Casper Suite Release Notes

Version 9.7

Contents

What's New in This Release

- **End-User License Agreement (EULA) updated**—The EULA for the Casper Suite has been updated and must be accepted by an administrator after the JSS is upgraded. The EULA now includes additional information about license types and legal protections that are important to our customers and our lawyers. Changes have also been made that allow us to be more transparent about privacy and the data provided to JAMF Software from the JSS.

- **Customer Experience Metrics (CEM) enhancements**—CEM data is now displayed in an easy-to-read format in the Customer Experience Metrics setting in the JSS. In addition, starting with the Casper Suite v9.7, the Customer Experience Metrics setting is enabled by default and CEM data is submitted automatically to JAMF Software.

  For detailed information, see the Customer Experience Metrics Knowledge Base article.

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

- **Additions to Event Logs**—You can now use Event Logs to view the status of Casper Imaging events.

- **Wipe multiple mobile devices**—You can now send a remote command to wipe multiple devices. You also have the option to clear Activation Lock when wiping those devices.

- **eBook distribution enhancement**—eBooks that are textbooks can now be added to the JSS and distributed with the Casper Suite.

- **New workflow for building OS packages**—Composer can now be used to create a single DMG that includes multiple partitions. As a result, you no longer need to create a separate DMG of the "Recovery HD" partition or manually add a partition to a configuration.

- **Mobile device PreStage enrollment enhancements**—Mobile device PreStage enrollments can now be configured to skip the Touch ID and Apple Pay steps in Apple's Setup Assistant.

- **New settings in OS X configuration profiles**:
  - Added the Fonts payload
  - Added the Check Point Mobile VPN type

- **New settings in iOS configuration profiles**:
  - Multiple fonts can be added to the Fonts payload
  - Added the renewal certificate option to the Single Sign-On payload

- **New remote commands available in the JSS API**:
  - Blank Push
  - Enable/Disable Voice Roaming
  - Enable/Disable Data Roaming
  - Clear Restrictions
  - Device Name
  - Wallpaper

- **Security enhancements**:
  - Failed login attempts are now logged to `JSSAccess.log` and the `jss_access_logs` database table.
  - Users can now be locked out after a specified number of failed attempts to log in to the JSS or the client applications.
  - JSS administrators can now set a required password complexity for JSS user accounts.
- **Casper Focus attention screen**—Teachers can now lock student devices to an unusable screen.
- **Volume Purchase Program (VPP) enhancements**:
  - Apps and eBooks can now be added to the App or eBook Catalog from a VPP assignment.
  - Apps and eBooks can now be viewed from a VPP assignment.
  - Mac App Store apps and iOS apps can now be distributed to users and user groups.
  - A content search can now be used to view the users and VPP assignments that the content is assigned to.
  - VPP invitations can now be resent to users.
- **Improvements to the JAMF Cloud**:
  - Log flushing can no longer be disabled for a cloud-hosted JSS.
  - Email notifications are no longer sent when Apache Tomcat is started or stopped.
  - The following settings are not applicable to a cloud-hosted JSS and have been removed:
    - Limited Access
    - Apache Tomcat
    - Clustering
    - JSS URL
    - Memory Usage
    - Database Table Status
- **iBeacon reporting enhancements**—When iBeacon region monitoring is enabled, iBeacon regions are now displayed in the inventory information for computers or mobile devices that are in a region. In addition, iBeacon regions can be used as criteria for advanced searches to return all devices within a region.
- **Change management improvements**—Change management logs can now be viewed in the JSS.

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 v9.7, go to:

https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=105

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
v9.7	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*

Starting with...	Change or Consideration	Description	Additional Resources
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
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

Starting with...	Change or Consideration	Description	Additional Resources
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
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 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 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 1.7 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-008438 Fixed an issue that prevented Casper Admin from mounting a file share with a space in its name.
- D-008485 Fixed an issue that prevented users from logging in to the client applications v9.62 or later with an LDAP directory account if the user's password contains a colon (:).
- D-008630 Fixed an issue that prevented Casper Admin from mounting an SMB share.

Casper Focus

- D-008507 Fixed an issue that prevented Casper Focus from loading when more than 500 apps are in the JSS.
- D-008693 Fixed an issue that prevented the *Casper Focus User Guide* from being available in Casper Focus v9.64.

Casper Imaging

D-008217 Fixed an issue that prevented Casper Imaging from creating multiple partitions when imaging a drive that has core storage enabled.

jamf binary

- D-006701 Fixed an issue that caused package downloads to fail if the file download URL is longer than 255 characters. This mainly applies to signed URLs.
- D-007695 Fixed an issue that caused the jamf binary to report an IP address that is not the local IP address of a computer if OpenVPN is running on that computer.
- D-008306 Fixed an issue that caused a kernel panic to occur on a computer with multiple FileVault 2 users if the originally-assigned FileVault 2 user has been disabled and one of the enabled users logs in after a reboot.
- D-008366 Fixed an issue that prevented an AFP file share distribution point from being mounted if the password for the distribution point contains a special character.
- D-008577 Fixed an issue that caused Self Service for OS X to display an error when a policy runs successfully if that policy failed the last time it was run.

JAMF Distribution Server

- D-008158 Fixed an issue that caused the JDS Installer for Linux to replace the existing Apache Tomcat configuration file instead of appending a self-contained file to the correct directory.

- D-008388 Fixed an issue that prevented the JDS Installer for Linux from successfully running on Ubuntu v14.04 when Apache Tomcat v2.4 is installed.

JAMF Software Server

- D-004883 Fixed an issue that prevented the Custom Settings payload from being accessed in a OS X configuration profile that was uploaded to the JSS.

- D-005202 Fixed an issue that caused a Managed Preference profile to be deleted after attempting to add and save certain payloads.

- D-005269 Fixed an issue that prevented the JSS from displaying values for extension attributes in the search results of a simple computer search for inventory items other than computers.

- D-005332 Fixed an issue that caused users with "Enrollment Only" privileges to be able to edit inventory information for a computer or mobile device.

- D-005407 Fixed an issue that sometimes caused the JSS to send multiple email notifications when a restricted software violation occurs.

- D-005477 Fixed an issue that caused an incorrect JSS URL to be sent for certain email notifications.

- D-005541 Fixed an issue that prevented the **Hide All** button from hiding all policies on the Policy pane if multiple policy categories start with the same word.

- D-005704 Fixed an issue that prevented operating system requirements from being removed from a package after they have been specified.

- D-006155 Fixed an issue that prevented Managed Preference profiles from allowing more than one application or document tile to be created for the Dock.

- D-006183 Fixed an issue that prevented the JSS from correctly sorting policy logs by date.

- D-006286 Fixed an issue that prevented Home Folder Reduction Managed Preference profiles from allowing more than one login redirection of the same type to be created.

- D-006368 Fixed an issue that prevented email notifications for Tomcat being started or stopped from including the name of the web application or a timestamp for the action.

- D-006771 Fixed an issue that caused the JSS to remain in edit mode when attempting to save a newly created user.

- D-006998 Fixed an issue that caused all users and devices to be returned when using an advanced search or smart group to return users or devices with a username that contains an underscore (_) or a percent sign (%).

- D-007063 Fixed an issue that prevented users without the "Create Computers" or "Create Mobile Devices" permission from preforming mass actions.

- D-007136 Fixed an issue that caused the deletion of a site included in a scope to result in the scope or limitation being incorrectly changed to include all devices.

- D-007203 Fixed an issue that prevented a user from saving a script with no limitations if the script/printer had a previously saved limitation.

- D-007491 Fixed an issue that prevented PDF attachments from being uploaded to a mobile device inventory record.
- D-007667 Fixed an issue that caused the JSS to remain in edit view after editing and saving a user object.
- D-007812 Fixed an issue that prevented fields for printer PPD file or PPD file path from appearing in the JSS API.
- D-008074 Fixed an issue that caused the JSS to format data using relative times/dates instead of absolute times/dates when exporting data based on the results of an advanced search.
- D-008166 Fixed an issue that prevented an app from being distributed to a mobile device if the mobile device was added to the scope of the app using the JSS API.
- D-008180 The JSS API now allows the PUT action to be used for an API object with a category of "None".
- D-008199 Fixed an issue that prevented a user group from being added to a Login Window OS X configuration profile.
- D-008220 Fixed an issue that caused the JSS to display an error when attempting to edit certain objects in the JSS using Google Chrome if there are saved passwords in Google Chrome.
- D-008228 Fixed an issue that prevented the JSS from respecting all iBeacon regions if each region has the same UUID.
- D-008244 Fixed an issue that prevented a policy from running the JAMF Helper as a background process using a script with a command followed by an ampersand (&).
- D-008282 Fixed an issue that prevented a custom icon from being displayed for an OS X configuration profile in Self Service.
- D-008302 Fixed an issue that prevented LDAP users from being created, assigned to a computer, and added to a site when a computer is enrolled using an enrollment invitation.
- D-008321 Fixed an issue that sometimes prevented an Energy Saver OS X configuration profile from being saved if Tomcat 7.0.57 is installed on the JSS host server and another payload is configured in the profile.
- D-008338 Fixed an issue that prevented an LDAP user from being assigned to a mobile device via user-initiated enrollment if a partial username was entered for the LDAP user and the LDAP server is set to use wildcards when searching.
- D-008376 Fixed an issue that caused a computer with OS X v10.9 to become unresponsive after attempting to log into the Guest account for the second time during a single session.
- D-008403 Fixed an issue that prevented the JSS from accurately reporting the usage information for a VPP invitation if the invitation includes users who have accepted a previously sent invitation.
- D-008475 Fixed an issue that prevented a mobile device from successfully enrolling using a PreStage enrollment if user authentication is required and the user's password contains a colon (:).
- D-008493 Fixed an issue that prevented the JSS from returning eBooks that are classified as textbooks in search results.
- D-008505 Fixed an issue that prevented Customer Experience Metrics from being submitted when computer extension attributes are in use.
- D-008555 Fixed an issue that caused certain management commands to be executed up to 10 times per minute on mobile devices enrolled using a PreStage enrollment until all automatically installed apps have finished installing.
- D-008570 Fixed an issue that caused Event Logs to load very slowly when there are hundreds of configuration profiles in the JSS.

- D-008572 Fixed an issue that prevented a package from installing if there are special characters in the package name.
- D-008573 Fixed an issue that prevented .cer files from being uploaded to the Certificate payload of an OS X configuration profile.
- D-008585 Fixed an issue that prevented policies containing an OS X installer from running on computers enrolled with Casper Suite v9.64 via Casper Imaging.
- D-008612 Fixed an issue that caused a VPN OS X configuration profile with an L2TP connection type set to require certificate user authentication to incorrectly require password user authentication if the SCEP payload is configured.
- D-008622 Fixed an issue that caused the JSS to enforce restricted software settings on applications that are not included in the restricted software records.
- D-008642 Fixed an issue that prevented users from being added to a static user group via the JSS API and caused all users to be removed from the group.
- D-008644 Fixed an issue that prevented VPP invitations from being accepted via the Self Service web clip if app installation is restricted using a configuration profile.
- D-008665 Fixed a reflected cross-site scripting (XSS) vulnerability in the JSS web application.
- D-008683 Fixed an issue that caused a JSS in a clustered environment to fail to communicate changes in VPP assignments to non-master JSS web applications.
- D-008801 Fixed an issue that prevented an in-house app from updating automatically and caused the app to be removed from the device.

Recon

- D-008335 Fixed an issue that prevented Recon from opening on OS X v10.9 or later if the preferred language setting in OS X System Preferences is set to a language other than English.
- D-008541 Fixed an issue that prevented a management account from being able to log in to a computer if the password for that account contains a dollar sign ($).

Self Service Mobile

D-008422 Fixed an issue that caused Self Service Mobile for iOS to be uninstalled if it is set to install automatically and be installed via the app catalog.

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 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-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-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-008272] If an iOS configuration profile is configured with a Restrictions payload specifying an Autonomous Single App Mode app and the profile is installed on a mobile device, the device is not immediately locked to the specified app and a prompt to enable Guided Access is displayed when the app is opened.
- [D-008286] When VMware Fusion is closed on a client computer, the computer loses its connection with the JSS. For more information see the following Knowledge Base article:

  Restoring a Computer's Connection with the JSS after Quitting VMware Fusion
- [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-008401] A paid app managed with VPP managed distribution sometimes fails to install on a mobile device after it is distributed to a 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-008742] Computer names that contain emoji characters do not display correctly.