



Casper Suite Release Notes

Version 9.8

JAMF Software, LLC
© 2015 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.

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

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

Contents

4 What's New in This Release

6 Backward Compatibility

7 Installation

7 Preparing to Upgrade

7 Functionality Changes and Other Considerations

10 Upgrading the JSS

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

14 Deprecations and Removals

15 Bug Fixes and Enhancements

15 Casper Focus

15 Casper Imaging

15 Documentation

15 jamf.exe

16 JAMF Software Server

17 JSS Database Utility

17 JSS Installer for Windows

17 Recon.exe

17 Self Service for iOS

18 Known Issues

What's New in This Release

- **Global Service Exchange (GSX) enhancements**—The JSS now supports certificate-based authentication for GSX.
- **New location for jamf binary**—The jamf binary is now located in `/usr/local/jamf/bin/jamf`. (The previous location was `/usr/sbin/jamf`.) The location is updated automatically during the upgrade to v9.8. Action is required if existing packages, scripts, or extension attributes reference the previous location of the binary. For detailed information, see the [Functionality Changes and Other Considerations](#) section.
- **Volume Purchase Program (VPP) enhancements**—You can now specify that all content purchased with a VPP account is populated in the app and eBook catalogs.
- **PreStage Enrollment enhancements:**
 - Mobile device PreStage enrollments can now be configured to skip the Zoom and Android Migration steps in Apple's Setup Assistant.
 - Computer PreStage enrollments can now be configured to skip the FileVault step in Apple's Setup Assistant.
 - You can now require users to authenticate during computer setup using an LDAP directory account or a JSS user account.
 - You can now specify that computers and mobile devices newly associated with a DEP instance be automatically added to the PreStage enrollment.
- **JSS API enhancement**—It is no longer necessary to create an XML file to pass parameter values to a computer or mobile device command. Parameter values can now be specified as part of the command. For detailed information about each computer or mobile device command, see the JSS REST API Resource Documentation.
- **User Management enhancements:**
 - Individual users, smart user groups, and static user groups can now be included in the scope of an OS X configuration profile or a policy.
 - A new execution frequency has been added for policies: Once per user per computer
- **TLS 1.2 requirement**—OS X v10.9 and later now use TLS 1.2 to communicate with the JSS based on the latest Apple security requirements.
- **Support for iOS 9**—Mobile devices with iOS 9 can be enrolled and managed with the Casper Suite. Also, new settings for iOS 9 are included in the Restrictions payload for configuration profiles.

- **Limited support for OS X v10.11**—The following basic management functions work with OS X v10.11:
 - User-initiated enrollment
 - Enrollment using a PreStage enrollment
 - Inventory
 - Deployment of configuration profiles
 - Automatic deployment of Self Service
 - Self Service policies

Full support for OS X v10.11 will be available in a future version of the Casper Suite.

For a complete list of deprecations, removals, bug fixes, and enhancements, see the [Deprecations and Removals](#) and the [Bug Fixes and Enhancements](#) sections.

To view a complete list of the feature requests implemented in v9.8, go to: <https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=116>

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 the JSS in a Clustered Environment](#)—Provides step-by-step instructions for upgrading the JSS in a clustered environment.

It is also recommended that you review the [Functionality Changes and Other Considerations](#) section to determine if changes made to the Casper Suite since your last upgrade could impact your environment or require you to take action.

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
v9.8	New location for jamf binary	<p>The jamf binary is automatically moved from <code>/usr/sbin/jamf</code> to its new location, <code>/usr/local/jamf/bin/jamf</code>, during an upgrade to the Casper Suite v9.8.</p> <p>During the upgrade, the database is scanned for packages, scripts, and extension attributes that reference the previous location of the binary. If items are found, notifications are displayed in the JSS after the upgrade is complete. These items need to be modified to reference the new location of the binary, which can be done in the JSS by clicking the notifications.</p> <p>Items that are not stored in the database and reference the previous location of the binary need to be modified to reference the new location.</p>	N/A

Starting with...	Change or Consideration	Description	Additional Resources
v9.73	Recommended update of encryption ciphers for HTTPS connections	If you are upgrading the Casper Suite v9.72 or earlier, you must update the list of encryption ciphers for HTTPS connections in order to remediate a known security vulnerability.	Configuring Supported Ciphers for Tomcat HTTPS Connections
v9.7	Wildcard character changes for smart groups	The JSS v9.7 or later no longer recognizes the percent sign (%) as a wildcard character for smart group criteria. The percent sign is now recognized as a literal character. Remove the percent sign from the smart group criteria and change the operator to "like" to ensure that smart group memberships are calculated correctly.	N/A
v9.7	Application deletion limitation in restricted software	An application can be deleted only if using the Restrict exact process name option. If you edit a restricted software record created using the Casper Suite v9.66 or earlier, the Restrict exact process name checkbox will be selected automatically if the Delete application option is enabled. This could cause the existing restricted software record to behave differently. For example, any wildcard character (*) used in the Process Name field will function as a literal character.	N/A
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 Allow installing apps checkbox deselected in the Restrictions payload.	Distributing Apps to Mobile Devices with App Store Restrictions After Upgrading to the JSS v9.5 or Later

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 Users tab in the JSS. To take advantage of this functionality, you must first complete the user migration process.	Migrating Users
v9.21	Distribution of signed iOS configuration profiles from Apple	Signed iOS configuration profiles from Apple can be uploaded to the JSS and distributed.	Distributing a Signed Configuration Profile from Apple
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. Note: 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.	Managed Preferences and Upgrading to the JSS v9.0 or Later
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.	Switching the Order of Smart Group Criteria
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.	Improvements in the JSS API v9.0

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.	Distributing Updated MDM Profiles
v8.3	Recommended enablement of certificate-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.	Certificate-Based Authentication for OS X Computers

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 v10.7 or later
- OS X Server (recommended)
- Java SE Development Kit (JDK) 1.7 or 1.8 for Mac OS X
You can download the JDK from:
<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.7 or 1.8
You can download the JCE from:
<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.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) 7 or 8
For installation information, go to <http://openjdk.java.net/install/>.
- 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), Windows Server 2012 (64-bit), or Windows Server 2012 R2 (64-bit)
- Java SE Development Kit (JDK) 1.7 or 1.8 for Windows x64
You can download the JDK from:
<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.7 or 1.8
You can download the JCE from:
<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.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 changes explained in the [Functionality Changes and Other Considerations](#) section, there are a few things to be aware of when upgrading 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 "Upgrading the JSS" in the [JSS Installation and Configuration Guide for Windows](#).

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 1.8 and JCE 1.8.
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 in this release.

The following functionality has been removed:

- **Support for Java 1.6 and Tomcat 6**—Support for Java 1.6 and Tomcat 6 has been removed. It is recommended that you start using a later version of Java and Tomcat. If you need assistance or have questions, contact your Technical Account Manager.
- **Removing a device from the Device Enrollment Program (DEP) using the JSS**—Devices can no longer be removed from DEP using the JSS v9.8 or later. To remove a device from DEP, you must use the Apple Deployment Programs website, available at: <https://deploy.apple.com/>

Bug Fixes and Enhancements

Casper Focus

[D-009374] Fixed an issue that caused text strings to incorrectly display in place of the French or German text in command feedback messages when Casper Focus is displayed in French or German.

Casper Imaging

- [D-008518] Imaging a computer with an Imaging PreStage that contains nested smart configurations no longer leaves the computer unmanaged.
- [D-008789] Fixed an issue that prevented Casper Imaging from imaging a computer when using a JSS user account with a password that contains a plus (+).

Documentation

- [D-007554] The *Casper Suite Administrator's Guide* has been updated to no longer include login hooks in the "Requirements" section for OS X configuration profiles.
- [D-007643] The "In-House Apps" section in the *Casper Suite Administrator's Guide* has been updated to no longer state that in-house apps can be cloned.
- [D-008358] The "Upgrading the JSS" section in the *JSS Installation and Configuration Guide for Windows* has been updated to include step-by-step instructions for upgrading the JSS.
- [D-008667] The "About Distribution Points" section in the *Casper Suite Administrator's Guide* has been updated to include information on selective replication for cloud distribution points and JDS instances.
- [D-008876] The **Include hidden systems account** checkbox is now displayed as **Include hidden accounts** in the JSS web interface.
- [D-009124] The "Integrating with VPP" section in the *Casper Suite Administrator's Guide* has been updated to include the operating system requirements for VPP integration.
- [D-009147] The "Configuring a Computer PreStage Enrollment" section in the *Casper Suite Administrator's Guide* has been updated to no longer include incorrect information about the **Authentication** checkbox.
- [D-009415] The *Casper Focus User Guide* has been updated to no longer state that focus actions are never performed on a teacher device, even if the device is included in a class.

jamf.exe

[D-008274] Fixed an issue that prevented jamf.exe v8.x or earlier from submitting the user and location information for a computer when connecting with the JSS v9.x or later.

JAMF Software Server

- [D-006743] When editing the user and location information for a computer, mobile device, or peripheral, a search in the Username field now searches with a wildcard at both the beginning and the end of the search term for manually added user accounts.
- [D-007017] Fixed an issue that caused the JSS to allow duplicate user objects to be created.
- [D-007135] Fixed an issue that caused the JSS to sometimes display an error and fail to install OS X configuration profiles on multiple computers after imaging a computer that was already enrolled with the JSS.
- [D-007857] Fixed an issue that caused the JSS to unnecessarily recalculate smart user group memberships when verifying the content for VPP-managed distribution.
- [D-007893] Fixed an issue that prevented the JSS from downloading a PreStage enrollment QuickAdd package if the **Allow MDM Profile Removal** option was deselected.
- [D-008082] Fixed an issue that prevented the local account password in the System keychain from being reset when the password for a FileVault 2-enabled user was changed using the jamf binary.
- [D-008327] Fixed an issue that caused Casper Focus and Self Service to fail to correctly display icons for some apps.
- [D-008386] In a clustered environment, the JSS no longer fails to remove non-master JSS web applications from the Limited Access list after the non-master JSS web application is removed from the cluster.
- [D-008560] Fixed an issue that caused a configuration profile set to log a user out after a certain amount of time to fail to do so.
- [D-008696] The JSS no longer continuously deploys configuration profiles with bad payloads to computers with OS X v10.9.
- [D-008699] Including quotation marks in a command executed using the Files and Processes payload of a policy no longer causes the policy or any subsequent policies to fail.
- [D-008714] Fixed an issue that prevented a JSS user from creating an advanced mobile device search when the JSS user account was configured to include the Create privilege for “Advanced Mobile Device Searches”.
- [D-008824] Fixed an issue that prevented the JSS API from updating the name of a mobile device.
- [D-008875] MD5 password hashes are no longer available through the JSS API.
- [D-008939] Fixed an issue that caused the JSS to sometimes fail to distribute managed in-house app updates to personally owned iOS devices.
- [D-009028] Performing a GET command using the JSS API on an advanced user search now returns the correct number of mobile devices or computers associated with a user.
- [D-009085] Fixed an issue that caused OS X configuration profiles to be continuously reinstalled if a blank or “No Name” username exists in the JSS.
- [D-009089] Fixed an issue that prevented apps set to install automatically from being reinstalled when a mobile device is re-enrolled.
- [D-009130] The JSS now only recalculates smart groups for which the site or attributes have changed when a computer or mobile device checks in with the JSS.
- [D-009156] Fixed an issue that caused the JSS API to fail to unassign peripherals from a computer.

- [D-009353] The JSS now displays a **VPP code** tab for paid eBooks.
- [D-009362] Fixed an issue that prevented an App Store restriction from being correctly applied to a mobile device.
- [D-009375] Fixed an issue that caused the JSS to fail to save an iOS configuration profile with a Custom SSL connection type configured in the VPN payload.
- [D-009430] Fixed an issue that prevented a licensed software record from being deleted.
- [D-009432] In a clustered environment, the JSS no longer installs, removes, and then reinstalls iOS apps configured with a scope based on user groups.
- [D-009507] Additional variable options have been added to managed app configuration settings and OS X and iOS configuration profile payloads.
- Fixed an issue that caused hidden inputs to display in the JSS web interface.
- Fixed an issue that prevented a management account password from being saved correctly if the management account was specified during user-initiated enrollment.

JSS Database Utility

[D-008638] The **Omit encryption key from backups** option in the JSS Database Utility is now only available for manual backups.

JSS Installer for Windows

[D-009350] The JSS Installer for Windows no longer fails if the `JAVA_HOME` environment variable is not set.

Recon.exe

[D-008995] Fixed an issue that prevented Recon.exe from submitting inventory for a computer if an external drive was connected to the computer.

Self Service for iOS

[D-008036] Fixed an issue that caused an incorrect message to be displayed on a mobile device when an end user attempts to reinstall a managed in-house eBook before it has completely installed.

Known Issues

The following issues are a result of bugs in third-party software. Defects have been filed for these bugs and are awaiting resolution.

- 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 [Updating the Self Service Web Clip for iOS 7](#) Knowledge Base article.
- 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 [Casper Remote Error: An Incorrect Username/Password is Entered for this Computer](#) Knowledge Base article.
- [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-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-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-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-006979] When enrolling a computer using a QuickAdd package, the QuickAdd installer incorrectly prompts users for local administrator credentials twice if the **Restrict re-enrollment to authorized users only** checkbox is selected.
- [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-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.
- [D-007245] The configuration page fails to display correctly when enrolling a mobile device via PreStage enrollment.
- [D-007486] SMB shares sometimes fail to mount on a computer with OS X v10.9.
- [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-007969] Compiled configurations created with Casper Admin using the `InstalledESD.dmg` file for OS X v10.10 fail to create a “Recovery HD” partition when the configuration is used to image computers.
- [D-007999] Screen saver settings in a configuration profile that is removed and re-applied to a computer are not retained.

- [D-008018] The JSS cannot connect to an Open Directory server hosted on OS X Server v10.10 using CRAM-MD5 authentication.
- [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-008212] If a mobile device is enrolled using a PreStage enrollment and is then re-added to the server token file (.p7m), the device becomes unassigned and the JSS incorrectly displays the device as still being in the scope of the PreStage enrollment.
- [D-008286] When VMware Fusion is closed on a client computer, the computer loses its connection with the JSS.
- [D-008309] A guest user is able to log in from the FileVault 2 login window when a configuration profile was used to disallow guest users and FileVault 2 is configured for the current or next user.
- [D-008484] iOS configuration profiles with a large number of permitted URLs added to the Content Filter payload fail to upload to the JSS.
- [D-008567] When a student device with iOS 8 is focused on a website, multiple icons with the website link are displayed.
- [D-008603] OS X configuration profiles with a Restrictions payload disable the widgets in the OS X v10.10 Notification Center.
- [D-008623] The JSS sometimes fails to display the correct model for a computer.
- [D-008688] OS X configuration profiles that include a Network payload configured with 802.1X authentication and the Auto Join checkbox selected fail to automatically connect a computer to the network after the computer leaves sleep mode.
- [D-008806] The `dsconfigad` binary fails to bind a computer to a directory service if the service account password contains an exclamation point (!).
- [D-008905] An OS X configuration profile with a Passcode payload does not enforce the required alphanumeric value or the maximum number of failed attempts allowed for a computer with OS X v10.10 or later.
- [D-008912] The **User names and passwords** checkbox in the Safari AutoFill options cannot be deselected when the **Allow Safari AutoFill** option is selected in the Restrictions payload of an OS X configuration profile.
- [D-009091] When the Safari "Accept Cookies" pop-up menu is set to "Always" for an iOS configuration profile, the setting is not applied on mobile devices with iOS 8.3.
- [D-009110] Configuration profiles with the "Internal Disks: Allow" option disabled do not prevent the use of memory cards.
- [D-009443] Casper Focus fails to focus a student device with iOS 7 on the attention screen if the device was being focused on an app or website.
- [D-009450] An OS X configuration profile with a Password payload incorrectly enforces a number of complex characters equal to the last value used.