Casper Suite Release Notes

Version 9.64

Contents

What's New in This Release

- **Event Logs**—You can now use Event Logs to view the distribution status of configuration profiles to computers and mobile devices.

- **Setting the wallpaper**—Added the ability for JSS administrators to set the wallpaper on supervised mobile devices with iOS 7 or later

- **Improved workflow for enabling MDM for local user accounts**—Added the ability to enable MDM on computers with OS X v10.10 without requiring local administrator credentials to be entered on end users' devices

- **New settings in OS X configuration profiles**—

  - Restrict AirPlay destinations in AirPlay payload

  - Additions to the Restrictions payload:
    - Disable Safari autofill
    - Force-enable System Preferences items

  - WPA2 Personal and WPA2 Enterprise security types in the Network payload

- **New settings in iOS configuration profiles**—

  - WPA2 Personal and WPA2 Enterprise security types in the Wi-Fi payload

  - Additions to the Restrictions payload:
    - Disable predictive text
    - Disable auto-correct
    - Disable spell check
    - Disable definition lookup

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 v9.64, go to:

https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=103

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

Backward Compatibility

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

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

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

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

Installation

Preparing to Upgrade

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

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

Functionality Changes and Other Considerations

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

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

Starting with...	Change or Consideration	Description	Additional Resources
v9.51	Modified support for OS X v10.5 and v10.6	Features implemented in the Casper Suite v9.51 or later are no longer supported on computers with OS X v10.5 and v10.6. Workflows implemented prior to v9.51 will continue to function, but they may require earlier versions of the client applications.	"Requirements" section in the *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

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 *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 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 certificated-based authentication	If you are upgrading the Casper Suite v8.2x or earlier, it is recommended that you enable certificate-based authentication. Doing so ensures that device certificates on OS X computers are valid.	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-007580] Fixed an issue that prevented printers from being added when the MySQL `max_allowed_packet size` is set to a small value (e.g., 16 MB or less).
- [D-008218] Fixed an issue that caused Casper Admin to crash when attempting to replicate files from a file share distribution point to an external drive with OS X v10.10 installed.

Casper Focus

- Random special characters are no longer displayed when viewing the app in German.
- [D-008213] Fixed an issue that sometimes prevented the focus from being removed from a website.
- [D-008237] Fixed an issue that caused a device to remain focused on an app when the focus is removed after the class has ended.

Casper Imaging

- [D-008070] Fixed an issue that prevented a computer from being enrolled on startup after being imaged offline.
- [D-008472] Fixed an issue that caused an OS X v10.10.2 DMG with a priority of "1" to copy excessively slowly when using Netboot or Target Mode Imaging.

Casper Remote

[D-008362] Fixed an issue that prevented users from being able to press the Space bar to select all the computers in a smart computer group in Casper Remote.

jamf binary

- [D-006938] Client applications no longer upgrade if the jamf binary fails to upgrade.
- [D-006986] Fixed an issue that prevented the jamf binary from killing a process using a policy if the process has an apostrophe in its name.
- [D-007365] Fixed an issue that caused a mounted SMB share to be displayed in multiple incorrect locations when mounted using the `jamf mount` command by a user that is not an administrator.
- [D-008091] Fixed an issue that caused information to be disclosed in the process list when setting an EFI password using a policy.

- [D-008092] Fixed an issue that caused the username and password for an SMB share to be displayed in the process list while running a policy to install a package from that SMB share.
- [D-008356] Fixed an issue that caused policies that were successfully run on a failover distribution point to have a a status of "failed" in the policy logs.

JAMF Distribution Server

- [D-005796] Fixed an issue that prevented a computer that is booted to a NetBoot image from being imaged when the master distribution point is a JDS instance.
- [D-007216] Fixed an issue that prevented the JDS Installer for Linux from enrolling a JDS instance with the JSS if all Apache modules are either disabled or not installed.
- [D-007811] Fixed an issue that caused the JDS Installer for Linux to modify the `/etc/sudoers` file.
- [D-008437] Fixed an issue that caused the JDS Installer for Linux to fail on certain CentOS Linux distributions.

jamf.exe

- [D-008275] Fixed an issue that caused jamf.exe to ignore the `-overrideJSS` flag.
- [D-008349] Fixed an issue that caused the MAC address for a virtual NIC to be collected.
- [D-008363] Fixed an issue that prevented the jamf.exe from supporting the `-skipCertificateCreation` flag.

JAMF Helper

[D-007611] Fixed an issue that prevented the JAMF Helper icon from being fully displayed when viewed using the `-fullScreenIcon` command.

JAMF Software Server

- [D-004624] Network segments are now evaluated on both the Last IP and the Last Reported IP.
- [D-005643] Fixed a session fixation vulnerability in the JSS web application.
- [D-005648] Added file type validation for files uploaded to the JSS.
- [D-005826] Fixed an issue that prevented JSS users that belong to multiple groups and have privileges for different sites from creating Recon QuickAdd packages for more than one site.
- [D-005872] Fixed an issue that prevented the JSS from collecting the IP address of Apple TV devices.
- [D-006453] Fixed an issue that caused a white page to display when clicking the **Management** tab in inventory information for a mobile device if the device is assigned to a class that is deleted from the JSS while it is in the scope of an eBook.
- [D-006480] Fixed an issue that caused the JSS URL link sent via email notifications for a change in smart user group membership to be invalid.

- [D-006518] Fixed an issue that prevented the JSS from binding OS X v10.9 computers to Open Directory using a policy if the configured LDAP server is running OS X Server v10.9.

- [D-006657] Fixed an issue that prevented the JSS from sending a VPP invitation configured to prompt the user on their device if the device was enrolled using a PreStage enrollment and the Setup Assistant was still active at the time that the JSS attempted to send the invitation.

- [D-006866] Fixed an issue that prevented the JSS from displaying the results page after a blank simple user search is performed if there are no users in the JSS.

- [D-007171] Fixed an issue that prevented the JSS from automatically reinstalling user-level configuration profiles after they are manually removed from System Preferences.

- [D-007180] Fixed an issue that prevented a user from being recognized as a member of an Active Directory group when the group has over 1,500 users and group membership information is retrieved from the group object.

- [D-007188] Fixed an issue that prevented Wi-Fi configuration profiles with a WPA2 security type and TTLS selected as the accepted EAP type from being generated correctly. This prevented mobile devices and computers from connecting to Wi-Fi.

- [D-007282] Fixed an issue that prevented the JSS Dashboard from loading quickly when attempting to display a policy that contains thousands of logs.

- [D-007422] Fixed an issue that prevented the **Description** field from being populated when adding a Mac App Store app to the JSS.

- [D-007604] Fixed an issue that prevented the value for the **Active Network Interface** field from being displayed in the inventory information for computers with OS X v10.10.

- [D-007627] The JSS now allows users to pull content recently purchased from VPP into the JSS when the content is not displayed in a VPP assignment.

- [D-007709] Fixed an issue that prevented users from completing VPP invitations sent via prompt on mobile devices if the App Store is restricted using an iOS configuration profile with **Allow installing apps** deselected in the Restrictions payload.

- [D-007884] Fixed an issue that prevented a policy from running if it is configured with a client-side limitation to require an Ethernet network connection and the Ethernet connection has been renamed from the default name.

- [D-007897] Fixed an issue that caused an app to permanently appear as "pending" in Self Service after it was installed if the configuration profile used to deploy the app was deleted.

- [D-007938] Fixed an issue with OS X configuration profiles where the Directory Type reverts to "Open Directory/LDAP" after being saved as "Active Directory".

- [D-007962] Fixed an issue that caused the JSS to incorrectly remove unmanaged apps from mobile devices if the apps were originally deployed as managed apps.

- [D-008050] Fixed an issue that prevented the site for an Apple TV from being saved after it is manually edited.

- [D-008121] Fixed an issue that prevented mobile devices with App Store restrictions from downloading App Store apps distributed using a VPP code spreadsheet.

- [D-008130] Fixed an issue that caused VPP content and user-level OS X configuration profiles to be removed from mobile devices and computers when the scope is limited to LDAP users or LDAP user groups and the JSS connection to the LDAP server is interrupted.

- [D-008137] Fixed an issue that prevented the JSS from retaining user and location information and site information after a computer with OS X v10.10 or later is enrolled using a PreStage enrollment.

- [D-008233] Fixed an issue where `InstallApplication` commands were delayed for devices enrolled using a PreStage enrollment.
- [D-008236] Fixed an issue that prevented computers from automatically joining the Wi-Fi network configured using an 802.1X configuration profile.
- [D-008279] Fixed an issue that prevented the SCEP Admin page password for an external CA with the "Dynamic-Microsoft CA" challenge type from being retained in the JSS after it is changed.
- [D-008283] Fixed an issue that prevented the JSS from sorting the list of assigned apps or eBooks in a VPP assignment.
- [D-008288] Fixed an issue that prevented the building and department from being updated in the inventory information for a mobile device that was re-enrolled using a PreStage enrollment with **Supervise Device** selected.
- [D-008289] Fixed an issue that prevented the Android version name from being displayed in mobile device inventory information for a device with Android 5.0 or later.
- [D-008322] Fixed an issue that prevented policies containing an OS X v10.10 Installer from running on computers with OS X v10.6.8.
- [D-008326] Fixed an issue where the **Use Per Connection Password** setting was not being saved for TTLS Wi-Fi configuration profiles.
- [D-008350] English text is now displayed for IKEv2 personal device profiles.
- [D-008354] A full list of computer reports is now displayed in JSON when using a GET method to return a list of all computer reports.
- [D-008368] When a Self Service policy set to require an inventory update is run, a message is displayed in the policy logs stating that inventory will be updated when all queued actions in Self Service are complete.
- [D-008399] LDAP membership tests are now available in the JSS API.
- [D-008411] Fixed an issue that caused text in the **Username** field to be logged following a failed login attempt to Self Service.
- [D-008415] App Store apps originally configured to be installed automatically that failed to do so can now be installed using Self Service Mobile for iOS.
- [D-008450] Fixed an issue that prevented a managed app from being removed from a mobile device after the app was deleted from the JSS.
- [D-008455] Fixed an issue that caused a SQL exception to be thrown when there are more than 127 log actions in a single log.
- [D-008500] Fixed an issue that prevented Autonomous Single App Mode from working when multiple configuration profiles containing restrictions are installed on a mobile device.

JSS Database Utility

[D-005833] Fixed an issue that caused the "Restart MySQL" and "MySQL Settings" options to be greyed out in the JSS Database Utility on Windows computers that have MySQL 5.6.

Recon

[D-006222] You can now configure a QuickAdd package created with Recon to randomly generate a password when a new management account is created.

Self Service Mobile

- [D-008036] Fixed an issue that caused an incorrect message to be displayed on a device when an end user attempts to reinstall a managed in-house eBook before it has completely installed.
- [D-008257] Fixed an issue that prevented Self Service Mobile for iOS from connecting to the JSS if the app is installed automatically during enrollment and it is not opened within 24 hours of being installed.
- [D-008443] Fixed an issue that sometimes prevented a user from using Self Service Mobile for iOS or the Self Service web clip to install a paid app.

Self Service for OS X

[D-008360] Fixed an issue that caused a Self Service policy to remain in the interface after it was run if it was the last policy to be run and it was set to run once per computer.

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-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-008286] When VMware Fusion is closed on a client computer, the computer loses its connection with the JSS.
- [D-008306] On a computer with multiple FileVault 2 users where the originally-assigned FileVault 2 user has been disabled, a kernel panic occurs when one of the enabled users logs in after a reboot.
- [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.