



# Casper Suite Release Notes

Version 9.63

■ JAMF Software, LLC

© 2014 JAMF Software, LLC. All rights reserved.

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

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

Apache Tomcat and Tomcat are trademarks of the Apache Software Foundation.

Apple, the Apple logo, and Mac OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

Composer, the Composer logo, JAMF Software, the JAMF Software logo, Recon, and the Recon logo are trademarks of JAMF Software, LLC, registered in the U.S. and other countries.

Intel is a registered trademark of the Intel Corporation in the U.S. and other countries.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

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

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

# Contents

<b>4</b>	<b>What's New in This Release</b>
<b>5</b>	<b>Backward Compatibility</b>
<b>6</b>	<b>Installation</b>
6	Preparing to Upgrade
6	Functionality Changes and Other Considerations
8	Upgrading the JSS
11	Upgrading the JSS Host Server to OS X Server v10.10
<b>12</b>	<b>Deprecations and Removals</b>
<b>13</b>	<b>Bug Fixes and Enhancements</b>
13	Casper Admin
13	Casper Imaging
13	Casper Remote
13	jamf binary
14	JAMF Distribution Server
14	JAMF Software Server
16	JSS Database Utility
16	Self Service Mobile
16	Self Service for OS X
<b>17</b>	<b>Known Issues</b>

# What's New in This Release

- **Additional support for iOS configuration profiles**—Support for the “IKEv2” connection type has been added to the VPN payload.
- **FileVault 2-authenticated restart**—An authenticated restart can now be performed on computers with FileVault 2 enabled.

For a complete list of bug fixes and enhancements, see the [Bug Fixes and Enhancements](#) section.

To view a complete list of the feature requests implemented in v9.63, go to:

<https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=100>

**Note:** New privileges associated with new features in the Casper Suite are disabled by default.

# Backward Compatibility

The following versions of the client applications are compatible with this version of the JSS:

- Casper Admin v9.4 or later
- Casper Imaging v8.6 or later
- Casper Remote v9.2 or later
- Recon v9.2 or later

Any version of Casper Focus, Composer, and Self Service Mobile are compatible.

To take full advantage of new features, bug fixes, and enhancements, use the most current version of the JSS and the client applications.

# Installation

## Preparing to Upgrade

To ensure the upgrade goes as smoothly as possible, review the best practices, tips, and considerations explained in the following Knowledge Base articles:

- [Preparing to Upgrade the JSS](#)—Explains the best practices for evaluating and preparing for an upgrade.
- [Upgrading a JSS Hosted on Windows](#)—Provides preparation tips and step-by-step instructions for upgrading a JSS hosted on a Windows server.
- [Upgrading the JSS in a Clustered Environment](#)—Provides step-by-step instructions for upgrading the JSS in a clustered environment.

## Functionality Changes and Other Considerations

Depending on the version you are upgrading from, changes made to the Casper Suite since your last upgrade could impact your current environment setup or workflows.

The following table explains key changes and additions to the Casper Suite, the versions in which they were implemented, and where to get more information.

Starting with...	Change or Consideration	Description	Additional Resources
v9.51	Modified support for OS X v10.5 and v10.6	Features implemented in the Casper Suite v9.51 or later are no longer supported on computers with OS X v10.5 and v10.6. Workflows implemented prior to v9.51 will continue to function, but they may require earlier versions of the client applications.	"Requirements" section in the <i>Casper Suite Administrator's Guide</i>
v9.5	App distribution allowed with App Store restrictions enabled	Apps can be distributed to mobile devices with iOS 7 or later even when the App Store is restricted on those devices. To do this, you must redistribute iOS configuration profiles that have the <b>Allow installing apps</b> checkbox deselected in the Restrictions payload.	<a href="#">Distributing Apps to Mobile Devices with App Store Restrictions After Upgrading to the JSS v9.5 or Later</a>

Starting with...	Change or Consideration	Description	Additional Resources
v9.3	User management and VPP integration	The JSS can be configured to integrate with VPP, and users can be managed from the <b>Users</b> tab in the JSS.  To take advantage of this functionality, you must first complete the user migration process.	<a href="#">Migrating Users</a>
v9.21	Distribution of signed iOS configuration profiles from Apple	Signed iOS configuration profiles from Apple can be uploaded to the JSS and distributed.	<a href="#">Distributing a Signed Configuration Profile from Apple</a>
v9.1	Enrollment profile requirements for iOS 7 or later	Enrollment profiles created using the Casper Suite v9.0 or earlier cannot be used to enroll mobile devices with iOS 7 or later.  If you plan to enroll devices with iOS 7 or later, create a new enrollment profile using the Casper Suite v9.1 or later.  <b>Note:</b> Mobile devices enrolled with the Casper Suite v9.0 or earlier using an enrollment profile do not need to be re-enrolled when upgraded to iOS 7.	"Enrollment Profiles" section in the <i>Casper Suite Administrator's Guide</i>
v9.0	Deprecation of support for custom reports	Custom reports are no longer supported and are not migrated during an upgrade from v8.x.	N/A
v9.0	Loss of certain of Managed Preferences	Due to a change in the way that Managed Preferences work in v9.x, two types of Managed Preferences are lost when upgrading from v8.x.	<a href="#">Managed Preferences and Upgrading to the v9.0 or Later</a>
v9.0	Deprecation of support for smart groups with certain criteria	The JSS no longer supports smart groups that contain "Version" and "Title" criteria listed in that order. It is recommended that you switch the order to "Title"–"Version" before upgrading from v8.x.	<a href="#">Switching the Order of Smart Group Criteria</a>
v9.0	API improvements	Earlier versions of the JSS API returned inconsistent values, making it difficult to compare values and maintain consistency. Several changes have been made to improve this.	<a href="#">Improvements in the JSS API v9.0</a>

Starting with...	Change or Consideration	Description	Additional Resources
v8.72	Deprecation of enrollment profiles downloaded from v8.71 or earlier	Enrollment profiles downloaded from the Casper Suite v8.71 or earlier cannot be used to enroll mobile devices with v8.72 or later.  Re-download any enrollment profiles that were downloaded with v8.71 or earlier. Use the newly downloaded versions to enroll mobile devices with v8.72 or later.	N/A
v8.3	MDM profile distribution required for app management on certain devices	An MDM profile that supports app management must be distributed via the Self Service web clip to managed iOS 4 devices that are upgraded to iOS 5 or later.	<a href="#">Distributing Updated MDM Profiles</a>
v8.3	Recommended enablement of certificated-based authentication	If you are upgrading the Casper Suite v8.2x or earlier, it is recommended that you enable certificate-based authentication. Doing so ensures that device certificates on OS X computers are valid.	<a href="#">Certificate-Based Authentication for OS X Computers</a>

## Upgrading the JSS

This section explains how to upgrade the JSS using the JSS Installers. If the JSS host server does not meet the JSS Installer requirements, you can install the JSS manually using the instructions in the [“Manually Installing the JAMF Software Server”](#) technical paper.

### Installed Components

The following components are installed on the JSS host server by the JSS Installer:

- JSS web application
- JSS Database Utility
- Apache Tomcat
  - To find out which version of Tomcat will be installed, see the [Apache Tomcat Version Installed by the JSS Installer](#) Knowledge Base article.

### JSS Installer Requirements

#### JSS Installer for Mac

To use the JSS Installer for Mac, you need a Mac computer with:

- A 64-bit capable Intel processor
- 2 GB of RAM



- 400 MB of disk space available
- OS X Server v10.7 or later
- Server.app (recommended)
- Java 1.6 or 1.7
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7  
You can download the JCE from:  
<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:  
<https://www.mysql.com/downloads/>
- Ports 8443 and 9006 available

### **JSS Installer for Linux**

To use the JSS Installer for Linux, you need a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- One of the following operating systems:
  - Ubuntu 12.04 LTS Server (64-bit)
  - Ubuntu 14.04 LTS Server (64-bit)
  - Red Hat Enterprise Linux (RHEL) 6.4 or later
- Open Java Development Kit (OpenJDK) 6 or 7  
For more information, go to <http://openjdk.java.net/>.
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:  
<https://www.mysql.com/downloads/>
- Ports 8443 and 8080 available

### **JSS Installer for Windows**

To use the JSS Installer for Windows, you need a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- Windows Server 2008 R2 (64-bit) or Windows Server 2012 (64-bit)
- Java SE Development Kit (JDK) 1.6 or 1.7 for Windows x64  
You can download the JDK from:  
<http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html>

- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7  
You can download the JCE from:  
<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:  
<https://www.mysql.com/downloads/>
- Ports 8443 and 8080 available

## Upgrading the JSS from v8.x to v9.x

In addition to the functionality changes explained in the [Functionality Changes and Other Considerations](#) section, there are a few things to be aware of regarding the upgrade process from v8.x to v9.x.

### Time to Upgrade

The amount of time it takes to upgrade the JSS has increased due to the number of changes and improvements in the JSS v9.x. The amount of time it takes depends on the size of the database and the number of features that are utilized.

In general, it is recommended that you upgrade the JSS during non-business hours.

### Upgrade Failures

If an upgrade fails, do not downgrade. Contact JAMF Software Support.

### Upgrading from v8.64 or Earlier

When upgrading from v8.64 or earlier, first upgrade to v8.73.

1. Upgrade the JSS to v8.73.
2. Ensure that the upgrade was successful.
3. Back up the database.
4. Upgrade to v9.x. See the [Upgrading the JSS](#) section.

### Rescheduling Database Backups

If database backups were scheduled using the JSS Database Utility v8.2, it is recommended that you reschedule them using the JSS Database Utility from the target version.

For more information, see the JSS installation and configuration guide for the appropriate platform.

## Upgrading the JSS

Use the following instructions to upgrade a JSS hosted on Mac or Linux. To upgrade a JSS hosted on Windows, see the [Upgrading a JSS Hosted on Windows](#) Knowledge Base article.

1. Back up the current database using the JSS Database Utility.
2. Copy the most current version of the JSS Installer for your platform to the server.
3. Double-click the installer and follow the onscreen instructions to complete the upgrade.

## Upgrading the JSS Host Server to OS X Server v10.10

This section explains how to upgrade the JSS host server from OS X Server v10.9 to v10.10.

1. Back up the current database.
2. Upgrade to OS X v10.10.
3. Install Java 1.7 and JCE 1.7.  
For instructions, see the [Installing Java and MySQL](#) Knowledge Base article.
4. Follow the instructions for upgrading the JSS.

# Deprecations and Removals

There are no deprecations or removals in this release.

# Bug Fixes and Enhancements

## Casper Admin

- [D-007344] Fixed an issue that caused the JSS to attempt to log in twice when invalid LDAP directory account credentials were used to log in to the JSS or client applications.
- [D-007861] Fixed an issue that caused Casper Admin to crash while analyzing a package when the **Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4** option is selected and Casper Admin is running on OS X v10.10.
- [D-007910] Fixed an issue that prevented Casper Admin from renaming a package on a JDS instance that is set as the master distribution point.

## Casper Imaging

- [D-007098] Fixed an issue that prevented a JSS user with full JSS access from changing the site a computer belongs to when imaging that computer with Casper Imaging. This issue only occurred when the computer belonged to a different site than the last site the user viewed the JSS. It also caused imaging to fail.
- [D-007213] If the **Computer Name** field in Casper Imaging is left blank, Casper Imaging now assigns the computer name that is configured in the image to the target computer.
- [D-008138] Fixed an issue that sometimes prevented Casper Remote, Casper Imaging, and Recon from authenticating to a JSS running on CentOS.

## Casper Remote

- [D-005309] The logs in the Casper Remote application now display HTTP file download paths for packages.
- [D-008019] Fixed an issue that prevented Casper Remote from displaying the `InstallESD.dmg` file for OS X v10.10 on the **Packages** tab.

## jamf binary

- [D-005170] Fixed an issue that caused the jamf binary to display sensitive information in the process list if the jamf binary is running on OS X v10.9 or later.
- [D-007095] Fixed an issue that could cause the jamf binary to submit blank Application Usage logs to the JSS, causing logs that are at least one day old to be overwritten with blank data.

## JAMF Distribution Server

- [D-006730] Fixed an issue that prevented a JDS instance from being enrolled in an environment that uses a non-standard network configuration.

## JAMF Software Server

- [D-005954] Policies configured to download packages from a file share distribution point over HTTP now attempt to run again if the network connection is lost and regained within five minutes.
- [D-006369] Policies triggered on Enrollment Complete that only require the OS X name and version can now run on newly enrolled computers that were enrolled using the -noRecon command.
- [D-006458] The JSS no longer allows the meeting time for a class to have an end time that is earlier than the start time.
- [D-006633] Fixed an issue that caused the JSS to incorrectly display a **Version** search field when performing a simple search for computers or mobile devices if an advanced search has been saved and sites have been configured in the JSS.
- [D-006820] Fixed an issue that prevented the JSS Dashboard from displaying the correct number of OS X computers that have run a policy successfully if a smart computer group was included in the scope of the policy.
- [D-006890] Fixed an issue that caused the JSS to display only the first 100 Computer Usage log entries for a computer.
- [D-006898] Fixed an issue that prevented the JSS from exporting a complete list of smart computer group memberships as a .csv or a .txt file if the export is based on computers and certain criteria was present in the smart group.
- [D-006915] Fixed an issue that caused the JSS to display an incorrect number of results when performing a simple computer search by application or application usage and viewing the results by department.
- [D-007021] Fixed an issue that caused a JSS in a clustered environment to fail to delete group membership data for a device in the scope of a deleted smart group when the device updates inventory information before the JSS web application syncs.
- [D-007048] Fixed an issue that caused the JSS to mount the master and the failover distribution point when a policy is used to run a script or deploy a package and the script or package has not been migrated.
- [D-007110] Fixed an issue that caused the JSS to remove serial numbers from the scope of an Imaging PreStage after the JSS is upgraded from v8.x to v9.x.
- [D-007317] Fixed an option in the **Method** pop-up menu for a VPP invitation to accurately reflect the devices on which users are prompted.
- [D-007477] The JDS Installer now displays a warning message when a user attempts to install a non-root JDS instance.
- [D-007605] Fixed an issue that prevented the JSS from reporting the enrollment method in the inventory information for a mobile device. This caused the JSS to incorrectly calculate advanced search results and smart group memberships based on "Enrollment Method" criteria.

- [D-007675] Fixed an issue that caused the JSS to incorrectly display "Install App – App no longer exists" in the list of completed commands for a mobile device after Self Service Mobile for iOS was installed automatically.
- [D-007925] Fixed an issue that caused the JSS to incorrectly display the criteria "Enrollment Method: User-initiated - no invitation" for a smart computer group.
- [D-007950] Binding computers to a directory service no longer fails if there are more than 127 directory bindings in the JSS.
- [D-007986] Fixed an issue that prevented the JSS from retaining the settings configured in the VPN payload of an iOS configuration profile created using Apple's Profile Manager if the payload was configured to have an IKEv2 connection type.
- [D-008003] Fixed an issue that caused the enrollment failure message and the **Try Again** button to display the word "null" when a personally owned device running iOS 6 or later fails to enroll.
- [D-008034] Fixed an issue that caused the jamf agent to crash when attempting to enforce a software restriction. This allowed time for the restricted software to be opened.
- [D-008055] Fixed an issue that could cause the jamf binary to display multiple pop-up messages on a computer when an application that has a restricted process name is opened.
- [D-008062] Fixed an issue that caused the JSS to refresh instead of returning to the All Users pane after the **Done** button is clicked when manually adding a user to the JSS.
- [D-008067] Fixed an issue that could cause smart user groups to return all users if criteria for the group are added and removed in a single editing session and the connector "or" is used.
- [D-008093] Fixed an issue that prevented smart group memberships from automatically recalculating after the criteria for the smart group was changed using the JSS API.
- [D-008131] Fixed an issue that caused the JSS to create duplicate users if the **Save** button is clicked multiple times when manually assigning a user to a computer or mobile device.
- [D-008141] Fixed an issue that prevented the JSS from collecting computer inventory information after the JSS is upgraded from v8.x to v9.x.
- [D-008154] The JSS API now displays site information for licensed software records and allows the GET, PUT, POST, and DELETE methods to be used on that information.
- [D-008157] Fixed an issue that caused the JSS to remove all Identification settings from an uploaded OS X configuration profile with an Identification payload.
- [D-008162] Fixed an issue that prevented queries for Self Service configuration profiles from returning more than one category when returned as a JSON response.
- [D-008168] Fixed an issue that caused the JSS to display OS X configuration profiles that are assigned to a category under the "no category assigned" heading.
- [D-008176] Fixed an issue that prevented JSS user accounts that belong to a JSS user group and have custom privileges for Casper Imaging, Casper Remote, or Recon from opening and using those applications.
- [D-008180] The JSS API now allows the PUT action to be used for an API object with a category of "None".
- [D-008188] Fixed an issue that prevented a configuration profile with the FileVault Recovery Key Redirection payload from saving correctly if the **Recovery Key Redirection** setting is changed from automatic to manual and **JSS Built-In Signing Certificate** is selected.

## JSS Database Utility

- [D-007759] The JSS Database Utility now displays a warning message stating that a database backup cannot be fully restored if it is created with the **Omit encryption key from backups** option selected.
- [D-008030] Fixed an issue that caused an error message to display when successfully creating a database backup using the JSS Database Utility with Java 1.6.

## Self Service Mobile

[D-007921] Web clips installed via a configuration profile now display a default icon until they are opened for the first time if an icon has not been uploaded.

## Self Service for OS X

- [D-006883] Self Service for OS X now displays an accurate error message when a user attempts to download a file from within a URL plug-in.
- [D-007406] Self Service for OS X now displays a failure message when a policy fails to run.
- [D-007564] Fixed an issue that prevented Self Service policies configured to require an ethernet network connection from displaying in Self Service if users are not required to log in.
- [D-007815] Fixed an issue that prevented Self Service for OS X from being opened when a user is logged into the computer with their Active Directory (AD) credentials and their username contains a space.
- [D-008196] Fixed an issue that prevented Self Service for OS X from being signed.



# Known Issues

This release includes the following known issues:

- When users try to access the Self Service web clip on a mobile device with iOS 7.0.1 or 7.0.2, Self Service opens in Safari instead of as a web clip.
- eBooks and unmanaged apps cannot be installed from the Self Service web clip on iOS 7 devices until the Self Service web clip is updated for iOS 7. For more information, see the following Knowledge Base article:  
[Updating the Self Service Web Clip for iOS 7](#)
- Management account passwords configured using the network scanner in Recon v9.01-9.11 are not saved correctly in the JSS if they contain an “at” symbol (@). This prevents management tasks from being performed on the affected computers. For more information, see the following Knowledge Base article:  
[Casper Remote Error: An Incorrect Username/Password is Entered for this Computer](#)
- [D-004197] Printers mapped using an OS X configuration profile are not displayed in “Print and Scan” in System Preferences unless the **Allow printers that connect directly to user’s computer** checkbox is selected in the configuration profile.
- [D-004198] OS X configuration profiles that are configured to display a heading on the login window fail to do so.
- [D-004382] Tapping the URL in an email enrollment invitation on an iOS 6 device draws a blank page. Users should copy-and-paste the URL into the Safari app instead.
- [D-005532] OS X configuration profiles with a Login Window payload that is configured to deny users and groups the ability to log in fail to do so.
- [D-005736] The **Require password after sleep or screen saver begins** and **Allow user to set lock message** settings in the Security & Privacy payload of an OS X configuration profile are not applied.
- [D-005750] An iOS configuration profile with a Restrictions payload that has Media Content settings configured causes the **Require Password** option to be set to “Immediately” on a mobile device that was originally set to “15 minutes”.
- [D-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of an OS X configuration profile is not applied at login.
- [D-005900] The JSS fails to install configuration profiles with a Web Clip payload on computers with OS X v10.9.
- [D-006026] The JSS fails to restrict Game Center when the **Allow use of Game Center** checkbox is deselected in the Restrictions payload in OS X configuration profiles.
- [D-006058] User-level OS X configuration profiles with widget restrictions fail to restrict widgets.
- [D-006250] A customized Self Service web clip icon uploaded using the JSS will revert to the default Casper Suite icon on iOS 7 devices.
- [D-006266] Policies running during the DarkWake state of Power Nap fail if DarkWake is terminated before the policy finishes running.
- [D-006393] The **Start screen saver after** option in a Login Window payload of an OS X configuration profile is not applied on computers with OS X v10.8.4 or v10.8.5.
- [D-006627] When restarting a computer that has been imaged using Casper Imaging, the computer fails to enroll if attempting to connect to the JSS via an Apple Thunderbolt to Ethernet Adapter.

- [D-006662] Installed OS X configuration profiles that include a VPN payload with the **Use Hybrid Authentication** checkbox selected append “[hybrid]” to the group name in the VPN authentication settings on the computer, which causes group authentication to fail.
- [D-006758] iOS configuration profiles with a Single App Mode payload fail to require a passcode on supervised iOS 7 devices when the devices have a passcode and are locked.
- [D-006793] Computer-level OS X configuration profiles that define options for Time Machine backups fail to do so.
- [D-007004] iOS configuration profiles with a cookies restriction fail to set the specified restriction and hide other cookies restrictions on the device. The restrictions that are hidden depend on the restriction specified in the profile.
- [D-007087] Mobile devices fail to enroll properly using a PreStage enrollment when they are powered off from the Login page after being restored to an iCloud backup.
- [D-007163] Casper Focus sometimes incorrectly removes the focus from a student device if the home button on the student device is pressed while the device is being focused.
- [D-007206] Attempting to install Self Service Mobile for iOS on an enrolled mobile device when the Self Service web clip is open causes the device to lock on the web clip. This prevents the user from accessing any other screens or content on the device.  
Workaround: Change the **Install Automatically** option to **Self Service web clip**.
- [D-007245] The configuration page fails to display correctly when enrolling a mobile device via PreStage enrollment.
- [D-007386] Mobile devices fail to enroll using a PreStage enrollment if an LDAP user has **User must change password at next logon** selected in Active Directory.
- [D-007508] Apps assigned to users for VPP-managed distribution sometimes fail to install completely on mobile devices that have Automatic Downloads enabled.
- [D-007511] If the option to skip the Restore page is selected for a PreStage enrollment in the JSS, the Restore page is not skipped during enrollment if the enrollment process is restarted during the Setup Assistant.
- [D-007537] Location Services are incorrectly disabled when the **Allow modifying Find My Friends settings (Supervised devices only)** checkbox is deselected in the Restrictions payload of an iOS configuration profile.
- [D-007628] iOS configuration profiles made available in Self Service cannot be removed manually from mobile devices with iOS 8 even when the profiles are configured to allow removal.  
Workaround: Remove the mobile device from the scope of the profile.
- [D-007638] An in-house eBook set to the **Install Automatically** distribution method will display as “Untitled” until it is opened on a mobile device.
- [D-007721] iOS configuration profiles with a Mail payload configured to log in to the app using a specified password fail to require a password after the configuration profile has been removed and redistributed to require a password on mobile devices with iOS 6.
- [D-007823] Policies configured to require users to enable FileVault 2 in a disk encryption payload fail to do so on a computer with OS X v10.10.
- [D-007825] OS X configuration profiles with a Software Update payload configured to allow installation of OS X beta releases fail to make OS X beta releases available to users.
- [D-007860] When the User value in the Exchange payload of an OS X configuration profile is an email address, an OS X Mail app user cannot authenticate and access their email on OS X v10.10 computers.

- [D-007898] If a PreStage enrollment is configured with the **Make MDM Profile Mandatory** checkbox selected and a user skips the Wi-Fi configuration step during the OS X Setup Assistant process, the computer will not be enrolled with the JSS.
- [D-007989] MySQL Server fails to start automatically on a computer running OS X v10.10 when “Automatically Start MySQL Server on Startup” is selected.
- [D-007999] Screen saver settings in a configuration profile that is removed and re-applied to a computer are not retained.
- [D-008152] End users are incorrectly prompted for an Airplay password when attempting to Airplay to a device for which an AirPlay password has been specified using an OS X configuration profile.
- [D-008167] When multiple Casper Suite disk images are mounted, the JSS Installer installs the version of the Casper Suite included in the disk image that was mounted first.
- [D-008255] On computers with OS X v10.9 or v10.10, configuration profiles that enforce an alphanumeric password intermittently prevent new passwords from being set.
- [D-008286] When VMware Fusion is closed on a client computer, the computer loses its connection with the JSS.
- [D-008306] On a computer with multiple FileVault 2 users where the originally-assigned FileVault 2 user has been disabled, a kernel panic occurs when one of the enabled users logs in after a reboot.