Casper Suite Release Notes

Version 9.25

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.

The Casper Suite v9.22 includes the following improvements:

- **OS X and iOS configuration profile improvements**—The JSS is now more consistent and reliable when installing configuration profiles.
- **JSS interface enhancements**—The JSS interface is now more consistent throughout and many of the columns in tables can now be resized.
- **JSS performance and stability improvements**—Continued improvements for more efficiency.
- **Administrative application enhancements**—Continued improvements for more reliability and efficiency.

The Casper Suite v9.23 includes the following improvements:

Recon efficiency and performance improvements—Computer inventory updates are now more efficient. In addition, improvements have been made to Recon for increased speed and performance.

Implemented Feature Requests

To view a complete list of feature requests that were implemented in v9.23, go to:

https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=56

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")	bus_speed_mhz
Mac processor speed	processor_speed	Integer value in MHz (e.g., "2260 MHz")	Integer value in MHz (e.g., "2314")	processor_speed_mhz
Mac total memory	total_ram	Integer value in MB (e.g., "2048 MB")	Integer value in MB (e.g., "2048")	total_ram_mb
Mac full internal drive size	size	String value in GB (e.g., "500.11 GB")	Integer value in MB (e.g., "512113")	drive_capacity_mb
Individual partition size				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")	cache_size_kb

Installation

Compatibility

The JSS v9.25 supports the following versions of client applications in the Casper Suite:

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

You can use any version of Composer and Casper Focus.

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 v9.25 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 v9.25 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) 6.4 or later
- 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 v9.25 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) or Windows Server 2012 (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. 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.

4. 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.

Removals

The local user authentication setting for Self Service has been removed from the JSS. You can no longer require users to authenticate locally before running Self Service policies.

Deprecations

The following functionality has been deprecated:

- **Policy status determined by checking script output for "error" and "fail"**—Historically, one of the ways the JSS has determined the status of a policy is by checking script output for the words "error" and "fail". As of v9.0, the JSS also uses exit codes to determine the status of a policy. This method is more reliable and accurate.

  Although the JSS v9.25 still checks script output for the words "error" or "fail", this will be removed in a future version. If you have written scripts that utilize this feature, consider implementing an alternative solution using exit codes as soon as possible.

- **Clear-text and masked password fields in the JSS Rest API**—Clear-text and masked password fields in the JSS Rest API have been deprecated and will be removed in a future version. Accordingly, new fields have been added that contain the MD5 and SHA-256 hashed versions of those fields.

  If you have any processes or applications that read clear-text or masked passwords from the JSS Rest API, consider implementing the MD5 or SHA-256 versions of those fields as soon as possible.

If you need assistance with the transition to new functionality, or if you have questions or concerns, contact your JAMF Software Account Manager.

Bug Fixes and Enhancements

Casper Admin

Fixed in v9.2:

[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 v9.21:

- [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.

Fixed in v9.23:

[D-006029] OS X v10.9 upgrades deployed using the .app file from the Mac App Store and the policy framework no longer require user interaction on computers with a Europe time zone.

[D-006245] Fixed an issue that prevented Casper Admin from replicating files from a JDS instance to a cloud distribution point.

Casper Focus

Fixed in v9.21:

- [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.

Fixed in v9.23:

[D-005798] Fixed an issue that caused the username text to overlap when logging in to Casper Focus in French, German, or Spanish.

Casper Imaging

Fixed in v9.2:

- [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 v9.21:

- [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.

Fixed in v9.22:

- [D-005762] Fixed an issue that caused Casper Imaging to attempt to enroll a computer twice if there are imaging tasks that must be complete after reboot using a PostInstall script.
- [D-005896] Fixed an issue that caused the PostInstall script to delete the "adobeinstall" user after installing packages that were configured to be installed on the boot drive after imaging, but before running scripts with a priority of "At Reboot".

Fixed in v9.23:

[D-006001] Fixed an issue that caused Casper Imaging to incorrectly create a third partition on a smart configuration that is two or more levels below a top-level configuration with two partitions.

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.

Fixed in v9.22:

[D-005847] Casper Remote no longer allows a user that does not have the Run Scripts Remotely privilege to access scripts.

Composer

Fixed in v9.21:

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

Fixed in v9.22:

[D-005723] Fixed an issue that caused an Active Directory (AD) account to be locked when using Composer while logged in to an OS X v10.9 computer with the account.

Fixed in v9.23:

- [D-005911] Fixed an issue that prevented Composer from capturing the background of a currently logged in user on a computer with OS X v10.9 when using the Desktop Pattern package manifest.
- [D-006072] Fixed an issue that prevented Composer from capturing clock settings for the menu bar on a computer with OS X v10.9 when using the Menu Bar Items package manifest.

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.

Fixed in v9.22:

- [D-003325] Fixed an issue that prevented the jamf binary from removing EFI passwords.
- [D-004010] The jamf binary now kills the JAMF Helper process after running policies with a logout trigger.
- [D-004048] Fixed an issue that caused Self Service to remain on a computer after the `sudo jamf removeFramework` command is executed.
- [D-005608] The jamf binary now submits policy logs after checking the JSS connection instead of before.
- [D-005621] The jamf binary now generates random passwords more securely.
- [D-005633] The jamf binary no longer collects inventory information for plug-ins installed in non-default locations unless the locations are specified in the Computer Inventory Collection settings.
- [D-005751] Fixed an issue that prevented computers from downloading files over HTTP(S) from file share distribution points that use digest authentication.

- [D-005763] Fixed an issue that prevented a computer from communicating with the JSS after attempting to enroll the computer twice using the same invitation.
- [D-005875] Fixed an issue that prevented the JSS from reporting that a package was cached after successfully caching the package using a policy or Casper Remote.
- [D-005938] The `mdm.mobileconfig` and the `JAMFTMP.keychain` files are now stored in a secure location.

Fixed in v9.23:
- [D-005880] The jamf binary now reports the display name of the package that is being cached when caching a package using a policy.
- [D-005953] Temporary FileVault 2 files are now stored in a secure location during deferred enablement.
- [D-005960] Fixed an issue that caused policies configured to issue a FileVault 2 institutional recovery key to fail on computers that are configured to have an individual recovery key.
- [D-005978] Fixed an issue that prevented the jamf binary from updating disk encryption configuration information on computers that have an institutional recovery key when they are in the scope of a policy configured to deploy a configuration that issues a new institutional recovery key.
- [D-006002] Fixed an issue that prevented policies that were previously deferred from being available again if a computer is re-enrolled with the JSS before the chosen policy deferral time has elapsed.
- [D-006103] Fixed an issue that prevented the jamf binary from removing the local copy of a cached package from a computer after the package is installed if it is a compressed PKG or MPKG that is installed using a policy.
- [D-006158] Fixed an issue that caused the `/Library/Application Support/JAMF/tmp` directory to remain on a computer after the `sudo jamf removeFramework` command is executed.

JAMF Distribution Server

Fixed in v9.22:
- [D-005729] Fixed an issue that caused JDS instances to submit inaccurate hard drive sizes to the JSS.
- [D-005991] The JDS Installer for Linux (.run) now supports the latest version of Red Hat Enterprise Linux (RHEL).

Fixed in v9.23:

[D-005596] Casper Admin and Casper Imaging can now mount a JDS instance on computers with OS X v10.9 or v10.9.1 after completing the instructions in the following Knowledge Base article:

Troubleshooting JAMF Distribution Server (JDS) Connection Issues on OS X v10.9 and v10.9.1

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.

Fixed in v9.22:

- [D-004067] 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.

- [D-004457] Fixed an issue that caused the JSS to display extra space above the PKI settings and the JDS settings in read view.

- [D-004877] Fixed an issue that caused the JSS to display overlapping text when viewing inventory information using a smartphone or an iPod touch.

- [D-004922] The JSS now displays the **Set System Wide** option for software update servers.

- [D-004927] The columns in inventory search results can now be resized.

- [D-004929] The JSS now allows duplicate names for all objects.

- [D-004942] Fixed an issue that prevented the JSS from automatically displaying the Policy pane after flushing all logs from a policy.

- [D-005007] Fixed an issue that prevented the JSS from sorting mobile device enrollment invitations based on last action.

- [D-005155] The JSS now displays the correct German translation for the display name in a configuration profile.

- [D-005172] Fixed an issue that caused the JSS to change the order of teacher usernames when saving a class.

- [D-005214], [D-005483] Fixed an issue that prevented the JSS from properly enabling or disabling app settings when adding a managed App Store app and deselecting the **Free** checkbox or selecting "Prompt User to Install" from the **Distribution Method** pop-up menu.

- [D-005221] The JSS no longer requires a domain in the Exchange payload of an OS X configuration profile.

- [D-005231] Fixed an issue that prevented the JSS from verifying certain parameters in the JSS URL.

- [D-005251] Self Service no longer uses hardcoded encryption keys.

- [D-005283] Fixed an issue that prevented the JSS from saving packages and scripts in policies created using Safari on OS X v10.6.8.
- [D-005294] App icons are now associated with the correct apps in the Self Service web clip if there were multiple icons with the same filename when the JSS was upgraded to v9.0 or later.
- [D-005312] The JSS now displays a progress indicator when loading policies, configuration profiles, and Managed Preference profiles.
- [D-005373] Sending two Unmanage Device remote commands to a mobile device now forces it to be unmanaged.
- [D-005412] The assistant for creating a push certificate now displays the Apple Push Certificate Portal.
- [D-005420] Fixed an issue that prevented the JSS from installing unmanaged, free App Store apps on iOS 5 devices.
- [D-005458] The JSS now allows you to remove the Energy Saver payload from an OS X configuration profile.
- [D-005475] Fixed an issue that prevented the JSS from cloning iOS configuration profiles with a Wi-Fi payload.
- [D-005481] Fixed an issue that caused the JSS to incorrectly add network segments as exclusions when the network segments were configured as limitations for the scope of a policy.
- [D-005500] The JSS now allows you to use parentheses to group criteria that are connected by "or" when editing a smart group.
- [D-005505] Fixed an issue that allowed JSS users with no privileges to access the JSS Summary settings.
- [D-005512] Fixed an issue that prevented the JSS from respecting exclusions in the scope of an OS X configuration profile with a Restrictions payload that restricts items in System Preferences.
- [D-005540] Fixed an issue that prevented the JSS from installing OS X configuration profiles with a Parental Controls payload that enforces time limits.
- [D-005553] Fixed an issue that disabled the ability to burn CDs or DVDs on the computer after using the JSS to deploy an OS X configuration profile with a Restrictions payload.
- [D-005562] Devices can now be removed from the scope of a signed iOS configuration profile that was uploaded to the JSS.
- [D-005564] Fixed an issue that caused OS X configuration profiles configured to create a portable home directory using a local home template to result in one that was created using a network home and default sync settings.
- [D-005611] Fixed an issue that prevented pop-up menus from displaying the choices when the pop-up menu is clicked before the page loads.
- [D-005616] Fixed an issue that prevented the jamf binary from installing custom Adobe CS3/CS4 installations that were created using Casper Admin.
- [D-005628] Fixed an issue that caused the JSS to initiate the "Back" action when typing "b" into the Filter Results field when viewing logs for a single policy.
- [D-005630] Fixed an issue that prevented configuration profiles from migrating properly when upgrading the JSS to v9.0 or later if one or more of them contain international characters.
- [D-005634] Fixed an issue that prevented the JSS from uninstalling iOS configuration profiles from all mobile devices in a group when the group is removed from the scope of the profile.
- [D-005644] Fixed an issue that prevented the JSS from adding trusted server certificate names to OS X configuration profiles with a Network payload and an Ethernet network interface.

- [D-005656] Fixed an issue that prevented the JSS from using the most restrictive network segment when a computer belongs to multiple network segments.

- [D-005690] Clicking the **Back** button on the Complete pane of the LDAP Server Assistant now takes the user back to the Test Group pane.

- [D-005709] Fixed an issue that prevented the JSS from installing OS X configuration profiles with a Security & Privacy payload on OS X v10.9 computers.

- [D-005717] Fixed an issue that prevented the JSS from saving the **Challenge Type** setting in the SCEP payload of an OS X configuration profile.

- [D-005732] The JSS now queries computer hardware and software history more efficiently.

- [D-005754] Fixed an issue that prevented the username and password fields in the Self Service web clip from fitting the page on mobile devices when the web clip is configured to require users to log in.

- [D-005756] The JSS API now accepts extension attribute values from the JSS v8.x.

- [D-005760] Fixed an issue that caused all but the last extension attribute in a list of two or more to display a blank value in inventory information if the extension attributes were updated via the JSS API.

- [D-005764] Fixed an issue that allowed JDS instances to be enrolled using computer invitations.

- [D-005772] The JSS now installs a configuration profile more efficiently when distributing the profile to more than one mobile device or computer.

- [D-005773] The JSS now queries smart groups based on extension attributes more efficiently.

- [D-005774] The JSS now updates inventory more efficiently after the `jamf manage` command is executed.

- [D-005775] The JSS now displays policy logs more efficiently.

- [D-005777] Fixed an issue that caused LDAP user group lookups to fail if the user does not belong to the user group search base.

- [D-005790] The JSS now updates inventory more efficiently after distributing MDM profiles.

- [D-005791] The JSS now updates inventory more efficiently after running the Wipe Computer remote command.

- [D-005792] The JSS now updates inventory more efficiently after running the Wipe Computer remote command and the Remove MDM Profile remote command.

- [D-005793] The JSS now updates inventory more efficiently after running a policy that contains a Management Account payload.

- [D-005794] The JSS now updates inventory more efficiently after Managed Preference profiles are updated.

- [D-005795] The JSS now updates inventory more efficiently after submitting a FileVault 2 recovery key.

- [D-005807] Fixed an issue that prevented computers from requiring a password after sleep or screen saver begins when using the JSS to install an OS X configuration profile with a Login Window payload.

- [D-005808] Fixed an issue that prevented OS X configuration profiles with a Login Item payload that included a blank Item from saving correctly.

- [D-005810] Fixed an issue that caused the JSS to unnecessarily execute some MySQL queries more than once for each Casper Focus command.

- [D-005811] The JSS now updates inventory more efficiently after the `jamf recon` command is executed.

- [D-005813] Fixed an issue that caused the JSS to execute unnecessary MySQL queries for VPP codes.

- [D-005814] Fixed an issue that caused the JSS to create updateInventory MDM commands for unmanaged mobile devices.
- [D-005815] Fixed an issue that prevented other payloads from being added or removed in an OS X configuration profile with a Per-App VPN payload.
- [D-005816] The JSS no longer allows a user with the Auditor privilege set to create a certificate from a CSR.
- [D-005820] The JSS now displays the certificate subject names when viewing issued certificates in the PKI settings.
- [D-005821] MySQL query warnings are now included in the `jamfsoftwareserver.log` file.
- [D-005823] The JSS now performs nested queries more efficiently.
- [D-005824] The JSS now distributes configuration profiles more efficiently.
- [D-005825] Fixed an issue that temporarily removed all failed commands from the management information in the JSS if there were multiple failed management commands and one command was canceled.
- [D-005848] The JSS now specifies that the **Allow modifying account settings** and **Allow modifying Find My Friends settings** options in the Restrictions payload in iOS configuration profiles only work for supervised devices.
- [D-005861] Fixed an issue that caused the JSS to change the criteria connectors of smart groups from "or" to "and".
- [D-005874] Fixed an issue that caused the RemoveProfile MDM command to run repeatedly after removing computers or mobile devices from the scope of a signed configuration profile from which the signature had been removed.
- [D-005876] The JSS now updates inventory more efficiently after running a policy on a computer with an out-of-date binary.
- [D-005881] The JSS now loads the History tab in computer inventory information more efficiently.
- [D-005886] The JSS now correctly updates queries for group membership when a computer or mobile device becomes unmanaged.
- [D-005887] The JSS no longer allows enrollment profiles to be uploaded as configuration profiles.
- [D-005889] The JSS now creates static groups more efficiently when logged in with a JSS user account that has site access, or has full access and is viewing a specific site.
- [D-005890] The JSS now displays a warning message when the **Database Table Status** button is clicked in JSS information warning that the JSS could become unresponsive.
- [D-005904] The JSS no longer incorrectly specifies that the **Allow adult content in iBookstore** option in the Restrictions payload in iOS configuration profiles only works for supervised devices.
- [D-005905] Fixed an issue that prevented the JSS from differentiating between two apps with different versions. This prevented the apps from being installed on mobile devices.
- [D-005909] Fixed an issue that prevented the JSS from enrolling computers imaged with Target Mode Imaging.
- [D-005932] Fixed an issue that prevented computers and mobile devices from being added to groups using the API.
- [D-005944] The columns in the custom search path tables in Computer Inventory Collection settings can now be resized.
- [D-005945] Apps are now displayed in alphabetical order in the Self Service web clip.

- [D-005949] The JSS no longer loads attachments and icons into memory until needed.
- [D-005972] Fixed an issue that caused the JSS to flush all logs when flushing just the policy logs in a computer's inventory information.
- [D-005974] Fixed an issue that caused duplicate configuration profiles after updating a configuration profile via the API.
- [D-005986] The JSS now removes attachments and icons from memory when they are no longer needed.

Fixed in v9.23:

- [D-004585] Enrollment profiles created using the JSS now retain their display name when imported to Apple Configurator or iPCU.
- [D-005021] Fixed an issue that caused the JSS to allow all mobile devices in the full JSS to be added to the scope of a new app or eBook that is created by a JSS user with site access.
- [D-005214], [D-005483] Fixed an issue that prevented the JSS from properly enabling or disabling app settings when adding a managed App Store app and deselecting the **Free** checkbox or selecting "Prompt User to Install" from the **Distribution Method** pop-up menu.
- [D-005381] Fixed an issue that caused the Self Service web clip to continue displaying a status of "Pending" for an iOS configuration profile even after the profile is installed.
- [D-005393] Fixed an issue that prevented the JSS from replacing a user's privileges with a user group's privileges when the user is added to a user group.
- [D-005406] Self Service now correctly opens as a web clip instead of opening in Safari when users access the Self Service web clip on a mobile device with iOS 7.0.3 or later.
- [D-005417] Fixed an issue that prevented the JSS from setting a default printer using an OS X configuration profile.
- [D-005530] Fixed an issue that prevented the JSS from populating the site in inventory information for a computer or mobile device that is enrolled via user-initiated enrollment by a JSS user with site access.
- [D-005551] Fixed an issue that permitted a JSS user with site access to add items to any site using the JSS API.
- [D-005588] Fixed an issue that caused the JSS to send unnecessary DeviceInformation MDM commands to mobile devices that were previously assigned to a class and then became unmanaged.
- [D-005607], [D-005879], [D-005912], [D-006106] The JSS now returns correctly formatted JSON responses from the JSS API.
- [D-005647], [D-005660] Updated the Restlet Framework to the latest version to make the JSS Rest API more secure.
- [D-005654] Fixed an issue that prevented the JSS from applying the **Restrict App Store to software updates only** option in the Restrictions payload in OS X configuration profiles.
- [D-005662], [D-005663], [D-005664], [D-005684] Fixed an issue that caused the JSS Rest API to disclose clear-text passwords for some JSS objects.
- [D-005688] Fixed an issue that caused user-initiated enrollment for computers to fail when using a JSS user account that belongs to a group with administrator privileges to a site, and another group with auditor privileges for the full JSS.
- [D-005771] Fixed an issue that caused the JSS to assign the same UUID to multiple commands when processing MDM commands for more than one mobile device or computer.

- [D-005803] Fixed an issue that prevented the JSS API from displaying information about the peripherals assigned to a computer.
- [D-005827] Fixed an issue that prevented the JSS from saving mobile device attachments after re-enrolling a device using Apple Configurator.
- [D-005852] The JSS now includes an option in User-Initiated Enrollment settings for computers that allows you to randomly generate a management account password for each newly enrolled computer.
- [D-005925] Fixed an issue that prevented the JSS from dynamically populating the policy restart message with the amount of time specified in the **Delay** field in the Restart Options payload for the policy.
- [D-005947] Improved JSS performance when refreshing the JSS Dashboard.
- [D-005971] The JSS no longer allows a user with the Auditor privilege set to manually flush logs.
- [D-005975] Fixed an issue that prevented the JSS from retaining all criteria on the page when attempting to save a smart group or advanced search that uses parentheses to group criteria but is missing either the opening or closing parenthesis.
- [D-005988] The JSS now displays an error when attempting to save a policy, Self Service Plug-in, app, or eBook that includes an uploaded icon with a file size that is too large to be saved.
- [D-006000] Fixed an issue that prevented the JSS from saving the magnification setting in a Dock payload of an OS X configuration profile.
- [D-006004] Fixed an issue that caused the Self Service web clip to continue displaying a **Pending** button for a mobile device app even after the app has been successfully installed. This allowed users to tap the button continually and restart the app installation multiple times.
- [D-006005] Fixed an issue that prevented the JSS from respecting changes to policy settings for trigger and execution frequency if the changes were made using the JSS API.
- [D-006006] Fixed an issue that caused the JSS to display an error when changing the password from the User menu.
- [D-006014] The JSS now includes a **Restrict re-enrollment to authorized users only** checkbox in User-Initiated Enrollment settings for both computers and mobile devices. If this checkbox is selected, users can only re-enroll a computer or mobile device if one of the following conditions is met:
  - The user has the "Computers" privilege (to re-enroll a computer)
  - The user has the "Mobile Devices" privilege (to re-enroll a mobile device)
  - The username of the user re-enrolling the computer or mobile device matches the **Username** field in the User and Location category in inventory information
  - The **Username** field in the User and Location category in inventory information is blank

  This checkbox applies only to re-enrollment; it does not apply to first-time enrollment of a computer or mobile device.
- [D-006018] Fixed an issue that prevented the JSS from installing user-level OS X configuration profiles with an AD Certificate payload on OS X v10.9 computers.
- [D-006036] Fixed an issue that caused mobile devices and computers in a clustered environment to install a newly created configuration profile from an incorrect site if they contact or check in with the JSS before the other web applications in the cluster become aware that the configuration profile belongs to a site.
- [D-006048] Fixed an issue that prevented a user with the Auditor privilege set from viewing logs for a computer.

- [D-006049] Fixed an issue that caused the JSS to incorrectly exclude some MacBook Air models from smart group memberships if the smart group is based on Model criteria using the model identifier (e.g., "MacBookAir6,1") instead of the model format displayed in computer inventory information (e.g., "MacBook Air (11-inch Mid 2013)").

- [D-006050], [D-006051], [D-006052] Fixed an issue that prevented the JSS from properly saving some OS X configuration profiles with a Network payload and an Ethernet interface. Also updated the network Ethernet settings for Accepted EAP Types and removed the **EAP-SIM** option.

- [D-006059] The JSS now calculates group membership more efficiently for nested smart groups.

- [D-006065] Fixed an issue that prevented the JSS from allowing site administrators to change their password.

- [D-006066] Fixed an issue that prevented the JSS from immediately updating smart group memberships that are based on an extension attribute populated using a pop-up menu if the value of the extension attribute is changed in inventory information.

- [D-006083] The JSS API now includes a computer_id field for peripherals.

- [D-006086] Fixed an issue that prevented computer-level OS X configuration profiles with a Network payload and Wi-Fi interface from saving properly if the security type is set to "WPA2 Enterprise".

- [D-006090] Fixed an issue that prevented the JSS from applying the 802.1X network authentication credentials specified in OS X configuration profiles with a Network payload.

- [D-006092] Fixed an issue that caused a blank page to be displayed when configuring PKI settings for an external CA and attempting to upload a CA certificate bundle for an additional CA using the assistant.

- [D-006102] Fixed an issue that prevented asset tags from being assigned to mobile devices using the JSS API.

- [D-006105] The JSS no longer completely deletes FileVault 2 individual recovery keys from the jamfsoftware database after a computer is decrypted and then submits an inventory update.

- [D-006141] Fixed an issue that caused the JSS to remove a Certificate payload from an OS X configuration profile if the payload includes a certificate in .p12 format and the profile (.mobileconfig) is downloaded from the JSS, deleted from the JSS, and then re-uploaded to the JSS.

- [D-006143] Fixed an issue that prevented the JSS in a clustered environment from displaying extension attributes as criteria in an advanced search on any JSS instance other than the JSS instance that the attributes were created on.

- [D-006144] Fixed an issue that prevented computers from being added to the JSS using the JSS API if the hard drive size value includes the terabyte (TB) unit of measure.

- [D-006165] The JSS now allows you to choose a certificate type of "Client Certificate" or "Web Server Certificate" when creating a certificate using a Certificate Signing Request (CSR) in the PKI settings.

- [D-006178] The JSS now correctly replaces the $USERNAME payload variable in a user-level OS X configuration profile with the username of the user logging in to the computer on which the profile is installed.

- [D-006211] Fixed an issue that prevented the JSS from enrolling mobile devices if the PKI settings are configured with an external CA.

- [D-006213] Fixed an issue that prevented the JSS from updating inventory for a computer if the computer's FileVault 2 status is not properly detected.

- [D-006214] Fixed an issue that prevented the JSS API from sending remote commands to mobile devices.

- [D-006215] The JSS API now accepts duplicate names for mobile devices.
- [D-006264] The JSS no longer allows the **Distribute to All** or **Distribute to New** buttons to be clicked multiple times after editing and saving a configuration profile. This could have resulted in the configuration profile settings being wiped.

Fixed in v9.24:

- [D-006031] Fixed an issue that prevented the JSS from loading policies when the JSS is running on Tomcat 6.0.
- [D-006321] Fixed an issue that prevented the JSS from installing OS X configuration profiles with a Network payload and a Wi-Fi network interface.

Fixed in v9.25:

- [D-006388] Improved JSS performance by no longer requiring Self Service web clip installation and inventory updates for every MDM token update.
- [D-006412] Fixed an issue that caused supervised mobile devices to be displayed as unsupervised in inventory after updating mobile devices using the JSS API.
- [D-006513] Fixed an issue that caused User and Location inventory information to be reset for a mobile device when upgrading to iOS 7.1 if the device was enrolled with a profile that used the **Create profile for use with iPCU** option.

JSS Database Utility

Fixed in v9.23:

[D-005403] Fixed an issue that caused the JSS Database Utility to always display a Maximum Memory Pool value of 512 MB regardless of the selected value when using the JSS Database Utility to set memory settings for Tomcat on Windows Server 2008.

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.

Fixed in v9.23:

- [D-006035] Fixed an issue that prevented the JSS Installer for Linux from successfully executing management commands for Tomcat 6.0 using the `service jamf.tomcat7` command.

Fixed in v9.25:

- [D-006351] Fixed an issue that prevented the JSS Installer for Linux from creating a `/temp/` directory in `/usr/local/jss/tomcat/` on Red Hat Enterprise Linux (RHEL).

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 v9.2:

- [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 v9.21:

[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:

% &

Fixed in v9.22:

[D-005898] Fixed an issue that caused client applications to crash when parsing large quantities of data.

Fixed in v9.23:

[D-005247] Updated the libssh library to the latest version to make Recon more secure.

Recon.exe

Fixed in v9.2:

[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 v9.21:

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

Self Service

Fixed in v9.21:

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

Fixed in v9.22:

[D-005028] Fixed an issue that prevented policies from displaying in Self Service.

Fixed in v9.23:

- [D-005625] Fixed an issue that caused a cross-site scripting (XSS) vulnerability of the search function in Self Service.
- [D-005849] Fixed an issue that prevented a policy from displaying in Self Service if the policy has an Ethernet limitation and Self Service is configured to require or allow login with an LDAP account.
- [D-006053] Fixed an issue that prevented policies from running on OS X v10.9 computers if the policy was made available in Self Service and it included a package or script that runs an application requiring access to the user account.
- [D-006057], [D-006039] Fixed an issue that caused policies with the Restart Options payload to fail when they are made available in Self Service.
- [D-006067] Fixed an issue that prevented a printer from immediately displaying in System Preferences if the printer is mapped using a policy that is made available in Self Service. Also fixed an issue that caused any existing printers to temporarily disappear from System Preferences after a printer is mapped to a computer using a policy that is made available in Self Service.
- [D-006068] Fixed an issue that prevented Self Service from running subsequent policies after running a policy that contains a script that executes a `jamf manage` command.
- [D-006069] Fixed an issue that sometimes prevented Self Service from displaying the sidebar.
- [D-006074] Self Service now correctly displays the webpage for a URL plug-in if "http://" is not included in the **URL** field for the URL plug-in.
- [D-006112] Fixed an issue that prevented Self Service from running on computers with OS X v10.5.8.
- [D-006191] Self Service now prompts users to try running a policy again if the policy fails because communication between Self Service and the jamf binary has timed out.

Known Issues

The following are known issues in the Casper Suite v9.25:

- 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.

- 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 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

- The JSS fails to install configuration profiles with a Web Clip payload on computers with OS X v10.9.

- Casper Focus crashes on iPads connected to a Bluetooth keyboard if the escape key is pressed.

- 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.

- iOS configuration profiles with a Single App Mode payload fail to lock mobile devices to an app if the devices have a passcode and have been turned off and then back on.

- OS X configuration profiles with an Energy Saver payload set incorrect startup and shutdown times on OS X v10.8 computers.

- Activity Monitor incorrectly shows that the jamfAgent process is not responding on managed computers with OS X v10.9.

- Some settings in the Security & Privacy payload of an OS X configuration profile are not applied.

- Casper Admin fails to compile configurations if the master distribution point is a file share distribution point hosted on Windows Server.

- 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".

- Casper Focus sometimes fails to focus mobile devices on an app when the devices are restarted after being focused on the app.

- 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.

- An error is displayed if a user logs in to a managed computer with a mobile account and the computer is bound to Active Directory, and the login takes several minutes.
- 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