Casper Suite Release Notes

Version 9.21

Contents

What's New in This Release

Key Features

The Casper Suite v9.2 includes the following key features:

- **Support for OS X Mavericks (v10.9)**—The Casper Suite now includes support for OS X v10.9.
- **Additions to OS X and iOS configuration profiles**—New payloads and settings have been added to OS X and iOS configuration profiles. This includes but is not limited to: OS X Per-App VPN payload, OS X Finder payload, and iOS Restrictions settings.
- **FileVault 2 enhancements**—Additional options have been added for managing FileVault 2 disk encryption in your environment. This includes new criteria for creating smart groups and advanced searches, the ability to issue a new recovery key to computers, and new options for enabling or disabling users for FileVault 2.
- **New workflow for upgrading computers to OS X v10.7 or later**—Computers can now be upgraded using the .app file from the Mac App Store and the policy framework.

The Casper Suite v9.21 includes the following improvements:

- **JSS performance and stability improvements**—The JSS is now more efficient at processing MDM commands and utilizing memory, and the amount of communication needed between the JSS and MySQL has been reduced.
- **JSS upgrade enhancements**—Upgrading the JSS from v8.x is now more reliable and efficient.
- **Advanced search, smart group, and static group enhancements**—The JSS now migrates advanced searches, smart groups, and static groups more reliably during upgrades. In addition, the JSS is now more efficient with advanced search results, and smart and static group memberships.
- **LDAP integration enhancements**—Adding LDAP servers, scopes based on LDAP users or groups, and JSS user accounts from LDAP are now more reliable. LDAP-based inventory information is also more accurate.
- **Administrative application enhancements**—The administrative applications are now more reliable and efficient.

Casper Focus v9.21 will be available from the App Store when it is approved by Apple.

Implemented Feature Requests

To view a complete list of feature requests that are implemented in this release, go to:

https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=47

API Improvements

Earlier versions of the JSS API returned inconsistent values, making it difficult to compare values and maintain consistency. In the JSS API v9.0 and later, the following changes have been made to improve this:

- Values are always returned as integers.
- There are new keys that provide pre-converted integer values in the associated unit of measure.
- Data is automatically converted to the appropriate integer value.

  For example, if a computer or mobile device submits data that is inconsistent with the integer values, the JSS API converts the value to the appropriate value.

The following table shows the items in the API that have changed as a result:

Item	Data Name	Previous Value	New Value	Additional Keys
Mac bus speed	bus_speed	String value in GHz (e.g., "1.07 GHz")	Integer value in MHz (e.g., "1095 MHz")	bus_speed_mhz
Mac processor speed	processor_speed	Integer value in MHz (e.g., "2260 MHz")	Integer value in MHz (e.g., 2314 MHz")	processor_speed_mhz
Mac total memory	total_ram	Integer value in MB (e.g., "2048 MB")	Integer value in MB (e.g., "2048 MB")	total_ram_mb
Mac full internal drive size Individual partition size	size	String value in GB (e.g., "500.11 GB")	Integer value in MB (e.g., "512113 MB")	drive_capacity_mb partition_capacity_mb
Mac size of cache	Mac size of cache	String value in MB (e.g., "3 MB")	Integer value in KB (e.g., "3072 KB")	cache_size_kb

Installation

Compatibility

The JSS v9.2 supports the following versions of client applications in the Casper Suite:

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

You can use any version of Composer.

To take full advantage of new features and bug fixes, use the most current version of each application.

Upgrading the JSS

Use the JSS Installer to upgrade the JSS.

Note: The time it takes to upgrade from the Casper Suite v8.x or earlier has increased due to the number of changes and improvements in the JSS. The amount of time added depends on the number of mobile devices and computers in your inventory and the number of features utilized in the Casper Suite.

Before You Upgrade

Before you upgrade, consider the following:

- **If you are using smart groups**—The JSS v9.0 and later 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" then "Version" before upgrading from v8.x to v9.0 or later. This applies to the "Title"/"Version" criteria for applications, fonts, plug-ins, and mobile device apps.

  For detailed instructions, see the following Knowledge Base article:

  Switching the Order of Smart Group Criteria

- **If you are using Managed Preferences**—There are two types of Managed Preferences that are lost when you upgrade from v8.x to v9.0 or later. For detailed information, see the following Knowledge Base article:

  Managed Preferences and Upgrading to v9.0 or Later

Mac Requirements

To upgrade to the JSS v9.21 on OS X Server, 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 later
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or later

  You can download the latest 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

Linux Requirements

To upgrade to the JSS v9.21 on 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 10.04 LTS Server (64-bit)
    - Ubuntu 12.04 LTS Server (64-bit)
    - Red Hat Enterprise Linux (RHEL) 6
- Open Java Development Kit (OpenJDK) 6 or later

  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

Windows Requirements

To upgrade to the JSS v9.21 on 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)
- Java SE Development Kit (JDK) 1.6 or 1.7 for Windows x64

  You can download the latest 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 latest 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

1. Back up the current database using the JSS Database Utility.

2. Back up custom reports.

3. Copy the most current version of the JSS Installer for your platform to the server.

4. Double-click the installer and follow the onscreen instructions to complete the upgrade.

5. If you scheduled database backups using the JSS Database Utility v8.2, it is recommended that you reschedule the backups using the updated version of the JSS Database Utility.

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

Enabling Certificate-Based Authentication

If you are upgrading from the JSS v8.2 or earlier, it is recommended that you enable certificate-based authentication. Enabling certificate-based authentication ensures the JSS verifies that device certificates on OS X computers are valid.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Computer Management**.

   On a smartphone, this option is in the pop-up menu.

4. In the "Computer Management–Management Framework" section, click **Security** 🔒 .

5. Click **Edit**.

6. Select the **Enable certificate-based communication** checkbox.

7. Click **Save**.

Distributing an MDM Profile for App Management

Distributing managed apps with the Casper Suite requires mobile devices with iOS 5 or later and an MDM profile that supports app management.

As of the Casper Suite v8.3, devices that have iOS 5 or later when they are enrolled with the JSS automatically obtain an MDM profile that supports app management. Managed iOS 4 devices that are upgraded to iOS 5 or later do not obtain this profile.

To update the MDM profile on devices, you must distribute an updated MDM profile using the Self Service web clip. When users install the profile on an iOS 5 device, the device has app management capabilities.

Note: You cannot distribute an updated MDM profile via the Self Service web clip to mobile devices enrolled using an enrollment profile.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Mobile Device Management**.

   On a smartphone, this option is in the pop-up menu.

4. Click **Self Service Web Clip** 📱 .

5. Click **Edit**.

6. Ensure that the **Install Automatically** checkbox is selected, and then select the **MDM profile updates** checkbox.

7. Click **Save**.

Enrolling Mobile Devices Using Enrollment Profiles

There are two things to consider if you plan to use enrollment profiles to enroll mobile devices with the Casper Suite:

- **Enrollment profiles downloaded from the Casper Suite v8.71 or earlier**—Enrollment profiles downloaded from the Casper Suite v8.71 or earlier cannot be used to enroll mobile devices with the Casper Suite v8.72 or later. Before enrolling devices with the upgraded version of the Casper Suite, re-download any enrollment profiles downloaded from v8.71 or earlier.

- **Enrolling mobile devices that have iOS 7**—Enrollment profiles created using the Casper Suite v9.0 or earlier cannot be used to enroll mobile devices that have iOS 7 or later. If you plan to enroll devices that have iOS 7 or later, you will need to create a new enrollment profile using the Casper Suite v9.1 or later.

Note: Mobile devices that were originally enrolled with the Casper Suite v9.0 or earlier using an enrollment profile do not need to be re-enrolled when the devices are upgraded to iOS 7.

For information on creating an enrollment profile, see the "Enrollment Profiles" section in the *Casper Suite Administrator's Guide*.

Distributing Signed Configuration Profiles from Apple

If you have a signed configuration profile from Apple, you can upload and distribute it to mobile devices with the Casper Suite v9.21 or later. For instructions, see the following Knowledge Base article:

Distributing a Signed Configuration Profile from Apple

Upgrading to OS X Server v10.9

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

1. Back up your current database.

2. Upgrade from OS X v10.8 to v10.9.

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.

Bug Fixes and Enhancements

Casper Admin

Fixed in 9.2:

[D-005084] Fixed an issue that prevented Casper Admin from connecting to the JSS after upgrading the JSS to v9.0 or later.

Fixed in 9.21:

- [D-005384] Fixed an issue that caused the installation if non-flat Adobe PKGs larger than 5 GB to fail if one of the following is true:
  - You upgraded to the JSS v9.0 and then migrated packages and scripts using Casper Admin.
  - You performed a fresh installation of the JSS v9.0.
- [D-005422] JSS user accounts with a password that contains an apostrophe (') can now be used to replicate files from the master distribution point to the root JDS instance.
- [D-005626] Fixed an issue that caused Casper Admin to crash when adding a .applescript file to the application if scripts are stored in the database.

Casper Focus

Fixed in 9.21:

- [D-005153] Casper Focus now displays an error when adding eBooks to a class if Tomcat is not running.
- [D-005211] Fixed an issue that allowed teachers to log in when the JSS URL in Casper Focus started with "http" instead of "https".
- [D-005259] Fixed an issue that allowed Casper Focus to focus a teacher mobile device on an app.
- [D-005300] Fixed an issue that prevented Casper Focus from displaying the full JSS timeout message.
- [D-005386] Fixed an issue that caused Casper Focus to crash when focusing 32 or more devices on an app.
- [D-005646] Casper Focus now displays a message to teachers indicating that student devices are focused.

Casper Imaging

Fixed in 9.2:

- [D-005079] Fixed an issue that caused duplicate computer records to be added to the JSS when imaging computers using ethernet dongles that have been added to the JSS as removable MAC addresses.
- [D-005084] Fixed an issue that prevented Casper Imaging from connecting to the JSS after upgrading the JSS to v9.0 or later.

Fixed in 9.21:

- [D-005369] Fixed an issue that prevented Casper Imaging from enrolling a computer using a JSS user account that was added from LDAP and has site access.
- [D-005617] Fixed an issue that caused Casper Imaging to fail when using debug mode and Autorun data.
- [D-005692] Fixed an issue that prevented Casper Imaging from displaying the **Site** button if there were multiple login attempts.

Casper Remote

Fixed in v9.2:

[D-005084] Fixed an issue that prevented Casper Remote from connecting to the JSS after upgrading the JSS to v9.0 or later.

Composer

Fixed in v9.21:

[D-005583] Fixed an issue that sometimes prevented Composer from updating package manifests.

jamf binary

Fixed in v9.21:

- [D-004798] Fixed an issue that caused excessive logging to occur in the jamf.log after executing the `sudo jamf manage -verbose` command.
- [D-005248] Improved the security of the JAMFCore when operating in CBC mode.
- [D-005274] Fixed an issue that caused policies that include a script with the "After" priority and a script with the "Before" priority to fail over HTTP(S) if the JSS has been upgraded from v8.x and scripts were not migrated to the database.
- [D-005277] Fixed an issue that prevented the JSS from excluding more than one user from the scope of restricted software records.
- [D-005537] Fixed an issue that caused the following fdesetup information to be displayed in the output after executing the `sudo jamf recon` command:

   "fdesetup: auth info dictionary path = stdin"
- [D-005552] Fixed an issue that prevented the jamf binary from collecting FileVault disk encryption information from computers that were encrypted using the JSS v8.72 or 8.73.
- [D-005598] Fixed an issue that prevented the jamf binary from collecting computer inventory information when the information contains an unsupported unicode character.

JAMF Helper

Fixed in v9.21:

[D-004503] Fixed an issue that prevented JAMF Helper messages from being displayed on a computer in Target Display Mode (TDM).

JAMF Software Server

Fixed in v9.2:

- [D-005032] Increased the speed of device migration during JSS upgrades.
- [D-005184] Fixed an issue that prevented the JSS from saving the **Enable Certificate-Based Authentication** option for parent JDS instances.
- [D-005226] Fixed an issue that prevented the JSS from properly updating license usage information for licensed software records.
- [D-005240] Fixed an issue that prevented the JSS from updating the building and department in inventory when computers and mobile devices enter a network segment that has a default building and department and is configured to override this information in inventory.
- [D-005341] Fixed an issue that caused web browsers to crash when editing configuration profiles in the JSS.
- [D-005343] Fixed an issue that caused the web browser to crash when editing an app in the JSS if the database is too large.
- [D-005349] The JSS now prevents you from clicking the **Next** button multiple times while creating sites from buildings and departments. This resulted in duplicate buildings and departments.
- [D-005411] Fixed an issue that prevented the JSS from updating inventory for mobile devices that have duplicate apps listed in inventory.
- [D-005413] The JSS now performs a check for the Java Cryptography Extension (JCE) files at startup.
- [D-005427] Fixed an issue that prevented the JSS from displaying the admin status of local user accounts in computer inventory information.
- [D-005429] Fixed an issue that could prevent devices from being migrated properly after upgrading the JSS to v9.0 or later.
- [D-005470] Improved JSS performance for LDAP lookups when configuring the scope of a management task.
- [D-005507] Improved JSS performance for redistributing mobile device apps and provisioning profiles.

Fixed in v9.21:

- [D-004316] Fixed an issue that prevented the values for `ldapServerID` and `userID` from being updated in the JSS when passed using the `sudo jamf recon` command.
- [D-004469] Fixed an issue that prevented the JSS from displaying the **Records Up To Date** tab when using a mobile device to mass look up and populate purchasing information from GSX for computers.
- [D-004726] Fixed an issue that allowed users to log in to Casper Suite applications using LDAP credentials that are no longer correct.
- [D-004732] Fixed an issue that caused the JSS to incorrectly map the LDAP attribute for **Room** to **Department** and/or **Building** if those fields are blank or contain invalid mappings.

- [D-005045] Fixed an issue that caused the JSS to report a computer's management status inaccurately after upgrading to v9.0 or later.
- [D-005062] Fixed an issue that prevented the JSS from retaining existing static group memberships when adding new members from a filtered list.
- [D-005222] The JSS now includes "Asset Tag", "Do Not Disturb", and "Device Location" as display options for advanced mobile device searches and Inventory Display settings.
- [D-005233] Fixed an issue that caused the JSS to clear non-LDAP building and department values from computer inventory information when computers submit inventory and the JSS is configured to collect user and location information from LDAP.
- [D-005235] Fixed an issue that prevented the JSS from displaying results for an advanced search or smart group that is based on a building or department with an apostrophe (') in the name.
- [D-005326] Fixed an issue that caused the JSS to display the **Mobile Device Groups** pop-up menu when "Assign Usernames" is selected from the **Method** pop-up menu for classes.
- [D-005367] Fixed an issue that caused advanced searches and smart groups to incorrectly return all computers or mobile devices when based on an extension attribute that collects an integer.
- [D-005372] Fixed an issue that caused LDAP user group mapping tests to fail if the group name starts with one of the following special characters:

  # \ / +
- [D-005379] Fixed an issue that prevented the JSS from migrating OS X computer inventory after upgrading to the JSS v9.0 or later if Strict Mode is enabled in MySQL.
- [D-005394] The JSS API documentation is now consistent with the results of a query for a computer name.
- [D-005399] The JSS can now apply managed app configuration variables on more than one device.
- [D-005401] Fixed an issue that prevented the JSS from displaying extension attribute values when adding mobile devices to a static group.
- [D-005405] The JSS now returns computers when performing a simple search using an IP address as the search term.
- [D-005408] After performing a search for an LDAP group, the JSS now displays the name of the LDAP server that each group belongs to as well as the group name.
- [D-005414] Fixed an issue that caused the JSS to remove payloads from iOS configuration profiles and change the display name to "No Name" after adding devices to the scope or removing devices from the scope several times.
- [D-005416] Fixed an issue that caused the JSS to display an error when clicking smart groups from the JSS Dashboard.
- [D-005418] Fixed an issue that prevented the JSS from returning results of an advanced search for members of a smart group if the advanced search belongs to a site and the smart group does not.
- [D-005423] Fixed an issue that prevented the JSS from removing smart group criteria from the database when a smart group is deleted from the JSS.
- [D-005434] Inventory Display settings are now organized alphabetically.
- [D-005436] Fixed an issue that caused the **Log out users after** checkbox in a Login Window of an OS X configuration profile to be reselected after saving if it was deselected.
- [D-005441] Fixed an issue that allowed JSS users to view lists of advanced searches when they didn't have privileges to do so.

- [D-005442] Fixed an issue that prevented advanced mobile device searches from being accessible via the JSS API.

- [D-005465] Fixed an issue that prevented JSS web applications in clustered environments from completing some MDM commands, such as using Casper Focus, or setting a Managed App Configuration.

- [D-005480] JSS user accounts from Active Directory now work after deleting and re-adding the LDAP server in the JSS.

- [D-005493] Fixed an issue that prevented computers with a value of "null" for the "last_ip" database column from being migrated properly after upgrading the JSS to v9.0 or later if Strict Mode is enabled in MySQL.

- [D-005497] Fixed an issue that prevented the JSS from sorting static groups.

- [D-005499] Fixed an issue that caused upgrading to the JSS v9.0 or later to stall if the number of user IDs in the "user_roles" database column exceeds the max number of database connections.

- [D-005501] Static groups can now be accurately cloned after upgrading to v9.12.

- [D-005514] Fixed an issue that caused inaccurate static group membership when adding members to the group after upgrading to the JSS v9.0 or later.

- [D-005518] Fixed an issue that caused the JSS to send a mass email each time the **Next** button was clicked.

- [D-005522] Orphaned smart group criteria is now automatically removed from the database when upgrading v9.21 or later.

- [D-005533] Fixed an issue that caused duplicate mobile devices to be displayed in mobile device reports for the .txt and .csv file formats.

- [D-005544] Fixed an issue that prevented the JSS from installing an OS X configuration profile with the **Manually redirect recovery keys to specified URL** option. Also fixed an issue that caused the JSS to revert to the **Automatically redirect recovery keys to the JSS** option when the profile is saved.

- [D-005550] Fixed an issue that caused the JSS to return no mobile devices when performing an advanced search based on an extension attribute that collects a date.

- [D-005555], [D-005590] Fixed an issue that prevented the JSS from displaying the settings in the Restrictions, Parental Controls, and Security & Privacy payloads in OS X configuration profiles that were created using the JSS v9.12 or earlier.

- [D-005556] Fixed an issue that prevented the JSS from returning computers or mobile devices with a blank extension attribute value when performing an advanced search based on that extension attribute.

- [D-005559] The JSS now displays only managed mobile devices and computers as possible values for smart group criteria.

- [D-005578] Improved JSS performance by reducing the overhead of OS X `CertificateList` and `ProfileList` commands.

- [D-005579] The JSS no longer sends unnecessary MDM commands to a computer or mobile device after an MDM command fails.

- [D-005580] Improved the performance of the JSS by reducing the overhead of mobile device inventory requests.

- [D-005582] Fixed an issue that caused a blank Finder payload to be added to OS X configuration profiles with a Login Window payload. This caused the "Shut Down" and "Restart" options to be removed from the Apple menu on computer that installed the profile.

- [D-005584] The JSS now calculates scope more efficiently.
- [D-005585] Improved JSS performance by removing VPP code lookups during mobile device inventory updates.
- [D-005586] Improved JSS performance by looking up the scope and the archived app file (.ipa) state for mobile device apps all at once instead of individually.
- [D-005587] Improved JSS performance by ensuring that orphaned MDM commands are deleted.
- [D-005593] The JSS no longer allows you to click the **Save** button multiple times while creating smart computer groups. This could have resulted in duplicate criteria.
- [D-005594] The JSS no longer allows you to click the **Save** button multiple times while creating smart mobile device groups. This could have resulted in duplicate criteria.
- [D-005602] The JSS now includes the name of a mobile device in an email notification if the device was deleted from the JSS and belonged to a smart group.
- [D-005605] Improved the performance of multiple MySQL queries.
- [D-005642] Fixed an issue that caused the JSS to incorrectly map LDAP attributes that are in the octet string variable format.
- [D-005658] The JSS now displays an error for invalid XML communication via the JSS URL.
- [D-005691] Fixed an issue that caused a blank page to be displayed in Google Chrome when adding the "Last Enrollment" criteria to a smart group.
- [D-005708] Improved JSS performance for looking up classes with devices assigned by username.
- [D-005716] Fixed an issue that prevented the JSS from displaying extension attributes as options for criteria and display fields in advanced mobile device searches.

JSS Installer for Linux

Fixed in v9.21:

- [D-005226] Fixed an issue that could prevent the JSS Installer for Linux from upgrading the JSS to v9.0 or later if rsync is not installed on the server.
- [D-005610] Fixed an issue that prevented the JSS Installer for Linux from backing up and restoring the log4j.properties file when upgrading the JSS.

JSS Installer for OS X

Fixed in v9.21:

[D-005568] Fixed an issue that occurred when upgrading to v9.2 that caused the JSS Installer for Mac to replace the existing server.xml file with the default server.xml file if Tomcat was stopped before the upgrade. This issue also may have changed the SSL certificate used for HTTPS.

Recon

Fixed in 9.2:

- [D-005084] Fixed an issue that prevented Recon from connecting to the JSS after upgrading the JSS to v9.0 or later.
- [D-005303] Fixed an issue that prevented JSS users with site access from scanning a network segment using Recon.
- [D-005340] Fixed an issue that prevented Recon from creating QuickAdd packages when logged in to the computer with an Active Directory (AD) account.
- [D-005387] Fixed an issue that prevented Recon from displaying extension attributes on the User and Location pane.

Fixed in 9.21:

[D-005703] Fixed an issue that caused Recon to fail when authenticating to the JSS if the password contains one of the following special characters:

% &

Recon.exe

Fixed in 9.2:

[D-005084] Fixed an issue that prevented Recon.exe from connecting to the JSS after upgrading the JSS to v9.0 or later.

Fixed in 9.21:

[D-005571] Fixed an issue that prevented Recon.exe from populating user and location information from LDAP.

Self Service

Fixed in 9.21:

[D-004753] Self Service can now open in a web browser.

Known Issues

The following are known issues in the Casper Suite v9.21:

- The JSS fails to install an OS X configuration profile with a FileVault Recovery Key Redirection payload and the "Manually redirect recovery keys to specified URL" option. The JSS also reverts to the "Automatically redirect recovery keys to the JSS" option when the profile is saved.

- Disk encryption configurations fail to activate FileVault 2 on computers with Fusion Drives.

- OS X configuration profiles that require users to change their passwords after a specified number of days fail to prompt users to change their passwords.

- Newly enrolled OS X JDS instances do not immediately trust the SSL certificate if it was created from the JSS's built-in CA. This prevents the JDS instance from submitting inventory, and the JDS instance cannot be used until the SSL certificate is trusted. Trust is usually established within five minutes of enrollment.

- Installing an OS X configuration profile with a Login Window payload always disables automatic login on computers, regardless of whether or not the **Disable automatic login** checkbox is selected.

- 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.

- OS X configuration profiles that are configured to display a heading on the login window fail to do so.

- 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.

- When users try to access the Self Service web clip on an iOS 7 device, 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

- The jamf binary fails to install custom Adobe CS3/CS4 installations that were created using Casper Admin.