Casper Suite Release Notes

Version 9.73

JAMF software

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

Contents

What's New in This Release

- **Volume Purchase Program (VPP) enhancements**:
  - VPP assignments can now be edited from the JSS API.
  - The JSS now displays a warning message when content purchased through VPP is in use and cannot be assigned to users.
- **Cloud distribution point enhancements:**
  - The JSS now supports the use of signed URLs created with Amazon CloudFront.
  - The JSS now supports the use of Akamai Remote Authentication.
- Individual users, smart user groups, and static user groups can now be included in the scope of an iOS configuration profile.
- **Mobile devices with iOS 6 or earlier no longer supported in Casper Focus—** Casper Focus no longer supports student and teacher devices with iOS 6 or earlier. Student and teacher devices must have iOS 7 or later.

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 v9.73, go to: https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=118

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.

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
v9.73	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

Starting with...	Change or Consideration	Description	Additional Resources
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 *Casper Suite Administrator's Guide*
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
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

Starting with...	Change or Consideration	Description	Additional Resources
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 *Casper Suite Administrator's Guide*
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
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

Starting with...	Change or Consideration	Description	Additional Resources
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 Server v10.7 or later
- Server.app (recommended)
- Java 1.6, 1.7, or 1.8
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6, 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) 6, 7, or 8
  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), Windows Server 2012 (64-bit), or Windows Server 2012 R2 (64-bit)
- Java SE Development Kit (JDK) 1.6, 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 1.6, 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 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 1.8 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

The following functionality has been deprecated:
Support for Java 1.6 and Tomcat 6 — Support for Java 1.6 and Tomcat 6 will be removed in a future version of the Casper Suite. 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.

The following functionality has been removed:
Casper Focus support for mobile devices with iOS 6 or earlier — Mobile devices with iOS 6 or earlier can no longer be used with Casper Focus. Student and teacher devices must have iOS 7 or later.

Bug Fixes and Enhancements

Casper Admin

- [D-007909] Fixed an issue that incorrectly caused a 403 connection error message to appear when a user is signed in to Casper Admin with an account that has no privileges.
- [D-007918] Fixed an issue that caused symbolic links to break when packages created with Adobe Creative Cloud were added to Casper Admin.
- [D-008602] Fixed an issue that prevented Casper Admin from functioning properly after replicating to the root JDS instance.

Casper Focus

- [D-008332] Casper Focus now displays the correct status of a student device after being refreshed.
- [D-008818] Fixed an issue that caused an App Lock command to be sent to a mobile device that does not have the selected app installed, causing the device to become unresponsive.
- [D-009166] Fixed an issue that sometimes caused Casper Focus to freeze when reopened after running in the background.

Casper Imaging

[D-008377] Fixed an issue that caused Casper Imaging to incorrectly increase the Recovery HD partition size during the imaging process.

jamf binary

- [D-008310] Fixed an issue that sometimes caused a FileVault 2 encryption key to be repeatedly submitted after it is uploaded.
- [D-008353] Fixed an issue that sometimes caused the jamf binary to attempt to download a non-existent package and repeatedly create log messages.

JAMF Software Server

- [D-005216] Fixed an issue that caused a push notification to be sent to an OS X computer after the computer is enrolled with the JSS, even if push notifications are disabled.
- [D-005545] Fixed an issue that sometimes caused incorrect computer inventory information to be displayed when adding a computer to the scope of a policy.

- [D-005697] Fixed an issue that caused user-initiated enrollment to be displayed as "failed" if an LDAP attribute mapping for a User ID has a non-numeric value.
- [D-006326] Fixed an issue that prevented a printer from being mapped using a policy if the printer was added to the JSS with the **Use generic PPD file** option selected.
- [D-006357] Fixed an issue that caused printers to be shared by default if they were installed using a policy.
- [D-006382] Fixed an issue that caused MAC addresses from unmanaged computers to be displayed as suggestions when using the ellipses (...) to choose a criteria for a smart group or advanced search.
- [D-006410] Fixed an issue that caused the JSS to incorrectly display an error in the management history for a computer if a user-level OS X configuration profile with a Printers payload is installed on the computer and the profile is then updated and redistributed to the computer.
- [D-006419] Fixed an issue that caused the JSS to incorrectly allow a site administrator to view license usage matches for computers in any site if the site administrator created the associated licensed software record from a template.
- [D-006549] Fixed an issue that caused the JSS to allow the deletion of a software update server on which a policy is based.
- [D-006629] Fixed an issue that caused a JSS user without the "create user" privilege to be able to create non-JSS users via the JSS API.
- [D-007716] Fixed an issue that sometimes prevented the JSS from distributing a managed app to a mobile device that has a configuration profile with a Restrictions payload and the **Allow installing apps** checkbox deselected if it is a supervised device with iOS 8.
- [D-007806] Fixed an issue that prevented JSS users with full access and JSS users with site access from viewing licensed software attachments when they viewed a specific site in the JSS.
- [D-007856] Fixed an issue that caused the JSS to incorrectly display a blank text field over the pane contents when saving a custom search path in the Computer Inventory Collection settings.
- [D-008145] Fixed an issue that caused the JSS to fail to include an attachment that was uploaded with a newly created enrollment profile.
- [D-008184] Fixed an issue that caused duplicate records to be displayed in smart group memberships and search results.
- [D-008230] You can now view limited information in the **Unknown** tab of a VPP account about an app or eBook purchased through Apple's Volume Purchase Plan (VPP) after it has been removed from iTunes or the Mac App Store and can no longer be assigned to a user.
- [D-008241] Fixed an issue that prevented an OS X computer from completing MDM enrollment if the organization name exceeds 64 characters in length.
- [D-008330] The JSS no longer sends an email notification about a clustering failure to all JSS user accounts with "read" or "update" privileges for clustering settings, and instead only sends the clustering failure notification to all JSS user accounts that have chosen to receive them.
- [D-008345] Fixed an issue that caused a mobile device to be incorrectly set to immediately require a password for all iTunes purchases after an iOS configuration profile with the Media Content **Apps** setting set to anything other than "Allow All Apps" is distributed.
- [D-008379] Fixed an issue that prevented Activation Lock from being cleared while attempting to wipe a device. As a result, the device was not wiped.

- [D-008395] Fixed an issue that caused an OS X computer imaged using Target Mode Imaging (TMI) via Casper Imaging v9.63 to have an incorrect FileVault 2 encryption status of "Ineligible - Eligible".
- [D-008401] Fixed an issue that sometimes caused a paid app managed with VPP managed distribution to fail to install on a mobile device after it is distributed to a user.
- [D-008551] The JSS now displays a notification when a VPP token has expired.
- [D-008552] Fixed an issue that caused a warning to be repeated multiple times in the `JAMFSoftwareServer.log`. This sometimes caused performance issues.
- [D-008663] Fixed an issue that prevented LDAP searches from timing out.
- [D-008688] Fixed an issue that caused OS X configuration profiles that include a Network payload configured with 802.1X authentication and the **Auto Join** checkbox selected to fail to automatically connect a computer to the network after the computer leaves sleep mode.
- [D-008691] Fixed an issue that caused the number of mobile devices in the scope of a configuration profile to be incorrectly listed as "1" after editing and re-distributing the configuration profile.
- [D-008772] Fixed an issue that caused the Password Policy complexity settings to be ignored when creating a JSS user account.
- [D-008788] Fixed an issue that caused the focus status to be incorrect for a device with the Self Service web clip installed when attempting to focus that device on the attention screen.
- [D-008853] Fixed an issue that caused timestamps in a PreStage enrollment to be inaccurate if the JSS and the Device Enrollment Program portal were out of sync.
- [D-008888] The JSS now displays the correct model for a MacBook Pro (Early 2015).
- [D-008898] Fixed an issue that prevented a SMB distribution point from being unmounted after running a policy after authenticating using an LDAP account.
- [D-008954] Fixed a persistent cross-site scripting (XSS) vulnerability that was identified in the JSS web application.
- [D-008955], [D-008956], [D-008957] Fixed multiple issues that caused a persistent cross-site scripting (XSS) vulnerability to exist in the JSS web application.
- [D-008970] Fixed an issue that prevented the JSS API from executing the `EraseDevice` and `DeviceLock` commands on OS X computers.
- [D-008989] Fixed an issue that caused duplicate eBooks to appear in the inventory information for a user.
- [D-008992] Fixed an issue that caused the JSS to display “Scope is corrupt” in the Scope column for a remote management task if the scope of the task was based on a specific user and the user was then deleted.
- [D-008993] Fixed an issue that sometimes prevented policies from being displayed in Self Service after viewing memberships for an LDAP user group.
- [D-009018] Fixed an issue that prevented the JSS API from being used to set the distribution method for an App Store app.
- [D-009031] The JSS no longer displays “No Disks” in the Storage category in the computer inventory information for some MacBook and MacBook Air 2015 models.
- [D-009049] Fixed an issue that caused the JSS to sometimes display duplicate computer records in the results of a simple computer search.
- [D-009077] Fixed an issue that prevented a policy with a Dock item from running properly if the Dock item was added via the JSS API.

- [D-009103] Fixed an issue that caused the policy dashboard in grid view to load slowly and consume large amounts of memory.
- [D-009109] Fixed an issue that sometimes prevented the JSS from stopping Tomcat due to scheduled user threads not being discarded in the `ScheduledThreadPool`.
- [D-009114] Fixed an issue that prevented an SMTP server configured to use TLS encryption from working when Java 1.8 is installed on the JSS host server.
- [D-009119] Cipher suites that use weak Diffie-Hellman key exchange algorithms are now disabled in the default `server.xml` file when performing a fresh installation.
  For more information on modifying the Tomcat `server.xml` file to specify a list of supported ciphers for HTTPS connections, see the Configuring Supported Ciphers for Tomcat HTTPS Connections Knowledge Base article.
- [D-009157] Fixed an issue that prevented classes, JSS users, and LDAP users from being correctly assigned when using the JSS API to POST or PUT ebooks or VPP assignments.
- [D-009198] Fixed an issue that caused an error to display when attempting to use the JSS API to PUT or POST an iOS app that is available in Self Service.

JSS Installer for Linux

[D-009024] The JSS Installer for Linux now correctly identifies the version of Java that is installed on the JSS host server.

JSS Installer for Windows

[D-008380] Fixed an issue that sometimes caused the JSS Installer for Windows to restart Tomcat before the `ROOT.war` file is fully extracted.

Self Service for iOS

[D-008621] Fixed an issue that sometimes prevented a configuration profile from deploying if two iBeacons with the same name were used as the basis for the scope of the profile.

Self Service for OS X

- [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-009084] Fixed an issue that caused a persistent cross-site scripting (XSS) vulnerability to exist in Self Service for OS X.

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-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-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-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-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-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-007843] Casper Focus incorrectly disables Speak Selection on a student device while the device is focused on an app.
- [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-007916] If a computer-level OS X configuration profile with a Password payload is installed on a computer with OS X v10.9, the user cannot log in to the computer after upgrading to OS X v10.10.
- [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-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-008560] A configuration profile set to log a user out after a certain amount of time fails to do so.
- [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-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.