.

Related Information

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

- Self Service Mobile
  Learn about Self Service Mobile for iOS.
- Self Service Web Clip
  Learn about the Self Service web clip.
- Installing Self Service on Mobile Devices
  Find out how to install Self Service on managed mobile devices.
- Sending a Mass Notification to Mobile Devices
  Find out how to send a mass notification to mobile devices.
- Self Service Configuration Profiles for Mobile Devices
  Find out how to make iOS configuration profiles available in Self Service.
- Self Service User Experience on Mobile Devices
  Learn how users log in and view notifications, as well as install configuration profiles, apps, and eBooks in Self Service.
- App Store Apps
  Find out how to make App Store apps available in Self Service.

- **In-House Apps**
  Find out how to make in-house apps available in Self Service.

- **eBooks Available in the iBooks Store**
  Find out how to make iBooks Store eBooks available in Self Service.

- **In-House eBooks**
  Find out how to make in-house eBooks available in Self Service.

For related information, see the following Knowledge Base article:

Creating a Link to Content in Self Service Mobile for iOS
Find out how to create a link to an app, eBook, or configuration profile in Self Service Mobile.

Installing Self Service on Mobile Devices

You can install Self Service Mobile for iOS or the Self Service web clip automatically on all managed mobile devices using the Self Service settings in the Jamf Software Server (JSS).

By default, Self Service Mobile is installed on all managed mobile devices with iOS 7 or later except Apple TV devices and personally owned devices.

Note: If you have upgraded from the Casper Suite v9.3x or earlier, the Self Service web clip remains installed on all managed mobile devices.

Installing 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 **Mobile Device Management**.

4. Click **Self Service** .

5. Click **Edit**.

6. Choose an option from the **Install Automatically** pop-up menu:

   - To install the app, choose "Self Service Mobile app".
     Note: Self Service Mobile requires mobile devices with iOS 7 or later. For earlier iOS versions, the web clip is installed by default.

   - To install the web clip, choose "Self Service web clip".

   - If you do not want to automatically install Self Service on all managed mobile devices, choose "Neither (manual installation)".
     For more information, see the Manually Deploying Self Service Mobile for iOS and Customizing the Self Service Web Clip Icon Knowledge Base articles .

7. Configure the settings on the pane.

8. Click **Save**.

   Self Service is installed on mobile devices the next time they check in with the JSS.

   If you choose to install Self Service Mobile, users are prompted to install the app from the App Store. Users are also prompted to install the app from the App Store on mobile devices as they are newly enrolled.

Related Information

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

- Self Service Mobile
  Learn about Self Service Mobile for iOS.
- Self Service Web Clip
  Learn about the Self Service web clip.

Self Service Mobile

Self Service Mobile for iOS allows you to distribute configuration profiles, apps, and eBooks to mobile devices for users to install. You can use the Jamf Software Server (JSS) to group configuration profiles, apps, and eBooks in categories, which makes those items easier to locate in Self Service Mobile. Users tap Self Service Mobile to browse and install items using an interface similar to the App Store.

In addition, you can send notifications to mobile devices with Self Service Mobile installed. (For more information, see Sending a Mass Notification to Mobile Devices. Also, see the Creating a Link to Content in Self Service Mobile for iOS Knowledge Base article.)

If iBeacon monitoring is enabled in your enviroment, Self Service Mobile is the component that detects when a mobile device enters or exits an iBeacon region.

Requirements

Self Service Mobile requires mobile devices with iOS 7 or later.

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 Self Service Mobile Settings

The Self Service settings in the JSS allow you to do the following:

- Install or uninstall Self Service Mobile on managed mobile devices.
- Require or allow users to log in to Self Service Mobile with an LDAP directory account.
- Display in-house app updates in Self Service Mobile.

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**.

4. Click **Self Service** .

5. Click **Edit**.

6. Select "Self Service Mobile app" from the **Install Automatically** pop-up menu and configure the settings on the pane.
   Note: The Self Service web clip will be installed on mobile devices with iOS 6 or earlier. (For more information, see Self Service Web Clip.)

7. (Optional) Click the **App Options** tab and configure the User Login setting.

8. Click **Save**.

   The changes are applied the next time mobile devices contact the JSS.

Related Information

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

iBeacon Regions
Learn what iBeacon regions can be used for and how you can add them to the JSS.

For related information, see the following Knowledge Base article:

Manually Deploying Self Service Mobile for iOS
Find out how to distribute Self Service Mobile to mobile devices in the scope.

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.

If you have upgraded from the Casper Suite v9.3x or earlier, the Self Service web clip remains installed on all managed mobile devices.

Note: By default, Self Service Mobile is installed on all managed mobile devices with iOS 7 or later except Apple TV devices and personally owned devices. (For more information, see Self Service Mobile.)

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 Self Service Web Clip Settings

The Self Service 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**.

4. Click **Self Service** .

5. Click **Edit**.

6. Select "Self Service web clip" from the **Install Automatically** pop-up menu and configure the settings on the pane.

7. (Optional) Click the **Web Clip Options** tab and configure the settings on the pane.

8. Click **Save**.

    The changes are applied the next time mobile devices contact the JSS.

Related Information

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.

Self Service Configuration Profiles for Mobile Devices

You can make any iOS configuration profile available in Self Service, but it is up to you to determine which profiles are appropriate.

When you make a configuration profile available in Self Service, you can specify which mobile devices display it in Self Service and which users can access it (called "scope").

You can also customize how Self Service configuration profiles are displayed to users by doing the following:

- Entering a description
- Uploading an icon
- Featuring the configuration profile
- Displaying the configuration profile in one or more categories

Creating a Self Service 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**.
4. Do one of the following:
   - To use the JSS to manually create a new configuration profile, click **New** ⊞ .
   - To upload a configuration profile (.mobileconfig) that was created using Apple's Profile Manager, click **Upload** ⬆ .

   For more information about configuration profiles, see Mobile Device Configuration Profiles.
5. On the General pane, select "Make Available in Self Service" from the **Distribution Method** pop-up menu and configure the rest of the settings as needed. You can customize the text displayed in the description for the profile in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text
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 configuration profile.
   For more information, see Scope.
8. Click the **Self Service** tab and configure how the configuration profile is displayed in Self Service using the settings on the pane.
9. Click **Save**.

   The configuration profile is displayed in Self Service on mobile devices 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:

[Installing Configuration Profiles from Self Service](#)
Learn how users install the configuration profiles available in Self Service.

Self Service User Experience on Mobile Devices

This section provides an overview of the Self Service login and notification experiences. It also describes what users do to install iOS configuration profiles, apps, and eBooks available in Self Service.

Logging in to Self Service

After opening Self Service Mobile for iOS, users may need to log in using their LDAP directory accounts. The login pane is only displayed if the User Login setting for Self Service is configured to require or allow login.

Note: This feature is also available in the Self Service web clip.

Viewing Notifications in Self Service

You can send notifications to mobile devices that have Self Service Mobile for iOS installed. (For more information, see Sending a Mass Notification to Mobile Devices. In addition, see the Creating a Link to Content in Self Service Mobile for iOS Knowledge Base article.)

Note: This feature is only supported on mobile devices with iOS 7 or later that have Self Service Mobile installed.

Notifications are displayed to users in the following ways:

- The Self Service Mobile icon displays a badge with the number of notifications that have not been viewed by the user.

- In Self Service Mobile, the **Notifications** browse button displays a badge with the number of notifications that have not been viewed by the user. Items are listed in the "Notifications" area of the app as they are added. Users can tap any item in "Notifications" to view the item.

- (Optional) Each notification can be configured to also display an alert and appear in Notification Center. Users can tap any notification to go directly to the item in Self Service Mobile.

Installing Configuration Profiles from Self Service

Users can browse configuration profiles from the "Featured" section or the list of categories in Self Service Mobile for iOS. A configuration profile is only displayed in the "Featured" section if you configured the profile to do so. (For more information, see Self Service Configuration Profiles for Mobile Devices.)

Note: This feature is also available in the Self Service web clip.

To install a configuration profile, users tap the button next to it.

Installing Apps from Self Service

Users can browse apps available from the App Store and in-house apps from the "Featured" section or the list of categories in Self Service Mobile for iOS. An app is only displayed in the "Featured" section if you configured the app to do so. (For more information, see App Store Apps and In-House Apps.)

Note: This feature is also available in the Self Service web clip.

To install an app, users tap the button next to it.

Installing Apps from Self Service

Users can browse apps available from the App Store and in-house apps from the "Featured" section or the list of categories in Self Service Mobile for iOS. An app is only displayed in the "Featured" section if you configured the app to do so. (For more information, see App Store Apps and In-House Apps.)

Note: This feature is also available in the Self Service web clip.

To install an app, users tap the button next to it.

Installing eBooks from Self Service

Users can browse eBooks available from the iBooks Store and in-house eBooks from the "Featured" section or the list of categories in Self Service Mobile for iOS. An eBook is only displayed in the "Featured" section if you configured the eBook to do so. (For more information, see eBooks Available in the iBooks Store and In-House eBooks.)

Note: This feature is also available in the Self Service web clip.

To install an eBook, users tap the button next to it.

Related Information

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

- Self Service Mobile
  Learn about Self Service Mobile for iOS.
- Self Service Web Clip
  Learn about the Self Service web clip.

VPP Content Distribution for Mobile Devices

VPP-Managed Distribution for Mobile Devices

You can distribute App Store apps and VPP store apps (including custom B2B apps) purchased through Apple's Volume Purchase Program (VPP) to mobile devices or users for VPP-managed distribution.

For more information about VPP, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Note: As an alternative to VPP-managed distribution, the JSS also supports distributing App Store apps, VPP store apps, and eBooks to mobile devices by associating redeemable VPP codes with the apps and eBooks. For more information, see VPP Code Distribution for Mobile Devices.

VPP-Managed Distribution for Mobile Devices

The JSS allows you to distribute App Store apps and VPP store apps directly to mobile devices for VPP-managed distribution. Because VPP-managed distribution for mobile devices is device-based, VPP user registration is not required and users do not need to provide an Apple ID.

The JSS can be used to automatically update apps in the JSS and on mobile devices on a schedule, and app updates can be forced at any time. Apps distributed directly to mobile devices do not appear in the user's own App Store purchase history and the apps cannot be updated by users.

VPP-managed distribution for mobile devices requires mobile devices with iOS 9 or later. To distribute App Store apps and VPP store apps to mobile devices using VPP, you need a VPP account set up in the JSS. For more information, see Integrating with VPP.

To distribute an App Store app or VPP store app directly to a mobile device, when configuring the app distribution settings, choose the VPP account that purchased the app for VPP-managed distribution. For more information, see App Store Apps.

Note: If you have apps that were distributed with user-based VPP assignments and the apps are device-assignable, you can move to device-based VPP-managed distribution for the apps. For more information, see the Moving from User- to Device-based VPP Assignments Knowledge Base article.

VPP-Managed Distribution for Users

The JSS also allows you to distribute App Store apps, VPP store apps, and eBooks to users for VPP-managed distribution. Because VPP-managed distribution for users is user-based, it involves VPP user registration and VPP user assignments. For more information, see VPP User Registration and User-Based VPP Assignments.

VPP-managed distribution for users requires mobile devices with iOS 7 or later.

Related Information

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

- Simple VPP Content Searches for Mobile Devices
  Find out how to search the VPP content in the JSS.

- VPP-Managed Distribution for Computers
  Find out how to assign content to computers for VPP-managed distribution.

VPP Code Distribution for Mobile Devices

The Jamf Software Server (JSS) allows you to distribute App Store apps, VPP store apps (including custom B2B apps), and eBooks purchased through Apple's Volume Purchase Program (VPP) to mobile devices by distributing redeemable VPP codes. When you distribute apps or eBooks using VPP codes, you can track VPP code redemption.

To distribute an app or eBook to mobile devices using VPP codes, you need an Excel spreadsheet (.xls) that contains VPP codes for the app or eBook.

For more information on VPP, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Note: As an alternative to VPP code distribution, The JSS also supports device-based VPP-managed distribution for mobile devices and user-based VPP-managed distribution for users. For more information, see VPP-Managed Distribution for Mobile Devices and User-Based VPP Assignments.

For information on distributing App Store apps and VPP store apps to mobile devices using redeemable VPP codes, see App Store Apps.

For information on distributing eBooks to mobile devices using redeemable VPP codes, see eBooks Available in the iBooks Store.

Simple VPP Content Searches for Mobile Devices

A simple VPP content search functions like a search engine, allowing you to quickly search the mobile device apps and eBooks in the Jamf Software Server (JSS) for a general range of results.

VPP content searches are based on the name of the app or eBook you are searching for.

Simple VPP content search results display the following information:

- Name of the app or eBook
- VPP account used to purchase the content
- Type of content
- Total content that has been purchased with the VPP account
- Number of apps or eBooks assigned to mobile devices, computers, or users
- Number of VPP assignments that the content is associated with

Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all content

In general, searches are not case-sensitive.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains". (For more information about configuring account preferences, see JSS User Accounts and Groups.)

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

Usage	Example
Use an asterisk after a search term to return all results with attributes that begin with that term.	Perform a search for "key*" to return all content with names that begin with "key".
Use an asterisk before a search term to return all results with attributes that end with that term.	Perform a search for "*note" to return all content with names that end with "note".
Use an asterisk before and after a search term to return all results that include that term.	Perform a search for "*ABC*" to return all content that includes "ABC".
Use an asterisk without any other terms to return all results for the item you are searching.	Perform a search for "*" to return all content.

Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform a user search for "key*, *note" to return all content that begins with "key" and ends with "note".

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a user search for "ABC*, -*note" to return all content with names that begin with "ABC" except for those that end with "note".

Returning All Content

There are two ways to return all content: use an asterisk (*) without any other characters or terms, or perform a blank search.

Performing a Simple VPP Content Search

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search VPP Content**.
4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see Search Syntax.
5. Press the Enter key.
   The list of search results is displayed.

Viewing the Mobile Devices that Content is Assigned To

You can view the mobile devices that content is assigned to.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search VPP Content**.
4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see Search Syntax.
5. Press the Enter key.
   A list of content is displayed.

6. To view the mobile devices that the content is assigned to, click the number displayed in the In Use column.
The mobile devices that have the content assigned to them are listed on the Mobile Devices pane.

Viewing the VPP Assignments that Content is Associated With

You can view the VPP assignments that content is associated with.

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

2. Click **Mobile Devices** at the top of the page.

3. Click **Search VPP Content**.

4. Enter one or more search terms in the field provided.
For information on the syntax to use to refine your search, see Search Syntax.

5. Press the Enter key.
A list of content is displayed.

6. To view the VPP assignments that the content is associated with, click the number displayed in the VPP Assignments column.

Related Information

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

- Advanced VPP Content Searches for Mobile Devices
Find out how to create and save an advanced VPP content search.

- VPP Content Reports for Mobile Devices
Find out how to export the data in your search results to different file formats.

- VPP-Managed Distribution for Mobile Devices
Find out how to assign apps to mobile devices for VPP-managed distribution.

- User-Based VPP Assignments
Find out how to assign content to users for VPP-managed distribution.

Advanced VPP Content Searches for Mobile Devices

Advanced VPP content searches allow you to use detailed search criteria to search mobile device apps and eBooks 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 VPP Content Search

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search VPP Content**.
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.
   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.

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 content is modified and meets or fails to meet the specified search criteria.

   To view the search results, click **View**.

Viewing Advanced VPP Content 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 VPP Content**.
4. Click the advanced VPP content 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:

- Simple VPP Content Searches for Mobile Devices
  Learn how to quickly search VPP content for a general range of results.

- VPP Content Reports for Mobile Devices
  Find out how to export the data in your search results to different file formats.

VPP Content Reports for Mobile Devices

The data displayed in VPP content 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

Creating VPP Content Reports

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search VPP Content**.
4. View simple or advanced VPP content search results. (For more information, see Simple VPP Content Searches for Mobile Devices or Advanced VPP Content Searches for Mobile Devices.)
5. At the bottom of the list, click **Export**.
6. Follow the onscreen instructions to export the data.

   The report downloads immediately.

App Distribution

Understanding Managed Apps

When an app is managed by the Jamf Software Server (JSS), you have more control over distribution and removal of the app, as well as the backup of app data and options for updating the app. The following table provides more detail:

	Unmanaged apps	Managed apps
Distribution Methods		
Make available in Self Service	✓	✓
Prompt users to install		✓
Removal Options		
Remove from Self Service	✓	✓
Remove from mobile devices		✓
Remove when MDM profile is removed		✓
Backup of App Data		
Prevent backup of app data		✓
App Update Options		
Schedule automatic app updates	✓	✓
Force an app update		✓
App Validation Options (in-house apps only)		
Schedule automatic app validation		✓
Force app validation		✓

Managed App Requirements

There are two factors that determine whether an app can be managed by the JSS:

- Whether users have to pay for the app
  The app must be free or paid for by the organization using Apple's Volume Purchase Program (VPP). For more information on VPP, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

- The mobile devices to which you distribute the app
  Mobile devices must have iOS 5 or later, or tvOS 10.2 or later and an MDM profile that supports managed apps.
  Mobile devices that have iOS 5 or later when they are enrolled with the JSS automatically obtain an MDM profile that supports managed apps. 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 managed apps, see the following Knowledge Base article:
  Distributing Updated MDM Profiles

If you try to make an app managed but these requirements are not met, the app behaves as unmanaged.

Understanding App Distribution Methods

The Jamf Software Server (JSS) provides two app distribution methods for iOS devices: install the app automatically/prompt users to install the app, or make the app available in Self Service.

Install Automatically/Prompt Users to Install

When you distribute an app using this method, it is managed by the JSS when possible. (For more information, see Managed App Requirements.)

To distribute an app using this method, the app must be free or paid for by the organization using Apple's Volume Purchase Program (VPP).

Free App or User-Based VPP Assignment
For free apps or apps distributed via VPP-managed distribution by assigning the app to users (user-based VPP assignment), the app is installed automatically if the following conditions are met:

- The device has iOS 7 or later.
- The device is supervised.
- The user is signed in to the iTunes Store on the device.

Users are prompted to install the app if these conditions are not met.

Device-Based VPP Assignment
For apps distributed via VPP-managed distribution by assigning the app directly to mobile devices (device-based VPP assignment), the app is installed automatically if the following conditions are met:

- The device has iOS 9 or later.
- The device is supervised.

Users are prompted to install the app if these conditions are not met.

Make Available in Self Service

When you distribute an app using this method, you can choose whether or not to make the app managed when possible. (For more information, see Managed App Requirements.)

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 Managed Apps
  Learn about managed apps and their requirements.

For related information, see the following Knowledge Base articles:

- [Distributing Apps to Mobile Devices with App Store Restrictions After Upgrading to the JSS v9.5 or Later](#)
  Learn about the steps necessary to redistribute iOS configuration profiles that contain App Store restrictions so that you can distribute apps to mobile devices with restrictions after upgrading from the JSS v9.4 or earlier.

- [Managing an App that is Currently Installed as an Unmanaged App](#)
  Learn how to convert an app from an unmanaged state to a managed state after the app has been installed on a mobile device.

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**.
4. Click **Upload** and upload the provisioning profile.
5. Enter a display name for the profile.
6. Click **Save**.

Further Considerations

- 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.

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**.
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 Mobile Device
  You can view the provisioning profiles installed on a mobile device by viewing the device's inventory information in the JSS.

- Viewing the Pending Management Commands for a Mobile Device
  Find out how to view and cancel pending provisioning profile installations and removals for a mobile device.

- Viewing Management History for a Mobile Device
  Find out how to view the completed, pending, and failed provisioning profile installations and removals for a 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 users, iOS devices, and Apple TV devices with tvOS 10.2 or later. After an 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 make the app managed. (For more information, see Understanding App Distribution Methods and Understanding Managed Apps.) Then, you specify the users and mobile devices that should receive it (called "scope").

Managed in-house apps that have been distributed to mobile devices can be validated using the app validation settings. (For more information, see In-House App Validation Settings.)

Note: To specify managed in-house apps to distribute to or remove from personally owned iOS devices, you must use the Apps payload of the personal device profile that is used to perform management tasks on the devices. For more information, see Personal Device Profiles.

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 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 user and mobile device 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
`$APPJSSID`	JSS ID of the App
`$SITEID`	Site ID
`$SITENAME`	Site Name
`$BUILDINGNAME`	Building Name
`$BUILDINGID`	Building ID
`$DEPARTMENTID`	Department ID
`$DEPARTMENTNAME`	Department Name

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, or Apple TV devices with tvOS 10.2 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**.

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.
   Note: Beginning with iOS 10.3, you can require a mobile device to have a tethered network connection to download the app. A tethered network connection requires a computer with macOS 10.12.4 or later, and must be connected to the Internet via Ethernet and have Wi-Fi turned off. Portable computers must be plugged in to a power source because the tethered caching service prevents computers from going to sleep. Select the **Require tethered network connection for app installation** checkbox. This checkbox is only displayed if "Install Automatically/Prompt Users to Install" is chosen in the **Distribution Method** pop-up menu. App updates will not require tethering; this setting is for initial installations of an app only.

7. Click the **Scope** tab and configure the scope of the app.
   For more information, see Scope.

8. (Optional, iOS only) Click the **Self Service** tab and configure the way the app is displayed in Self Service. You can customize the text displayed in the description for the app in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text
   Note: The **Self Service** tab is only displayed if "Make Available in Self Service" 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. If users were added as targets to the scope, the app is distributed to the devices those users are assigned to the next time the devices 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**.

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 user(s) or 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**.

4. Click the app you want to remove.

5. Click the **Scope** tab and remove users or 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 Mobile Device](#)
  Find out how to view the apps in the scope of a mobile device.

- [Viewing the Pending Management Commands for a Mobile Device](#)
  Find out how to view and cancel pending app installations and removals for a mobile device.

- [Viewing App Installations for a Mobile Device](#)
  Find out how to view the completed, pending, and failed app installations for a mobile device. Also, find out how to cancel pending app installations.

- [Mobile Device Configuration Profiles](#)
  You can create a mobile device 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 host in-house apps on the Tomcat instance that hosts the JSS.

In-House App Validation Settings

The Jamf Software Server (JSS) allows you to configure settings to automatically validate all managed in-house apps on mobile devices. You can use the App Validation settings in the JSS to do the following:

- **Enable Automatic App Validation**–You can enable automatic app validation for all managed in-house apps on mobile devices. This allows you to customize how frequently apps are validated.
- **Force App Validation**–You can force the JSS to immediately send app validation commands to all managed in-house apps on mobile devices.

The validation status for a managed in-house app on a mobile device is collected each time inventory information for the device is reported to the JSS, and is displayed in the inventory information for that device. If an app cannot be validated, the validation status is reported as "not validated", and the app will not open until a successful validation occurs. For information about the situations in which an app may be reported as "not validated", see the following Knowledge Base article:
Cannot Validate a Managed In-House App

Enabling Automatic App Validation

Enabling automatic app validation allows you to customize how frequently you want the JSS to attempt to validate all managed in-house apps on mobile devices. You can choose to validate apps every week, every two weeks, every four weeks, or every eight weeks. The default validation frequency is "every week".

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**.
4. Click **App Maintenance** .
5. Click the **App Validation** tab, and then click **Edit**.
6. Select **Automatically validate all managed in-house apps.**
7. To specify how often the JSS attempts to validate apps, use the **Validation Frequency** pop-up menu.
8. Click **Save**.

   Managed in-house apps are validated on mobile devices according to the selected validation frequency based on the time of day and day of the week that the setting was saved.

Forcing App Validation

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**.

4. Click **App Maintenance** .

5. Click the **App Validation** tab, and then click **Edit**.

6. Click **Force Validation**.

7. Click **Save.**

   The JSS immediately sends an app validation command to all managed in-house apps on mobile devices.

App Store Apps

The Jamf Software Server (JSS) allows you to distribute App Store apps and VPP store apps (including custom B2B apps) to users and mobile devices. After an app has been distributed, you can also use the JSS to update the app or remove the app from mobile devices.

When you distribute an App Store app or VPP store app, you add it to the JSS and configure settings for the app, such as the distribution method and whether to make the app managed. (For more information, see Understanding App Distribution Methods and Understanding Managed Apps.) Then, you specify the users and mobile devices that should receive it (called "scope").

Note: To specify managed App Store apps and VPP store apps to distribute to or remove from personally owned iOS devices, you must use the Apps (iOS only) payload of the personal device profile that is used to perform management tasks on the devices. For more information, see Personal Device Profiles.

App Store apps and VPP store apps purchased through Apple's Volume Purchase Program (VPP) can be distributed to mobile devices or users with VPP-managed distribution. For more information, see VPP-Managed Distribution for Mobile Devices and User-Based VPP Assignments.

As an alternative to VPP-managed distribution, the JSS also supports distributing App Store apps and VPP store apps using redeemable VPP codes. For more information, see VPP Code Distribution for Mobile Devices.

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 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 user and mobile device 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

Variable	Mobile Device Information
`$POSITION`	Position
`$MACADDRESS`	MAC Address
`$JSSID`	JSS ID
`$APPJSSID`	JSS ID of the App
`$SITEID`	Site ID
`$SITENAME`	Site Name
`$BUILDINGNAME`	Building Name
`$BUILDINGID`	Building ID
`$DEPARTMENTID`	Department ID
`$DEPARTMENTNAME`	Department Name

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.

Requirements

To install an App Store app, VPP store app, or update, users may be prompted to enter an Apple ID.

To distribute apps directly to mobile devices via VPP-managed distribution, you need mobile devices with iOS 9 or later.

To associate VPP codes with an App Store app or VPP 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 or VPP 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**.
4. Click **New** ➕ .
5. Select **App Store app or VPP store app** and click **Next**.
6. Do one of the following:
   - To add the app by browsing the App Store or VPP 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 and whether to make the app managed. You can also enable automatic app updates for the app. (For information, see Enabling Automatic App Updates.)
   Note: Beginning with iOS 10.3, you can require a mobile device to have a tethered network connection to download the app. A tethered network connection requires a computer with macOS 10.12.4 or later, and must be connected to the Internet via Ethernet and have Wi-Fi turned off. Portable computers must be plugged in to a power source because the tethered caching service prevents computers from going to sleep. Select the **Require tethered network connection for app installation** checkbox. This checkbox is only displayed if "Install Automatically/Prompt Users to Install" is chosen in the **Distribution Method** pop-up menu. App updates will not require tethering; this setting is for initial installations of an app only.

8. Click the **Scope** tab and configure the scope of the app.
   For more information, see Scope.

9. (Optional) Click the **Self Service** tab and configure the way the app is displayed in Self Service. You can customize the text displayed in the description for the app in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text
   Note: The **Self Service** tab is only displayed if "Make Available in Self Service" is chosen in the **Distribution Method** pop-up menu.

10. (Optional) If you want to distribute the app directly to mobile devices via VPP-managed distribution, do the following:

    a. Click the **VPP** tab, and then click the **Device Assignments** tab.

    b. Select the **Assign VPP Content** checkbox.

    c. Choose the VPP account that has purchased the app to distribute to mobile devices.

11. (Optional) If you want to associate VPP codes with the app and have not already uploaded a VPP code spreadsheet, do the following:

    a. Click the **VPP** tab, and then click the **VPP Codes** tab.

    b. Upload the Excel spreadsheet (.xls) that contains VPP codes for the app.

12. (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.

13. Click **Save**.

    The app is distributed the next time mobile devices in the scope contact the JSS. If users were added as targets to the scope, the app is distributed to the devices those users are assigned to the next time the devices contact the JSS.

Updating an App Store App or VPP Store App

The JSS allows you to update an individual App Store app or VPP store app in the following ways:

- **Enable automatic app updates**–This automatically updates the app description, icon, and version in the JSS and on mobile devices. This update happens once a day depending on the time of day you specify.

- **Force an app to update**–You can force an app to update immediately on mobile devices if there are updates available in the JSS. This update only applies to managed apps. (For more information, see Understanding Managed Apps.)

- **Distribute an app update**–You can distribute an update for an App Store app by manually updating the version number and URL for the app in the JSS. The update is distributed to mobile devices the next time they contact the JSS.

Note: The JSS also allows you to enable automatic updates for all App Store apps and VPP store apps, or force all App Store apps and VPP store apps to update immediately. For more information, see App Store App Update Settings.

Enabling Automatic App Updates

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
4. Click the app for which you want to enable automatic app updates.
5. Click **Edit**.
6. Select **Automatically update app**.
7. To select a country or region to use for syncing apps with iTunes, choose an option from the **iTunes Country or Region** pop-up menu.
8. To specify a time of day to sync apps with iTunes, set the time using the **iTunes Sync Time** pop-up menus.
9. Click **Save**.

   The app is updated in the JSS and on mobile devices in the scope based on the time you configure the app to sync with iTunes.

Forcing an 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**.
4. Click the app you want to update.

5. Click **Edit.**

6. Click **Force Update**.

7. Click **Save**.

The app is updated immediately on mobile devices in the scope if there is an update available in the JSS.

Distributing an App Store App or VPP Store 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**.

4. Click the app you want to update.

5. Click **Edit.**

6. 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.

7. Click **Save**.

The update is distributed the next time mobile devices in the scope contact the JSS.

Removing an App Store App or VPP Store App from Mobile Devices

To remove an App Store app or VPP store app from one or more devices, you remove the user(s) or 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**.

4. Click the app you want to remove.

5. Click the **Scope** tab and remove users or 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 Mobile Device**
  You can view the apps installed on a mobile device by viewing the device's inventory information in the JSS.

- **Viewing Apps for a Mobile Device**
  Find out how to view the apps in the scope of a mobile device.

- **Viewing the Pending Management Commands for a Mobile Device**
  Find out how to view and cancel pending app installations and removals for a mobile device.

- **Viewing App Installations for a Mobile Device**
  Find out how to view the completed, pending, and failed app installations for a mobile device. Also, find out how to cancel pending app installations.

- **Mobile Device Configuration Profiles**
  You can create an iOS configuration profile with a Per-App VPN connection.

For related information, see the following Knowledge Base article:

Managing an App that is Currently Installed as an Unmanaged App
Learn how to convert an app from an unmanaged state to a managed state after the app has been installed on a mobile device.

App Store App Update Settings

The Jamf Software Server (JSS) allows you to configure settings to update all App Store apps and VPP store apps (including custom B2B apps) in the JSS and on mobile devices. You can use the App Updates settings in the JSS to do the following:

- **Enable automatic app updates**–You can enable automatic app updates for all App Store apps and VPP store apps. This automatically updates app descriptions, icons, and versions in the JSS and on mobile devices. This update happens once a day depending on the time of day you specify.

- **Force apps to update**–You can force all App Store apps and VPP store apps to update immediately on mobile devices if there are updates available in the JSS. This update only applies to managed apps. (For more information, see Understanding Managed Apps.)

Note: The JSS also allows you to enable an automatic app update and force an update for an individual App Store app or VPP store app. For more information, see App Store Apps.

Enabling Automatic 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**.

4. Click **App Maintenance** .

5. On the App Updates pane, click **Edit**.

6. Select **Automatically update all App Store apps**.

7. To select a country or region to use for syncing apps with iTunes, choose an option from the **iTunes Country or Region** pop-up menu.

8. To specify a time of day to sync apps with iTunes, use the **iTunes Sync Time** pop-up menus.

9. Click **Save**.

   App Store apps and VPP store apps are updated in the JSS and on mobile devices based on the time you configure apps to sync with iTunes.

Forcing 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**.

4. Click **App Maintenance** 🖥 .

5. On the App Updates pane, click **Edit**.

6. Click **Force Updates**.

7. Click **Save.**

   Managed App Store apps and VPP store apps are updated immediately on mobile devices if there are updates available in the JSS.

Classroom Management

Apple Education Support Settings

The Apple Education Support settings allow you to enable support for Shared iPad and Apple's Classroom app. When you enable Apple Education Support, you allow iPads to be enrolled with the JSS as Shared iPad using a mobile device PreStage enrollment. In addition, Classes in the JSS can be configured for use with Apple's Classroom app.

User Images

You can enable user images as a part of Apple Education Support. When you enable user images, you allow an image or student photo to be displayed in the Classroom app and on the login screen for Shared iPads. The user image is also displayed in the inventory information for each user.

User images must be hosted on a distribution point with an enabled web server. The URL for that distribution point must be specified in the JSS when you enable user images.

When setting up the distribution point URL, it is recommended that you use a variable in the URL and name the image files so that they function with the variable you choose. For example, if the distribution point URL is https://www.mycompany.com/$USERNAME.png, the username in the JSS for each user will be inserted into the URL in place of the $USERNAME variable. If you name each image file using the username in the JSS for each user, the correct image will be displayed for each user.

You can use the following variables in the distribution point URL for user images:

- $USERNAME
- $FULLNAME
- $REALNAME
- $EMAIL
- $PHONE
- $POSITION
- $EXTENSIONATTRIBUTE_<#>

Note: Once you have specified a distribution point URL for user images, you can choose to specify a custom URL for a single user's image from the inventory information for a user. The custom URL overrides the specified distribution point URL. For more information about specifying a custom URL, see Viewing and Editing Inventory Information for a User.

For step-by-step instructions on preparing to use user images, see the following technical paper:

Integrating with Apple School Manager to Support Apple's Education Features Using the Casper Suite

Requirements

Apple Education Support only applies to supervised iPads with iOS 9.3 or later. In addition, you need a valid push certificate in the JSS. (For more information, see Push Certificates.)

To enable user images, you need:

- Images hosted on a distribution point with an enabled web server. It is recommended that you disable directory index browsing for your distribution point to ensure that the image files on the server are secure.
  Note: Although not required, it is recommended that the user images are in PNG format and are 256x256 pixels.

- A CA certificate (.pem) downloaded from the JSS is needed to establish a secure connection between the JSS and the distribution point so that the user images are populated for each user in the JSS. (For more information about CA certificates, see PKI Certificates.)

Enabling Apple Education Support

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**.

4. Click **Apple Education Support** 🔲 .

5. Click **Edit**.

6. Select the **Enable Apple Education Support** checkbox.

7. (Optional) To enable user images, do the following:

   a. Select the **Enable User Images** checkbox.

   b. Enter a distribution point URL for user images.
      Important: Editing the distribution point URL for user images causes existing EDU profiles to be redistributed. This can increase network traffic.

   c. If you have not already downloaded the CA certificate (.pem), click **Download** to download the certificate, and then save the certificate in the appropriate location dictated by your web server vendor.

   d. (Optional) If needed to establish trust between the JSS and the distribution point, upload an additional certificate (.p12 or .pem) from your web server to the JSS.

8. Click **Save**.

9. (Optional) Use the **Test** button to ensure that the user images on your distribution point are accessible.

Due to caching, user images may not appear immediately on devices. You may need to restart the device or the Classroom app in order for user images to appear.

Related Information

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

- Mobile Device PreStage Enrollments
  Find out how to enable Shared iPad when enrolling an iPad with the JSS.
- Classes
  Find out how to create Classes in the JSS for use with Apple's Classroom app.

For related information, see the following technical papers:

Supporting Apple's Classroom App and Shared iPad Using the Casper Suite
Get step-by-step instructions on how to support Shared iPad and Apple's Classroom app with the Casper Suite v9.9.

Integrating with Apple School Manager to Support Apple's Education Features Using the Casper Suite
Get step-by-step instructions on how to integrate with Apple School Manager to support Apple's education features with the Casper Suite.

Integrating with Apple School Manager

The Apple Education Support settings allow you to integrate the Jamf Software Server (JSS) with Apple School Manager. Integrating with Apple School Manager allows you to do the following:

- Specify a class naming format. This is applied to all classes imported from Apple School Manager. (For more information, see Class Naming and Description Format.)

- Specify a class description format. This is applied to all classes imported from Apple School Manager. The description is displayed in Apple's Classroom app. (For more information, see Class Naming and Description Format.)

- Sync the JSS with Apple School Manager to automatically update user and class information in the JSS at a scheduled time. You can also force the JSS to sync immediately with Apple School Manager. (For more information, see Apple School Manager Sync Time.)

- Choose user criteria for matching imported users from Apple School Manager with existing users in the JSS. Imported user information is appended to the Roster category of user inventory information for the existing user in the JSS. (For more information, see Matching Criteria for Importing Users from Apple School Manager.)

- Automatically create new users in the JSS by importing users from Apple School Manager.

- Automatically create classes in the JSS by importing classes from Apple School Manager.

Integrating the JSS with Apple School Manager creates one instance of Apple School Manager in the JSS. To integrate with Apple School Manager, you need to associate a Device Enrollment Program (DEP) instance with the Apple School Manager instance. You can associate one DEP instance with one Apple School Manager instance.

For more information about Apple School Manager, see Apple's Help documentation: https://help.apple.com/schoolmanager/

Class Naming and Description Format

When you integrate with Apple School Manager, you choose variables in the JSS that match values for class information in Apple School Manager. The JSS allows you to specify variables that apply to a class name and class description when the class is imported from Apple School Manager to the JSS. You can specify variables for the following settings:

- **Class Naming Format**—When a class is imported, the variables are applied to the display name of the class in the order you select. For example, if you select "Course Name" and "Class Source ID", the class is imported to the JSS with a name like "Biology12345".
  The default values for the class naming format are "Course Name" and "Class Source ID".

- **Class Description Format**—When a class is imported, the variables are applied to the description of the class in the order you select. For example, if you select "Location" and "Instructor", the class is imported to the JSS with a description like "EauClaireSamanthaJohnson".
  This setting overwrites existing class descriptions the next time the JSS syncs with Apple School Manager for classes that have already been imported.

The following table displays the available variables in the JSS and the values for class information that the variables match in Apple School Manager. The same variables are available for the class naming format and the class description format:

Variable in the JSS	Class Information in Apple School Manager	Notes
Location Name	Role /Location	
Class Source ID	Course ID	
Course Name	Course Name	
Class Name	Class Name	
Course Number	Course Number	
Course Source ID	N/A	Apple School Manager applies a value to a class when the class is imported to the JSS.
Class Room	Room	
Class Site	N/A	Value is populated based on the site the class is imported to in the JSS.
Instructor Name	N/A	Value is populated based on "Last Name" for the teacher that is imported with the class. If there is no value for "Last Name", this value is populated with the value for "Full Name". If there are multiple teachers in a class, the "Instructor Name" value is populated with the teacher name that comes first alphabetically by last name.
Instructor Grade	N/A	Value is populated based on "Grade" for the teacher that is imported with the class. If there are multiple teachers in a class, the "Instructor Grade" value is populated with the teacher name that comes first alphabetically by last name.
Class Number	Class Number	
Custom	N/A	In addition to variables, you can apply a custom field to the class naming format to separate variables or enter custom text. For example, if you select "Course Name", "Custom Text", and "Class Source ID", and enter a hyphen (-) in the Custom Text field, the class is imported to the JSS with a name like "Biology-12345".

Note: If a value is not available in Apple School Manager for the variable selected in the JSS, a blank value is displayed in the JSS for that selected variable in the class name.

Apple School Manager Sync Time

You can configure how frequently the JSS syncs information from Apple School Manager. Configuring a sync time allows user and class information to be updated automatically if there is updated information available in Apple School Manager. You can choose to sync never, daily, once a week, every other week, or once a month. The default sync time is "Never". In addition, you can force the JSS to sync immediately with Apple School Manager. (For more information, see Forcing an Apple School Manager Sync.)

Information is only synced from Apple School Manager to the JSS, not from the JSS to Apple School Manager.

When the configured sync time is reached or you have forced an Apple School Manager sync, inventory information in the Roster category is updated for the imported users and users associated with an imported class. Class information, such as the display name, is also updated. If you modify the class naming format after a class has been imported, the class name is updated and the class naming format is re-applied to the classes that have been imported.

Important: Any information that is manually entered in the Roster category of user inventory information is replaced with information from Apple School Manager during a sync.

If a student or teacher is added to a class in Apple School Manager after a class has been imported, the user is imported to the JSS and matched with existing users during a sync based on the criteria for matching imported users from Apple School Manager. If there is no match, the imported user is added to the JSS as a new user in the Users tab. (For more information, see Matching Criteria for Importing Users from Apple School Manager .)

If you have not yet imported users or classes from Apple School Manager when the configured sync time is reached, information is synced at the time configured and stored in the JSS database for the class or user until they are imported. (For more information, see Importing Users to the JSS from Apple School Manager and Classes.)

Note: The JSS performs one sync at a time.

Matching Criteria for Importing Users from Apple School Manager

When you integrate the JSS with Apple School Manager, you choose JSS user criteria to match with Apple School Manager user criteria. Users that are imported to the JSS are matched to existing users in the JSS based on the selected user criteria.

The following table displays the criteria you can use to match imported users from Apple School Manager to existing users in the JSS:

JSS User Criteria	Apple School Manager User Criteria
Email (JSS)	Managed Apple ID
Username (JSS)	Source System Identifier
User Extension Attributes*	

*It is recommended that you match "Source System Identifier" from Apple School Manager with the student ID number in the JSS. One way to do this is to create a user extension attribute that collects the student ID number in the JSS. (For more information on how to create a user extension attribute, see User Extension Attributes.)

The default criteria matches "Email (JSS)" with "Managed Apple ID" from Apple School Manager and an operator of "equals".

Note: Imported users from Apple School Manager cannot be matched to users with manually entered information in the Roster category of user inventory information. This results in duplicate users.

Requirements

To integrate with Apple School Manager, you need to integrate the JSS with DEP. (For more information, see Integrating with the Device Enrollment Program.)

Configuring an Instance of Apple School Manager

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**.
4. Click **Apple Education Support** 🖼 .
5. Click **Edit.**
6. Click the **Apple School Manager** tab.
7. Select the **Enable Apple School Manager Integration** checkbox.
8. Click **Add.**
   If you have not integrated the JSS with DEP, click the **Device Enrollment Program settings** link. For instructions on how to integrate with DEP, see Integrating with the Device Enrollment Program.
9. Enter a display name for the Apple School Manager instance.
10. Choose a DEP instance from the **Device Enrollment Program Instance** pop-up menu.

11. Use the **Class Naming Format** options to select a variable to apply to the name of a class when importing the class from Apple School Manager. To add more variables, click **Add** and select "Variable" or "Custom Text".
To remove a variable, click the "X" next to the variable field.

12. (Optional) Use the **Class Description Format** options to select a variable to apply to the description of a class when importing the class from Apple School Manager. To add more variables, click **Add** and select "Variable" or "Custom Text".
To remove a variable, click the "X" next to the variable field.

13. (Optional) To select a time that the JSS should sync with Apple School Manager, choose a time interval from the **Apple School Manager Sync Time** pop-up menu, and then configure the days and time to sync.
The time zone that is displayed is the time zone that is configured in System Preferences.
Note: It is recommended that you choose to sync with Apple School Manager at a time other than when you choose to flush logs or back up your database.

14. Choose criteria to use for matching imported users from Apple School Manager with existing users in the JSS using the **Matching Criteria for Importing Users** options:

    a. Select JSS or Apple School Manager user criteria from the **User Criteria** pop-up menu on the left.

    b. Choose an operator from the **Operator** pop-up menu.

    c. Select JSS or Apple School Manager user criteria from the **User Criteria** pop-up menu on the right.

15. Click **Save.**

When you import users or classes, the variables selected for the Class Naming Format are applied to the class display name, and the user information from Apple School Manager is matched to existing user information in the JSS based on the selected criteria.

The JSS updates user and class information from Apple School Manager at the time configured.

Forcing an Apple School Manager Sync

You can force the JSS to sync immediately with Apple School Manager. This allows you to update user and class information in the JSS when needed. (For more information about syncing the JSS with Apple School Manager, see Apple School Manager Sync Time.)

Note: Forcing the JSS to sync with Apple School Manager can add significant network traffic in the JSS. It is recommended that you force sync at a time other than when you choose to flush logs or back up your database.

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**.

4. Click **Apple Education Support** 📇 .
   A list of Apple School Manager instances is displayed.

5. Click the **Force Sync** button next to the Apple School Manager instance that you want to manually sync the JSS with.

   The JSS immediately syncs information from Apple School Manager.

   If you force the JSS to sync with more than one instance of Apple School Manager, the JSS performs one sync at a time.

Further Considerations

Deleting an Apple School Manager instance removes the information in the Roster category of user inventory information that is imported from Apple School Manager. This disables Shared iPad for users.
Note: Deleting an Apple School Manager instance does not remove the users or classes that have been imported from Apple School Manager.

Related Information

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

- Mobile Device PreStage Enrollments
  Find out how to enable Shared iPad when enrolling an iPad with the JSS.

- Classes
  Find out how to create Classes in the JSS for use with Apple's Classroom app.

- Apple Education Support Settings
  Find out how to enable support for Shared iPad and Apple's Classroom app.

For related information, see the following technical papers:

Integrating with Apple School Manager to Support Apple's Education Features Using the Casper Suite
Get step-by-step instructions on how to integrate with Apple School Manager to support Apple's education features with the Casper Suite.

Importing Users to the JSS from Apple School Manager

You can import users to the Jamf Software Server (JSS) from Apple School Manager. This allows you to automatically create new users in the JSS from the users in Apple School Manager or append information to existing users in the JSS.

When you import users from Apple School Manager, the following fields are populated in the Roster category of the user's inventory information:

- Last Sync
- Status
- User Number
- Full name from Roster
- First Name
- Middle Name
- Last Name
- Managed Apple ID
- Grade
- Password Policy

An assistant in the JSS guides you through the process of importing all users or a subset of users from Apple School Manager. If you choose to import a subset of users, you need to choose the criteria and values for the users you want to import. For example, you could import the students from an "Addition & Subtraction" course or an "Algebra" course only.

You can select from the following options when importing users from Apple School Manager:

- **Match to an existing user in the JSS** —Imported users are matched to existing users in the JSS based on the criteria selected when integrating the JSS with Apple School Manager. (For more information, see Integrating with Apple School Manager.) The JSS displays potential existing users in the JSS that match the specified criteria. When you select an existing user in the JSS to match the imported user to, information is populated in the Roster category of the user's inventory information. If this information existed prior to matching the imported user with the existing user, the information is updated.

- **Create a new user in the JSS** —If you choose to create a new user, the imported user is automatically added to the JSS in the Users tab and inventory information is entered in the Roster category of the user's inventory information.

Note: The number of users you can import and match varies depending on your environment. Importing a large number of users at once may affect performance. You may need to perform more than one import to import all users to the JSS from Apple School Manager.

After users are imported, if an Apple School Manager Sync Time is configured for the Apple School Manager instance, user information is updated automatically based on the scheduled frequency and time. (For more information about configuring the Apple School Manager Sync Time, see Integrating with Apple School Manager.)

Requirements

To import users to the JSS from Apple School Manager, you need the following:

- The JSS integrated with Apple School Manager. (For more information, see Integrating with Apple School Manager.)
- A JSS user account with the "Users" privilege.

Importing Users from Apple School Manager

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.

3. Click **Search Users**.

4. Leave the search field blank and press the Enter key.

5. Click **Import** ⬇ .
   If you choose to import a subset of users, choose the criteria, operator, and values to use to define the subset of users to import.
   Note: When importing a subset of users based on multiple criteria, choose "or" from the **And/Or** pop-up menu(s) if the criteria are the same.

6. Follow the onscreen instructions to import users.
   Note: If you are importing a large number of users (e.g., 10,000), a progress bar is displayed in the assistant during the import process. You can click **Done** and perform other management tasks while the import takes place.

   User information is imported to the JSS and applied in the Users tab.

   If you have site access only, users are imported to your site only.

Related Information

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

Classes
Find out how to create classes in the JSS for use with Apple's Classroom app or Casper Focus.

For related information, see the following technical paper:

Integrating with Apple School Manager to Support Apple's Education Features Using the Casper Suite
Get step-by-step instructions on how to integrate with Apple School Manager to support Apple's education features with the Casper Suite.

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, website, or attention screen. Focusing a device locks it on the app, website, or attention screen, preventing students from accessing any other screens or content on the device.

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 Self Service.

Casper Focus is available for free from the App Store.

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 7 or later

Student device:

- iPad, iPhone, or iPod touch with iOS 7 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	Supervised by Apple Configurator	--
Focus on Website	▪ Supervised by Apple Configurator ▪ Managed by the Casper Suite v9.3 or later	--
Focus on Attention Screen	▪ Supervised by Apple Configurator ▪ Managed by the Casper Suite v9.7 or later ▪ Self Service Mobile v9.7 or later installed	--
Clear Passcodes	(Minimum requirements only)	--
Mirror Device on Apple TV	▪ Supervised by Apple Configurator ▪ Managed by the Casper Suite v9.1 or later	Apple TV device with Apple TV software based on 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 Mobile or 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 iBooks 3.2 or later	--

For more information on Casper Focus features, see the Casper Focus User Guide. This guide is available at:

https://www.jamf.com/resources/resources-jamf-focus/product-documentation/

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.

- **Check Web Content Filter payload settings**—If you currently use the Web Content Filter payload in an iOS configuration profile to limit student devices to specific websites only, you need to ensure that the payload's Specific Websites list includes the URLs of any websites that teachers will focus student devices on.

- **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 Mobile Device.)

Related Information

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

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:

https://www.jamf.com/resources/resources-jamf-focus/product-documentation/

Classes

The Jamf Software Server (JSS) allows you to create classes for use with Apple's Classroom app or the Casper Focus app. When you create a class in the JSS, you use a payload-based interface to configure settings to apply to teacher and student mobile devices. These settings are then applied to the devices in a class for both Apple's Classroom app and Casper Focus.

In addition, you can use an assistant in the JSS to import classes created in Apple School Manager. You can configure the class to be used with Apple's Classroom app or the Casper Focus app. When you import a class to the JSS, you also import the users associated with the class.

Class Payloads

The payloads you choose to configure for the class depend on if you plan to use Apple's Classroom app or Casper Focus, and if your environment uses Shared iPad. The following table explains the payloads you can configure in Classes:

Payload	Description	Applies to Classroom App	Applies to Casper Focus
General	This payload allows you to enter a display name and description for a class.	✓	✓ **Note**: The description does not apply to Casper Focus.
Students	This payload allows you to add students to a class.	✓	✓
Student User Groups	This payload allows you to add student user groups to a class.	✓	✓
Teachers	This payload allows you to add teachers to a class.	✓	✓
Teacher User Groups	This payload allows you to add teacher user groups to a class.	✓	✓
Mobile Device Groups	This payload allows you to add mobile device groups to a class.	✓	✓

Payload	Description	Applies to Classroom App	Applies to Casper Focus
App Usage Restrictions	This payload allows you to restrict which apps are available to a student.	✓ Shared iPad only	
Home Screen Layout	This payload allows you to configure the layout of the Dock and the pages on the student iPad.	✓ Shared iPad only	
Apple TV	This payload allows you to assign Apple TV devices to a class for Casper Focus. 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.		✓
Meeting Times	This payload allows you to specify meeting times for a 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.		✓

Apple's Classroom App Class Configuration

When creating a class for Apple's Classroom app, you can configure settings for the following environments:

- **Environment with Shared iPad**— In this environment, you add a student user group that contains students with Managed Apple IDs to a class. You also add a mobile device group that contains Shared iPad devices. You assign the teacher to an iPad in the JSS, and then add the teacher to the class (either as an individual user or as a user group).
  In addition, you can include app usage restrictions and Home screen layout settings to customize the student experience on the iPad.

- **Environment without Shared iPad**— In this environment, you assign each student to an iPad in the JSS. Then, you add the students (either as individual users or as a user group) to a class. You assign the teacher to an iPad in the JSS, and then add the teacher to the class (either as an individual user or as a user group).

When you create a class for use with Apple's Classroom app, the JSS automatically creates an associated EDU profile that is installed on the iPads. This profile allows student and teacher iPads to communicate. It also ensures that students can log in to a Shared iPad device if Shared iPad has been enabled on the iPad.

Casper Focus Class Configuration

When creating a class for Casper Focus, you have two options for adding students, teachers, and devices to the class:

- **Users/user groups—** With this option, you assign students or teachers to devices in the JSS, and then add the students or teachers (either as individual users or as a user group) to a class.

- **Mobile device groups—** With this option, you assign students or teachers to devices in the JSS. Then, you add a smart or static mobile device group to a class that contains the devices that have the users assigned to them.
  Note: To ensure that focus actions are not applied to the teacher device in a mobile device group in Casper Focus, the JSS ID of the teacher device must be excluded from Casper Focus commands using App Configuration. (For more information, see the App Configuration Settings for Casper Focus Knowledge Base article.)

Classes Imported from Apple School Manager

You can automatically create classes in the JSS by importing classes from Apple School Manager. When you integrate with Apple School Manager, you configure a class naming format by choosing variables that are applied to the display name for all imported classes. (For more information about class naming, see Integrating with Apple School Manager.) In addition, the Students payload and Teachers payload for imported classes are automatically populated with the information imported from Apple School Manager.

An assistant in the JSS guides you through the process of importing classes from Apple School Manager. It allows you to choose the class you want to import from a list of classes in Apple School Manager. When you import a class, you also import the users associated with the class. This automatically creates new users in the JSS and appends inventory information to existing users. (For information about users imported from Apple School Manager, see Importing Users to the JSS from Apple School Manager.)

Note: If a user is added to a class in Apple School Manager after the class has been imported, the user is imported to the JSS and matched with existing users at the configured sync time based on the criteria for matching imported users from Apple School Manager. If there is no match, the imported user is added to the JSS as a new user in the Users tab. (For more information, see Matching Criteria for Importing Users from Apple School Manager.)

After a class is imported, class information is updated automatically based on the Apple School Manager Sync Time. (For more information about configuring the Apple School Manager Sync Time, see Integrating with Apple School Manager.)

Requirements

If you are creating a class to work with Apple's Classroom app, you need the following:

- Apple Education Support enabled in the JSS. (For more information, see Apple Education Support Settings.)
- Teacher assigned to an iPad in the JSS. (For more information, see User Assignments.)

In addition, you must ensure that teacher and student iPads meet the minimum device requirements for use with Apple's Classroom app. For more information about device requirements, see Apple's Classroom documentation:
https://help.apple.com/classroom/ipad

If you are configuring a class to work with Casper Focus, see Casper Focus for a list of requirements.

To import class information from Apple School Manager, you need the following:

- The JSS integrated with Apple School Manager. (For more information, see Integrating with Apple School Manager.)
- A JSS user account with the "Users" and "Classes" privileges.

Configuring 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**.

4. To create a new class, click **New** ➕ and do the following:

   a. Use the General payload to enter a display name and description for the class.
      If you specify a Class Description Format when integrating with Apple School Manager, the Description field is not editable. (For more information, see Integrating with Apple School Manager.)
      Note: The description for the class is not synced from the JSS to Apple School Manager.

   b. Add students to the class using the Students payload or the Student User Groups payload.

   c. Add teachers to the class using the Teachers payload or the Teacher User Groups payload.

5. To import class information from Apple School Manager, click **Import** ⬇ and do the following:

   a. Follow the onscreen instructions to import class information.
   Note: If you are importing a large number of classes (e.g., 10,000), a progress bar is displayed in the assistant during the import process. You can click **Done** and perform other management tasks while the import takes place.
   If you import users from Apple School Manager that match current users in the JSS, you can choose to match the imported user with the current user, or create a new user in the JSS with the information imported from Apple School Manager.

   b. Click **Done**.
   Class information is imported to the JSS, and user information is applied in the Users tab. (For more information about importing user information, see Importing Users to the JSS from Apple School Manager.)
   If you have site access only, classes are imported to your site only.

   c. Click the class you imported, and then click **Edit** to add devices and optional Shared iPad payloads to the class.

6. Add mobile device groups to the class using the Mobile Device Groups payload.

7. (Optional) If your environment uses Shared iPad, do the following:

   a. Use the App Usage Restrictions payload to restrict which apps are available to users on Shared iPad.

   b. Use the Home Screen Layout payload to configure the layout of the Dock and the pages on the iPad.

8. (Optional) If your environment uses Casper Focus, do the following:

   a. Use the Apple TV payload to add targets to assign Apple TV devices to the class.

   b. Use the Meeting Times payload to specify the times and days the class meets.

9. Click **Save**.

Further Considerations

- If you change the site of a class, mobile devices in the class are removed from the class. Users that are not already added to the new site are also removed from the class.

- Deleting a class also deletes the EDU profile from iPads in the class.

Related Information

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

- Mobile Device PreStage Enrollments
  Find out how to enable Shared iPad when enrolling an iPad with the JSS.

- About Mobile Device Groups
  You can create smart or static mobile device groups based on Shared iPad.

- About User Groups
  You can create smart or static user groups based on Managed Apple IDs.

For related information, see the following technical papers:

- [Supporting Apple's Classroom App and Shared iPad Using the Casper Suite](#)
  Get step-by-step instructions on how to support Apple's Classroom app and Shared iPad with the Casper Suite.

- [Integrating with Apple School Manager to Support Apple's Education Features Using the Casper Suite](#)
  Get step-by-step instructions on how to integrate with Apple School Manager to support Apple's education features with the Casper Suite.

Managing Users

About User Management

User management with the Casper Suite allows you to distribute the following items to users:

- Mac App Store apps
- In-house apps
- App Store apps
- In-house eBooks
- iBooks Store eBooks
- iOS configuration profiles
- macOS configuration profiles
- Policies

Inventory for Users

User Assignments

The Jamf Software Server (JSS) allows you to assign users to computers, mobile devices, and peripherals.

There are two ways to assign a user to a computer or mobile device:

- Manually (Requires the computer or mobile device to be enrolled with the JSS)
- During user-initiated enrollment

Users must be assigned to peripherals manually.

This section explains how to do the following:

- Manually assign a user to a computer, mobile device, or peripheral. (For information on assigning users to computers and mobile device during user-initiated enrollment, see User-Initiated Enrollment Settings.)
- Remove the user assignment from a computer, mobile device, or peripheral.

Manually Assigning a User to a Computer or Mobile Device

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

2. Click **Computers** or **Mobile Devices** at the top of the page.

3. Perform a simple or advanced search.
   For more information on computer searches, see Simple Computer Searches or Advanced Computer Searches.
   For more information on mobile device searches, see Simple Mobile Device Searches or Advanced Mobile Device Searches.

4. Click the computer or mobile device you want to assign a user to.

5. Select the **User and Location** category and click **Edit**.

6. Do one of the following:

   - To assign an existing user, enter the user's partial or full username in the **Username** field and click the **Search** icon. Click **Choose** across from the user you want to assign, and then click **Save**. The **Full Name**, **Email Address**, **Phone Number**, and **Position** fields are populated automatically.
   - To assign and create a new user, enter information about the user and click **Save**.

Assigning a User to 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**.

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 assign a user to.

8. Select the **User and Location** category and click **Edit**.

9. Do one of the following:

   - To assign an existing user, enter the user's partial or full username in the **Username** field and click
     the **Search** icon. Click **Choose** across from the user you want to assign, and then click **Save**.
     The **Full Name**, **Email Address**, **Phone Number**, and **Position** fields are populated automatically.

   - To assign and create a new user, enter information about the user and click **Save**.

   - If you specified user and location information, the information is applied in the **Users** tab and the
     user is assigned to the peripheral. This specified information is also applied in the inventory
     information for computers, mobile devices, and other peripherals that the user is assigned to.

Removing a User Assignment from a Computer or Mobile Device

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

2. Click **Computers** or **Mobile Devices** at the top of the page.

3. Perform a simple or advanced search.
   For more information on computer searches, see Simple Computer Searches or Advanced Computer
   Searches.
   For more information on mobile device searches, see Simple Mobile Device Searches or Advanced
   Mobile Device Searches .

4. Click the computer or mobile device you want to remove a user assignment from.

5. Select the **User and Location** category and click **Edit**.

6. Remove the username from the **Username** field and click **Save**.
   The information in the **Full Name**, **Email Address**, **Phone Number**, and **Position** fields is removed
   automatically.

Removing a User Assignment from 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**.

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 remove a user assignment from.

8. Select the **User and Location** category and click **Edit**.

9. Remove the username from the **Username** field and click **Save**.
   The information in the **Full Name**, **Email Address**, **Phone Number**, and **Position** fields is removed
   automatically.

Related Information

For related information, see the following Knowledge Base article:

Migrating Users
Find out how to migrate users using the Migration Assistant.

User Extension Attributes

User extension attributes are custom fields that you can create to collect almost any type of data about a user.

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

- Type of data being collected, such as string, integer, or date
- Input type, which determines how the extension attribute is populated with data

Note: Extension attributes are displayed in the General category of user inventory information.

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.

User Extension Attribute Input Types

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

- **Text field**—This displays a text field in user inventory information. You can enter a value in the field at any time using the JSS.
- **Pop-up menu**—This displays a pop-up menu in user inventory information. You can enter a value in the field at any time using the JSS.

Creating a User 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 **User Management**.

4. Click **Extension Attributes** 📋 .

5. Click **New** ➕ .

6. Configure the settings on the pane.

7. Click **Save**.

Related Information

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

- Viewing and Editing Inventory Information for a User
  You can view the extension attributes collected from a user and edit extension attribute values for that user.

- Smart User Groups
  You can create smart user groups based on extension attributes.

Simple User Searches

A simple user search functions like a search engine, allowing you to quickly search the users in your inventory for a general range of results.

You can base searches on any of the following attributes:

- Username
- Full name
- Email address

Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all users

In general, searches are not case-sensitive.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains". (For more information, see Configuring Account Preferences.)

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

Usage	Example
Use an asterisk after a search term to return all results with attributes that begin with that term.	Perform a search for "John*" to return all users with full names that begin with "John".
Use an asterisk before a search term to return all results with attributes that end with that term.	Perform a search for "*@mycompany.com" to return all users with email addresses that end with "@mycompany.com".
Use an asterisk before and after a search term to return all results that include that term.	Perform a search for "*Jane*" to return all users that include "Jane".
Use an asterisk without any other terms to return all results for the item you are searching.	Perform a search for "*" to return all users.

Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform a search for "John*, *Doe" to return all users that begin with "John" and end with "Doe".

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a search for "Jane*, -*@mycompany.com" to return all users with full names that begin with "Jane" except for those with email addresses that end with "@mycompany.com".

Returning All Users

There are two ways to return all users: use an asterisk (*) without any other characters or terms, or perform a blank search.

Performing a Simple User Search

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

2. Click **Users** at the top of the page.

3. Click **Search Users**.

4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see Search Syntax.

5. Press the Enter key.

   The list of search results is displayed.

Related Information

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

- Viewing and Editing Inventory Information for a User
  Find out how to view and edit inventory information for a user.

- Advanced User Searches
  Find out how to create and save an advanced user search.

Advanced User Searches

Advanced user searches allow you to use detailed search criteria to search for users 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 User Search

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Users**.
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.
   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.

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 user information is modified and users meet or fail to meet the specified search criteria.

To view the search results, click **View**.

Viewing Advanced User Search Results

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

2. Click **Users** at the top of the page.

3. Click **Search Users**.

4. Click the advanced user 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:

- Viewing and Editing Inventory Information for a User
  Find out how to view and edit inventory information for a user.

- Simple User Searches
  Learn how to quickly search users in the JSS for a general range of results.

User Reports

The data displayed in smart or static group membership lists or user 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

Creating User Reports

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Do one of the following:
   - View user group memberships. (For more information, see Smart User Groups or Static User Groups.)
   - View simple or advanced user search results. (For more information, see Simple User Searches or Advanced User Searches.)
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 Users

Mass actions allow you to perform potentially tedious tasks for multiple users at the same time. You can use the JSS to perform the following mass actions:

- Add users to a site.
- Delete users from the JSS.

Mass actions can be performed on static or smart group membership lists or user search results.

Adding Multiple Users to a Site

You can use the JSS to add multiple users to a site from static or smart group membership lists or user search results. When you add multiple users to a site, those users retain previous site memberships.

You can only add multiple users to a site if there are one or more sites in the JSS. (For more information, see Sites.)

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Do one of the following:
   - View user group memberships. (For more information, see Smart User Groups or Static User Groups.)
   - View simple or advanced user search results. (For more information, see Simple User Searches or Advanced User Searches.)
4. At the bottom of the list, click **Action**.
5. Select **Add Users to a Site**.
6. Follow the onscreen instructions to add users to a site.

Mass Deleting Users

You can mass delete users from the JSS.

If you have site access only and you mass delete users that belong to the site, the users are deleted from the full JSS (not just the site).

A user cannot be deleted from the JSS if there are dependencies for the user. For example, a user cannot be deleted if the user is assigned to a mobile device.

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Do one of the following:

- View user group memberships. (For more information, see Smart User Groups or Static User Groups.)

- View simple or advanced user search results. (For more information, see Simple User Searches or Advanced User Searches.)

4. At the bottom of the list, click **Action** .

5. Select **Delete Users**.
A list of dependencies is displayed if you cannot delete users. The number of users is displayed next to the dependency.

6. Follow the onscreen instructions to delete users.

Related Information

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

Viewing and Editing Inventory Information for a User
Find out how to edit the site for a single user.

Viewing and Editing Inventory Information for a User

The Jamf Software Server (JSS) stores detailed inventory information for each user. You can view and edit this information from the JSS.

The following table lists the information that you can view and edit for each user.

Note: Extension attributes are displayed in the General category of user inventory information.

Field	Editable	Notes
General Category		
User Image	✓ You can edit the URL for the user image by selecting the **Custom Image URL** checkbox. This allows you to overwrite the existing distribution point URL for a single user image.	Displays a user image when user images are enabled and the requirements for enabling Apple Education Support are met Shared iPad only
Username	✓	
Full Name	✓	
Email Address	✓	
Phone Number	✓	
Position	✓	
Extension Attributes	✓	
Site	✓	
Roster Category		
Last Sync		Field is not displayed if your environment is not integrated with Apple School Manager.
Status		Field is not displayed if your environment is not integrated with Apple School Manager.
User Number		Field is not displayed if your environment is not integrated with Apple School Manager.

Field	Editable	Notes
Full Name from Roster	✓ You can only edit the **Full Name from Roster** field if you create the user in the JSS. If the user is imported from Apple School Manager, this field is not editable.	
First Name	✓ You can only edit the **First Name** field if you create the user in the JSS. If the user is imported from Apple School Manager, this field is not editable.	
Middle Name	✓ You can only edit the **Middle Name** field if you create the user in the JSS. If the user is imported from Apple School Manager, this field is not editable.	
Last Name	✓ You can only edit the **Last Name** field if you create the user in the JSS. If the user is imported from Apple School Manager, this field is not editable.	
Managed Apple ID	✓ You can only edit the **Managed Apple ID** field if you create the user in the JSS. If the user is imported from Apple School Manager, this field is not editable.	Shared iPad only
Grade		Field is not displayed if your environment is not integrated with Apple School Manager.
Password Policy	✓ You can only edit the **Password Policy** field if you create the user in the JSS. If the user is imported from Apple School Manager, this field is not editable	The following options are available for the Password Policy: ▪ 4-Digit ▪ 6-Digit ▪ Standard (8 or more numbers and letters) Shared iPad only

Field	Editable	Notes
Mobile Devices Category		
		Displays a list of mobile devices that the user is assigned to
Computers Category		
		Displays a list of computers that the user is assigned to
eBooks Category		
		Displays a list of eBooks distributed to the user
Peripherals Category		
		Displays a list of peripherals that the user is assigned to, and peripherals assigned to computers that the user is assigned to
VPP Assignments Category		
		Displays a list of content assigned to the user via VPP assignments
VPP Codes Category		
		Displays a list of VPP codes redeemed by the user

Viewing Inventory Information from the Users Tab

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

2. Click **Users** at the top of the page.

3. Perform a simple or advanced user search.
   For more information, see Simple User Searches or Advanced User Searches .

4. Click the user you want to view information for.
   The user's inventory information is displayed.

5. Use the categories to view information for the user.

Editing Inventory Information from the Users Tab

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

2. Click **Users** at the top of the page.

3. Perform a simple or advanced user search.
   For more information, see Simple User Searches or Advanced User Searches.

4. Click the user you want to edit information for.
   The user's inventory information is displayed.

5. Click **Edit**.

6. Make changes as needed.
   Note: You cannot make changes to user and location information for peripherals that are assigned to a computer.

7. Click **Save**.

   Changes to a user's site are only applied in the Users tab. All other changes to a user's inventory information are applied in the Users tab and also in the inventory information for computers, mobile devices, and peripherals that the user is assigned to. (For more information on making changes to a user's site, see Sites.)

   Note: Removing a user from a site will remove the user assignment from all computers and mobile devices that belong to that site.

Related Information

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

- Viewing and Editing Inventory Information for a Computer
  Find out how to view and edit user inventory information from the inventory information for a computer that the user is assigned to.

- Viewing and Editing Inventory Information for a Mobile Device
  Find out how to view and edit user inventory information from the inventory information for a mobile device that the user is assigned to.

- Apple Education Support Settings
  Find out how to enable user images as a part of Apple Education Support.

For related information, see the following Knowledge Base article:

Redoing VPP Registration for an Unintended Apple ID
Find out how to redo the VPP registration for a user that registered with VPP using an unintended Apple ID.

Manually Adding a User to the JSS

You can manually add a user to the Jamf Software Server (JSS).

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

2. Click **Users** at the top of the page.

3. Click **Search Users**.

4. Leave the search field blank and press the Enter key.

5. Click **New** [+] .

6. Enter information about the user.

7. Click **Save**.

Related Information

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

- User Assignments
  Find out how to assign a user to a computer or mobile device in inventory.

- Importing Users to the JSS from Apple School Manager
  Find out how to create or update users in the JSS by importing users from Apple School Manager.

Deleting a User from the JSS

You can remove a user from your inventory by deleting it from the Jamf Software Server (JSS).

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search Users**.
4. Perform a search for the user you want to delete.
   For more information, see Simple User Searches.
5. Click the user.
6. Click **Delete**, and then click **Delete** again to confirm.

User Groups

About User Groups

User groups allow you to organize users that share similar attributes. You can use these groups as a basis for configuring the scope of remote management tasks.

There are two kinds of user groups: smart user groups and static user groups. Smart user groups are based on criteria and have dynamic memberships. Static user groups have fixed memberships that you manually assign.

Related Information

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

- Smart User Groups
  Find out how to create user groups that are based on criteria and have dynamic memberships.

- Static User Groups
  Find out how to create user groups that have fixed memberships.

Smart User Groups

Smart user groups give you a way to organize users based on one or more attributes, such as username, full name, and email address. These groups have dynamic memberships that are updated whenever user information is edited.

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 user group, you can view its memberships.

Creating a Smart User Group

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

2. Click **Users** at the top of the page.

3. Click **Smart User Groups**.

4. Click **New** .

5. Use the User 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 **Show Advanced 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.
      Note: Creating a smart user group with no criteria will cause all managed users to be included in the group's membership.

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.

9. Click **Save**.

   Operations in the group take place in the order they are listed (top to bottom).

   Group memberships are updated each time user information is edited.

   To view the group memberships, click **View**.

Viewing Smart User Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Smart User Groups**.
4. Click the smart user 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 section in this guide:

Scope
Find out how to configure scope based on smart user groups.

Static User Groups

Static user groups give you a way to organize users by assigning them to a group. These groups have fixed memberships that must be changed manually.

After creating a static user group, you can view its memberships.

Creating a Static User Group

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Static User Groups**.
4. Click **New** ＋ .
5. Use the User Group pane to configure basic settings for the group.
6. Click the **Assignments** tab and select the checkbox for each user you want to add.
7. Click **Save**.

   To view the group memberships, click **View**.

Viewing Static User Group Memberships

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Static User Groups**.
4. Click the user 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 section in this guide:

Scope
Find out how to configure scope based on static user groups.

VPP-Managed Distribution for Users

VPP User Registration

Before you can assign content purchased through Apple's Volume Purchase Program (VPP) to users for user-based VPP-managed distribution, users must be registered with VPP.

A user registers with VPP by accepting a VPP invitation. The following table describes the different methods you can use to distribute invitations:

Distribution Method	User Experience on macOS	User Experience on iOS	Notes
Send the invitation via email	The user clicks the URL in the email invitation and, if prompted, enters credentials for their LDAP directory account or a JSS user account. The user then connects to the App Store where they enter their Apple ID and complete the registration process.		
Prompt the user to accept the invitation and make the invitation available in Self Service for macOS	A notification appears on the user's computer prompting them to register with VPP. The user can also access the VPP invitation in Self Service for macOS. The user then connects to the App Store where they enter their Apple ID and complete the registration process.	A notification appears on the user's mobile device prompting them to register with VPP. The user then connects to the App Store where they enter their Apple ID and complete the registration process.	The user only needs to accept the VPP invitation on one device, even if the invitation is shown on multiple devices.
Make the invitation available in Self Service only	The user can access the invitation in Self Service for macOS. The user then connects to the App Store where they enter their Apple ID and complete the registration process.	The user can access the invitation in Self Service Mobile for iOS by clicking **VPP Invitations**. The user then connects to the App Store where they enter their Apple ID and complete the registration process.	The user only needs to accept the VPP invitation on one device, even if the invitation is shown on multiple devices.

Distribution Method	User Experience on macOS	User Experience on iOS	Notes
Automatically register only users with Managed Apple IDs and skip invitation	N/A	Only users that are in the scope of the invitation that have Managed Apple IDs are automatically registered with VPP. The users do not receive a VPP invitation and are not prompted to register with VPP. Users that are in the scope of the invitation that do not have Managed Apple IDs do not receive an invitation and are not registered with VPP.	To configure automatic registration options for the VPP invitation, the **Automatically Register with VPP if users have Managed Apple IDs** option must be enabled for the VPP account. (For more information, see Integrating with VPP.)

After a VPP invitation is sent, it is available in Self Service on any computer or mobile device that the user is assigned to. If the user has more than one VPP invitation, they must accept each invitation individually. If the user does not accept the VPP invitation and attempts to install an app or eBook assigned through VPP, they are prompted to accept the VPP invitation before the app or eBook is installed.

Note: The JSS also supports device-based VPP-managed distribution, which allows distributing Mac App Store apps directly to computers and App Store apps directly to mobile devices. For device-based distribution, VPP user registration is not required. For more information, see VPP-Managed Distribution for Computers and VPP-Managed Distribution for Mobile Devices.

Requirements

To register users with VPP, you need a VPP account set up in the JSS. (For more information, see Integrating with VPP.)

To send a VPP invitation via email, you need an SMTP server set up in the JSS. (For more information, see Integrating with an SMTP Server.)

If you send a VPP invitation via email and require users to log in, users must log in to a registration page with an LDAP directory account or a JSS user account. For users to log in with their LDAP directory account, you need an LDAP server set up in the JSS. (For more information, see Integrating with LDAP Directory Services.)

To send a VPP invitation by prompting users, you need:

- Computers with macOS 10.9 or later that are bound to a directory service and/or mobile devices with iOS 7.0.4 or later (For more information, see Binding to Directory Services.)

- A push certificate in the JSS (For more information, see Push Certificates.)

To configure automatic registration options for the VPP invitation, the **Automatically Register with VPP if users have Managed Apple IDs** option must be enabled on the VPP account. (For more information, see Integrating with VPP.)

Sending a VPP Invitation

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

2. Click **Users** at the top of the page.

3. Click **VPP Invitations**.

4. Click **New** + .

5. Use the General pane to configure basic settings for the invitation, including the VPP account and the method to use for sending the invitation.
   Note: The invitation is automatically added to the site that the VPP account belongs to.

6. (Optional) To automatically register users in the scope of the invitation that have Managed Apple IDs and send an invitation to the users that do not have Managed Apple IDs, select the **Automatically register with VPP if users have Managed Apple IDs** checkbox.
   Users that have Managed Apple IDs are automatically registered with VPP and do not receive an invitation or get prompted to register with VPP. Users that do not have Managed Apple IDs receive the invitation via the method selected from the **Distribution Method** pop-up menu.
   Note: This checkbox is only displayed if the **Automatically register with VPP if users have Managed Apple IDs** option is enabled for the VPP account. (For more information, see Integrating with VPP.)

7. Click the **Scope** tab and configure the scope of the invitation.
   Note: If the site of the VPP account is changed at any point, users that do not belong to that VPP account's site are removed from the scope of the invitation. For more information, see Scope.

8. Click **Save**.

A VPP invitation is immediately sent to the users you specified. You can view the status of the invitation in the list of invitations.

Viewing VPP Invitation Usage

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

2. Click **Users** at the top of the page.

3. Click **VPP Invitations**.

4. Click the invitation you want to view usage for.

5. Click **Usage**.
   Basic invitation usage information is displayed, such as the status and last action.

6. To view additional details such as the date sent and the invitation ID, click the username for that item.

Resending a VPP Invitation

The JSS allows you to resend VPP invitations to users that have not yet registered with VPP.

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **VPP Invitations**.
4. Click the invitation you want to resend.
5. Click **Resend**.

   A VPP invitation is immediately sent to users in the scope that have not yet registered with VPP.

Related Information

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

User-Based VPP Assignments
Find out how to assign content to users for VPP-managed distribution.

For related information, see the following Knowledge Base article:

Redoing VPP Registration for an Unintended Apple ID
Find out how to redo the VPP registration for a user that registered with VPP using an unintended Apple ID.

User-Based VPP Assignments

The Jamf Software Server (JSS) allows you to assign content purchased through Apple's Volume Purchase Program (VPP) to users for user-based VPP-managed distribution.

The JSS allows you to assign the following types of content to users:

- iOS apps
- Mac apps
- eBooks

After apps have been assigned to users, you can also use the JSS to revoke them from users. eBooks cannot be revoked.

When you create a VPP assignment in the JSS, you choose a VPP account, and all content purchased for VPP-managed distribution using the account is automatically available. Then you specify the content that you want to assign, and the users you want to assign it to (called "scope").

Note: The JSS also supports device-based VPP-managed distribution, which allows distributing Mac App Store apps directly to computers, as well as App Store apps and VPP store apps directly to mobile devices. For device-based distribution, VPP user assignments are not required. For more information, see VPP-Managed Distribution for Computers and VPP-Managed Distribution for Mobile Devices.

For more information on VPP and VPP-managed distribution, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Requirements

VPP user assignments require computers with macOS 10.9 or later and mobile devices with iOS 7 or later.

To assign VPP content to users, you need:

- A VPP account set up in the JSS (For more information, see Integrating with VPP.)
- Users that are registered with VPP (For more information, see VPP User Registration.)

Creating a VPP Assignment

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

2. Click **Users** at the top of the page.

3. Click **VPP Assignments**.

4. Click **New** ➕ .

5. Use the General payload to configure basic settings for the VPP assignment, including the VPP account.
   Note: The assignment is automatically added to the site that the VPP account belongs to.

6. Use the Apps and/or eBooks payload to select the checkbox for each app and/or eBook you want to assign.
   If a recently purchased app or eBook is not displayed in the list, follow the steps in the Recently Purchased Content is not Displayed in VPP Assignment Knowledge Base article to add that app or eBook to the list.

7. Click the **Scope** tab and configure the scope of the assignment.
   Note: If the site of the VPP account is changed at any point, users that do not belong to that VPP account's site are removed from the scope of the invitation. For more information, see Scope.

8. Click **Save**.

Revoking Apps from Users

To revoke specific apps from all users in the scope of a VPP assignment, you remove the apps from the VPP assignment.

To revoke all the apps in a VPP assignment from specific users, you remove the users from the scope.

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

2. Click **Users** at the top of the page.

3. Click **VPP Assignments**.

4. Click the VPP assignment you want to revoke.

5. Select the Apps payload and remove apps from the assignment as needed.

6. Click the **Scope** tab and remove users from the scope as needed.
   For more information, see Scope.

7. Click **Save**.

   If the **Notify users when an app is no longer assigned to them** checkbox is selected for the VPP account, a notification is sent to users.

Revoking All Apps from Users

For each VPP account, you can revoke all apps that have been assigned to users.

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**.

4. Click **VPP Accounts** .

5. Click the VPP account for which you want to revoke all apps.

6. Click **Revoke All** and then click **OK** to confirm.

   If the **Notify users when an app is no longer assigned to them** checkbox is selected for the VPP account, a notification is sent to users.

Viewing Content Associated with a VPP Assignment

For each VPP assignment, you can view the apps or eBooks in the App Catalog or eBook Catalog in the JSS if the content has been added to the catalog. This allows you to modify the scope of the content to redistribute it.

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

2. Click **Users** at the top of the page.

3. Click **VPP Assignments**.

4. Click a VPP assignment to view the content.

5. Select the Apps and/or eBooks payload.
   A list of content is displayed.

6. If the app or eBook has been added to the App Catalog or eBook Catalog in the JSS, click the link next to the app or eBook to view the content in the respective catalog.

   The content is displayed in the App Catalog or eBook Catalog, and you can modify the scope to redistribute the content. For information, see the following: App Store Apps, Mac App Store Apps, and eBooks Available in the iBooks Store.

Adding Content Associated with a VPP Assignment

For each VPP assignment, you can add the assigned apps and eBooks to the App Catalog or eBook Catalog in the JSS if the content has not yet been added to the catalog.

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

2. Click **Users** at the top of the page.

3. Click **VPP Assignments**.

4. Click the VPP assignment for the content you want to add to the App Catalog or eBook Catalog.

5. Select the Apps and/or eBooks payload.
   A list of content is displayed.

6. If the app or eBook has not been added to the App Catalog or eBook Catalog in the JSS, click the button next to the app or eBook to add it to the respective catalog.

   The content is displayed in the App Catalog or eBook Catalog, and you can add the content to the catalog for distribution. For information, see the following: App Store Apps, Mac App Store Apps, and eBooks Available in the iBooks Store.

Viewing the Users that VPP Content is Assigned To

For each VPP assignment, you can view the users that VPP content is assigned to.

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

2. Click **Users** at the top of the page.

3. Click **VPP Assignments**.

4. Click the VPP assignment for which you want to view the users that the content is assigned to.

5. Select the Apps and/or eBooks payload.
   A list of content is displayed.
   For each app or eBook, you can view the number of users that the content is assigned to in the In Use column.

6. To view the users that the content is assigned to, click the number displayed in the In Use column.

Simple VPP Content Searches for Users

A simple VPP content search functions like a search engine, allowing you to quickly search the mobile device apps, Mac App Store apps, and eBooks in the Jamf Software Server (JSS) for a general range of results.

VPP content searches are based on the name of the app or eBook you are searching for.

Simple VPP content search results display the following information:

- Name of the app or eBook
- VPP account used to purchase the content
- Type of content
- Total content that has been purchased with the VPP account
- Number of apps or eBooks assigned to computers, mobile devices, or users
- Number of VPP assignments that the content is associated with

Search Syntax

This section explains the syntax to use for the following search functions:

- Wildcard searches
- Including multiple search terms
- Excluding a search term
- Returning all content

In general, searches are not case-sensitive.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains". (For more information about configuring account preferences, see JSS User Accounts and Groups.)

Wildcard Searches

Asterisks (*) function as wildcard characters in simple searches. The following table explains the different ways asterisks can be used to refine a search:

Usage	Example
Use an asterisk after a search term to return all results with attributes that begin with that term.	Perform a search for "key*" to return all content with names that begin with "key".
Use an asterisk before a search term to return all results with attributes that end with that term.	Perform a search for "*note" to return all content with names that end with "note".
Use an asterisk before and after a search term to return all results that include that term.	Perform a search for "*ABC*" to return all content that includes "ABC".

Usage	Example
Use an asterisk without any other terms to return all results for the item you are searching.	Perform a search for "*" to return all content.

Including Multiple Search Terms

Use multiple search terms separated by a comma (,) to return all results that include those search terms.

For example, perform a user search for "key*, *note" to return all content that begins with "key" and ends with "note".

Excluding a Search Term

Use a hyphen (-) before a search term to exclude results that include the term.

For example, perform a user search for "ABC*, -*note" to return all content with names that begin with "ABC" except for those that end with "note".

Returning All Content

There are two ways to return all content: use an asterisk (*) without any other characters or terms, or perform a blank search.

Performing a Simple VPP Content Search

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search VPP Content**.
4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see <u>Search Syntax</u>.
5. Press the Enter key.
   The list of search results is displayed.

Viewing the Users that Content is Assigned To

You can view the users that content is assigned to.

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search VPP Content**.
4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see <u>Search Syntax</u>.

5. Press the Enter key.
   A list of content is displayed.

6. To view the users that the content is assigned to, click the number displayed in the In Use column.
   The users that have the content assigned to them are listed on the Users pane.

Viewing the VPP Assignments that Content is Associated With

You can view the VPP assignments that content is associated with.

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

2. Click **Users** at the top of the page.

3. Click **Search VPP Content**.

4. Enter one or more search terms in the field provided.
   For information on the syntax to use to refine your search, see Search Syntax.

5. Press the Enter key.
   A list of content is displayed.

6. To view the VPP assignments that the content is associated with, click the number displayed in the VPP Assignments column.

Related Information

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

- Advanced VPP Content Searches for Users
  Find out how to create and save an advanced VPP content search.

- VPP Content Reports for Users
  Find out how to export the data in your search results to different file formats.

- User-Based VPP Assignments
  Find out how to assign content to users for VPP-managed distribution.

- VPP-Managed Distribution for Computers
  Find out how to assign apps to computers for VPP-managed distribution.

- VPP-Managed Distribution for Mobile Devices
  Find out how to assign apps to mobile devices for VPP-managed distribution.

Advanced VPP Content Searches for Users

Advanced VPP content searches allow you to use detailed search criteria to search mobile device apps, Mac App Store apps, and eBooks 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 VPP Content Search

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search VPP Content**.
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.
   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.

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 content is modified and meets or fails to meet the specified search criteria.

To view the search results, click **View**.

Viewing Advanced VPP Content Search Results

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search VPP Content**.
4. Click the advanced VPP content 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:

- Simple VPP Content Searches for Users
  Learn how to quickly search VPP content for a general range of results.
- VPP Content Reports for Users
  Find out how to export the data in your search results to different file formats.

VPP Content Reports for Users

The data displayed in VPP content 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

Creating VPP Content Reports

1. Log in to the JSS with a web browser.
2. Click **Users** at the top of the page.
3. Click **Search VPP Content**.
4. View simple or advanced VPP content search results. (For more information, see Simple VPP Content Searches for Users or Advanced VPP Content Searches for Users.)
5. At the bottom of the list, click **Export**.
6. Follow the onscreen instructions to export the data.

   The report downloads immediately.

eBook Distribution

Understanding Managed eBooks

The Jamf Software Server (JSS) allows you to manage eBooks that are distributed to iOS devices. When an eBook is managed by the JSS, you have more control over distribution and removal of the eBook. The following table provides more detail:

	Unmanaged eBooks (iOS and macOS)	Managed eBooks (iOS only)
Distribution Methods		
Make available in Self Service	✓	✓
Install automatically/prompt users to install		✓
Removal Options		
Remove from Self Service	✓	✓
Remove in-house eBooks from mobile devices		✓
Remove from computers		
Remove in-house eBooks when MDM profile is removed		✓

Managed eBook Requirements

The following requirements determine whether an eBook can be managed by the JSS:

- The device has iOS 8 or later
- The eBook is an in-house eBook, or an eBook available in the iBooks Store that is free or paid for by the organization using Apple's Volume Purchase Program (VPP) and assigned to the user via VPP-managed distribution (For information, see User-Based VPP Assignments.)

If you try to make an eBook managed and these requirements are not met, the eBook behaves as unmanaged.

Understanding eBook Distribution Methods

The Jamf Software Server (JSS) provides two eBook distribution methods: install the eBook automatically/prompt users to install the eBook (iOS only), or make the eBook available in Self Service.

Install Automatically/Prompt Users to Install

When managed eBook requirements are met, the eBook is installed on iOS devices and users can view it with Apple's iBooks app. If managed eBook requirements are not met, the eBook will be made available in Self Service for users to install. (For more information, see Managed eBook Requirements.)

The eBook is installed automatically if the following conditions are met:

- The device has iOS 8 or later.
- The device is supervised.
  Note: For more information on supervision, see Apple's documentation at:
  http://help.apple.com/configurator/mac
- The user is signed in to the iTunes Store on the device.
- The iBooks Store has not been disabled on the device.
- The device is not configured to require an Apple ID password for all purchases.
- If the eBook wasn't assigned to the user for VPP-managed distribution, the user has recently authorized an iTunes Store purchase on the device, or the user's Apple ID has previously been used to install the eBook.

If these conditions are not met, users are prompted to install the eBook.

Note: If a user is in the scope for an eBook, the eBook will be installed automatically on all iOS devices that the user is assigned to in the JSS if managed eBook requirements are met. On other iOS devices that do not meet managed eBook requirements or computers assigned to the same user, the eBook will be made available in Self Service.

Make Available in Self Service

When you distribute an eBook using this method, it is made available in Self Service for users to install. You can choose whether or not to make the eBook managed when possible. (For more information, see Managed eBook Requirements.)

Related Information

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

- Understanding Managed eBooks
  Learn about managed eBooks and their requirements.

- In-House eBooks
  Find out how to distribute in-house eBooks.

- eBooks Available in the iBooks Store
  Find out how to distribute eBooks available in the iBooks Store.

In-House eBooks

In-house eBooks are eBooks that are not available from the iBooks Store. The Jamf Software Server (JSS) allows you to distribute in-house eBooks to computers, mobile devices, and users. The JSS provides two distribution methods for in-house eBooks: install the eBook automatically/prompt users to install the eBook (iOS only), or make the eBook available in Self Service. After an eBook is installed, users 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 computers, mobile devices, and users that should receive it (called "scope").

Note: In-house eBooks cannot be distributed to personally owned mobile devices.

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

To install an ePub file, you need:

- A mobile device with iOS 4 or later and iBooks 1.0 or later
- A computer with macOS 10.7 or later and an application to view eBooks

To install an iBooks file, you need:

- An iPad with iOS 5 or later and iBooks 2.0 or later
- A computer with macOS 10.9 or later and iBooks 1.0 or later

Distributing an In-House eBook

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

2. Click **Computers**, **Mobile Devices**, or **Users** at the top of the page.

3. Click **eBooks**.

4. Click **New** ➕ .

5. Select **In-house eBook** and click **Next**.

6. Use the General pane to configure settings for the eBook, including the display name and distribution method.
   Note: If you choose "Make Available in Self Service" as the distribution method, the **Make eBook managed when possible** checkbox is selected by default. However, in-house eBooks distributed to computers cannot be managed. For more information, see Managed eBook Requirements.
   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. (Optional) Click the **Self Service** tab and configure the way the eBook is displayed in Self Service. You can customize the text displayed in the description for the eBook in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text
   Note: The **Self Service** tab is only displayed if "Make Available in Self Service" is chosen in the **Distribution Method** pop-up menu.

9. Click **Save**.

   For eBooks set to the "Install Automatically" distribution method, eBooks are installed the next time mobile devices in the scope check in with the JSS. Users can view installed eBooks with Apple's iBooks app.

   For eBooks set to the "Make Available in Self Service" distribution method and eBooks that cannot be installed automatically, eBooks are available in Self Service for users to install the next time Self Service is launched.

Removing a Managed In-House eBook from Mobile Devices

To remove a managed in-house eBook 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 **Computers**, **Mobile Devices**, or **Users** at the top of the page.

3. Click **eBooks**.

4. Click the eBook 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 eBook is removed the next time the mobile devices check in with the JSS.

Related Information

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

- [eBooks Available in the iBooks Store](#)
  Find out how to distribute eBooks available in the iBooks Store.

- [Viewing eBooks for a Computer](#)
  Find out how to view the eBooks in the scope of a computer.

- [Viewing eBooks for a Mobile Device](#)
  Find out how to view the eBooks in the scope of a mobile device.

- [Viewing the Pending Management Commands for a Mobile Device](#)
  Find out how to view and cancel pending eBook installations and removals for a 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 host in-house eBooks on the Tomcat instance that hosts the JSS.

eBooks Available in the iBooks Store

The Jamf Software Server (JSS) allows you to distribute eBooks that are available in the iBooks Store to computers, mobile devices, and users. The JSS provides two distribution methods for iBooks Store eBooks: install the eBook automatically/prompt users to install the eBook (iOS only), or make the eBook available in Self Service. After an eBook is installed, users can view it using Apple's iBooks app.

When you distribute an eBook available in the iBooks Store, you add it to the JSS and configure settings for the eBook. Then, you specify the computers, mobile devices, and users 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:

https://www.jamf.com/resources/resources-jamf-focus/product-documentation/

Note: eBooks available in the iBooks Store cannot be distributed to personally owned mobile devices.

VPP Codes

When you distribute an eBook available in the iBooks Store, you can also associate Volume Purchase Program (VPP) codes with the eBook and track their redemption.

Note: The JSS also supports VPP-managed distribution, which involves VPP assignments instead of VPP codes. For more information, see User-Based VPP Assignments.

For more information on VPP, visit one of the following websites:

- Apple Deployment Programs Help
  https://help.apple.com/deployment/business/
- Volume Purchase Program for Business
  https://www.apple.com/business/vpp/
- Apple School Manager Help
  https://help.apple.com/schoolmanager/

Requirements

To distribute an eBook available in the iBooks Store, the eBook must be an ePub file (.epub) or iBooks file (.ibooks).

To install an ePub file, you need:

- A mobile device with iOS 4 or later and iBooks 1.0 or later
- A computer with macOS 10.9 or later and an application to view eBooks

To install an iBooks file, you need:

- An iPad with iOS 5 or later and iBooks 2.0 or later

- A computer with macOS 10.9 or later and iBooks 1.0 or later

Distributing an iBooks Store eBook

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

2. Click **Computers**, **Mobile Devices**, or **Users** at the top of the page.

3. Click **eBooks**.

4. Click **New** [+] .

5. Select **eBook available in the iBooks Store** and click **Next**.

6. Do one of the following:

   - To add the eBook by browsing the iBooks Store, enter the name of the eBook, choose an iBooks Store 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 settings for the eBook, including the display name and distribution method.

8. Click the **Scope** tab and configure the scope of the eBook.
   For more information, see Scope.

9. (Optional) Click the **Self Service** tab and configure the way the eBook is displayed in Self Service. You can customize the text displayed in the description for the eBook in Self Service by using Markdown in the Description field.
   For information about Markdown, see the following Knowledge Base article:
   Using Markdown to Format Text

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**.

    For eBooks set to the "Install Automatically" distribution method, eBooks are installed the next time mobile devices in the scope check in with the JSS. Users can view installed eBooks with Apple's iBooks app.

    For eBooks set to the "Make Available in Self Service" distribution method and eBooks that cannot be installed automatically, eBooks are available in Self Service for users to install the next time Self Service is launched.

    The eBook is available for users to install the next time Self Service is launched.

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 Computer
  Find out how to view the eBooks in the scope of a computer.

- Viewing eBooks for a Mobile Device
  Find out how to view the eBooks in the scope of a mobile device.

- Viewing the Pending Management Commands for a Mobile Device
  Find out how to view and cancel pending eBook installations and removals for a mobile device.