Casper Suite Release Notes

Version 9.32

JAMF software

JAMF Software has made all efforts to ensure that this guide is accurate.

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

Contents

4 What's New in This Release
4 Key Features
5 Implemented Feature Requests

7 Installation
7 Compatibility
7 Upgrading the JSS
10 Upgrading to OS X Server v10.9

10 Removals

11 Deprecations

12 Bug Fixes and Enhancements

12 Casper Admin
12 Casper Focus
12 Casper Imaging
13 Casper Remote
13 Composer
13 jamf binary
14 JAMF Distribution Server
14 JAMF Helper
14 JAMF Software Server
20 JSS Database Utility
20 JSS Installer for Linux
20 JSS Installer for Windows
20 Recon
21 Self Service

22 Known Issues

What's New in This Release

Key Features

The Casper Suite v9.3 includes the following key features:

- **User Management**—The JSS now allows you to view and manage user inventory information.
- **VPP-Managed Distribution**—Apps and eBooks purchased through Apple's Volume Purchase Program (VPP) can now be assigned to users for VPP-managed distribution.
- **Device Enrollment Program**—After the JSS is integrated with the Apple Device Enrollment Program, you can use the JSS to configure enrollment and setup settings for mobile devices and computers using a PreStage enrollment. In addition, you can use PreStage enrollments to customize the user experience of the Setup Assistant.
- **Casper Focus enhancements**—Casper Focus updates include a redesigned interface and the ability to focus mobile devices on a website. In addition, you can now exclude a device from a class temporarily if you do not want the device to receive focus actions.
- **Activation Lock Bypass support**—When viewing management information for a mobile device, you can now view the Activation Lock bypass code for the mobile device. The Activation Lock bypass code can be used to bypass the Activation Lock associated with a mobile device.
- **Apple Configurator Enrollment**—You can enroll mobile devices with the JSS by connecting them to a computer via USB and using Apple Configurator, an enrollment URL, and an anchor certificate that you download from the JSS.
- **Improved connection speeds for Casper Remote**—To improve connection speeds, Casper Remote will first attempt to contact a computer using the computer's reported IP address. The IP address reported by Tomcat will be used as the failover.
- **Security enhancements**—Options have been added for validating software distribution packages using checksum. In addition, user-initiated re-enrollment of computers can now be restricted to authorized users.

The Casper Suite v9.31 includes the following key features:

- **User Reporting**—The JSS now allows you to create advanced user searches to give you more control over your search. You can also export data displayed in smart or static group membership lists and user search results.
- **Content Reporting**—The JSS now allows you to create simple content searches to search the mobile device apps, Mac App Store apps, and eBooks in your inventory for a general range of results, and advanced content searches to give you more control over your search. You can also export data displayed in content search results.
- **Account Preferences**—Language, date format, and search preferences can be configured for each JSS account.
- **JSS Object History**—The JSS allows you to view the history of changes made to each JSS object using v9.31 or later. History information includes the date/time the JSS object was created or edited, the username of the administrator who made the change, and notes associated with the changes.
- **Activation Lock enhancements**—Organization-owned devices that are managed by the Casper Suite, are supervised, and have the Activation Lock bypass code saved in the JSS will be able to receive a command which allows end users to enable Activation Lock.

- **Customer Experience Metrics**—As part of JAMF Software's effort to continuously improve the Casper Suite, anonymous usage data will be collected from organizations that enable Customer Experience Metrics.

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

  For additional information, visit the following webpage:

  http://www.jamfsoftware.com/products/casper-suite/customer-experience-metrics/
- **Mass Actions for mobile devices and computers**—Expanded functionality allows remote commands to be sent to any group of devices or to the search results of devices in the JSS inventory.
- **Device Enrollment Program and VPP technical paper**—This technical paper explains how to use Apple's Device Enrollment Program and VPP-managed distribution to easily set up and enroll devices with the JSS so that an administrator can deploy and manage apps and eBooks.

  You can download it from:

  http://www.jamfsoftware.com/resources/deploying-devices-with-the-device-enrollment-program-vpp-managed-distribution-and-the-casper-suite/

Note: Privileges associated with new Casper Suite features will be disabled by default. To use a new feature, you must enable the corresponding privileges.

The Casper Suite v9.32 includes the following key features:

- **User Extension Attributes**—The JSS now allows you to collect data from users by creating user extension attributes.
- **Activation Lock enhancements**—When viewing management information for a mobile device, you can now clear the Activation Lock when sending a Wipe Device command.
- **VPP registration enhancements**—VPP invitations sent via email now include an optional user login requirement.

Implemented Feature Requests

To view a complete list of feature requests that were implemented in v9.32, go to:
https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=70

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 Individual partition size	size	String value in GB (e.g., "500.11 GB")	Integer value in MB (e.g., "512113")	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")	cache_size_kb

Installation

Compatibility

The JSS v9.32 supports the following versions of client applications in the Casper Suite:

- Casper Admin v9.3 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 v9.32 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 v9.32 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 12.04 LTS Server (64-bit)
  - Ubuntu 14.04 LTS Server (64-bit)
  - Red Hat Enterprise Linux (RHEL) 6.4 or later
- Open Java Development Kit (OpenJDK) 6 or 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 v9.32 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.

After You Upgrade

After you upgrade, consider the following:

- **Migrating Users**—If you have upgraded from the Casper Suite v9.2x or earlier and want to integrate with VPP and utilize the **Users** tab, you must first complete the user migration process. This creates user inventory from the existing user information in computer and mobile device inventory.

  For more information, see the following Knowledge Base article:

  Migrating Users
- **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

- **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 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.

  For detailed instructions, see the following Knowledge Base article:

  Distributing Updated MDM Profiles
- **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.

  For detailed instructions, see the following Knowledge Base article:

  Certificate-Based Authentication for OS X Computers

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 v9.32 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 v9.3:

- [D-005693] Fixed an issue that prevented Casper Admin from appearing on the primary display after disconnecting from an external display on which it has been viewed.

Fixed in v9.31:

- [D-006274] Fixed an issue that caused Casper Admin to display some DMGs in incorrect categories.
- [D-006516] Fixed an issue that prevented Casper Admin from selecting all text entered in the **Filter** field using the Command-A keyboard shortcut.
- [D-006666] Fixed an issue that caused Casper Admin to close after two failed connection attempts when opening Casper Admin and authenticating to the JSS.
- [D-006799] Fixed an issue that prevented the JSS from storing the checksum when using Casper Admin to add a package to a file share distribution point.

Casper Focus

Fixed in v9.3:

- [D-005906] Fixed an issue that sometimes caused Casper Focus to display an error on a student device when app focus is removed.

Casper Imaging

Fixed in v9.3:

- [D-006316] Fixed an issue that prevented smart configurations two or more levels below a top-level configuration from inheriting settings from the top-level configuration.
- [D-006498] Fixed an issue that prevented the application version number and icon from displaying in the Finder for Casper Imaging and Casper Remote.

Fixed in v9.31:

- [D-006431] Fixed an issue that sometimes prevented Casper Imaging from completing the imaging process, resulting in "Connection failure" errors and a "Valid Device Signature is required" error displayed in the `jamf.log`.
- [D-006514] The JSS now allows site administrators to delete computer inventory records if an error occurs when enrolling computers imaged with an Imaging PreStage.
- [D-006580] Fixed an issue that prevented Casper Imaging from immediately booting to the target drive after imaging if booting to an OS X v10.9 computer.
- [D-006663] Fixed an issue that prevented Casper Imaging from imaging computers using a configuration when the configuration name includes either of the following special characters:

  / :

Fixed in v9.32:

- [D-006809] Fixed an issue that caused Casper Imaging to incorrectly create and install management items on a computer before the computer is enrolled.

Casper Remote

Fixed in v9.3:

- [D-005744] Fixed an issue that prevented Casper Remote from sharing the screen of an OS X v10.9 computer when using the "Log In" screen sharing option.
- [D-006196] Fixed an issue that prevented Casper Remote from using a computer's secondary IP address to contact the computer if attempts to contact the computer using the computer's primary IP address fail.

Fixed in v9.31:

[D-006420] Fixed an issue that caused Casper Remote to switch 12:xx a.m. and 12:xx p.m., causing an incorrect countdown time when running scheduled tasks.

Composer

Fixed in v9.31:

- [D-006262] Fixed an issue that sometimes prevented Composer from building DMG packages using a snapshot.
- [D-006698] Fixed an issue that caused Composer to display an incorrect package size when building a package source by dragging an OS package to Composer.

Fixed in v9.32

- [D-006344] Fixed an issue that sometimes caused Composer to fail to create a package source from a QuickAdd package.

jamf binary

Fixed in v9.3:

- D-006088] Fixed an issue that caused errors to be written repeatedly to the `jamfsoftwareserver.log` file when a v8.x jamf binary attempts to upload a cached policy log to a v9.x JSS.
- [D-006091] Fixed an issue that prevented the jamf binary from encrypting OS X v10.8.5 computers using a Self Service policy if the enabled FileVault 2 user is the management account.
- [D-006220] Fixed an issue that prevented the jamf binary from creating the `/Downloads/` and `/Documents/` directories when using a policy or Casper Remote to create a local account on a computer with OS X v10.9.
- [D-006283] Fixed an issue that caused application usage information to be lost for applications running during computer inventory updates.

- [D-006385] Fixed an issue that caused the jamf binary to become unresponsive when the `createAccount` command is executed without including the `–password` flag.
- [D-006504] The jamf binary now properly creates policy logs when executing the `sudo jamf policy -offline` command.
- [D-006511] Fixed an issue that caused the jamf binary to submit logs for invalid policies.
- [D-006539] Fixed an issue that caused user-level MDM enrollment to fail on OS X computers because of directory permissions.

Fixed in v9.31:

- [D-005615] Fixed an issue that prevented the JSS from adding a directory binding to an Active Directory user's home directory when using a Managed Preference profile that contains a user-level Managed Preference.
- [D-006132] Fixed an issue that caused the jamf binary to add an extra "/index.sucatalog" to the end of the software update server (SUS) URL in the SUS PLIST file when using the `runSoftwareUpdate` command to point a computer at a SUS branch.
- [D-006352] Fixed an issue that prevented the jamf binary from removing the `/private/var/run/jamf` directory when the `sudo jamf removeFramework` command is executed.
- [D-006766] Fixed an issue that sometimes prevented downloading a package from a JDS instance that is configured with certificate-based authentication.

JAMF Distribution Server

Fixed in v9.3:

- [D-006613] Casper Admin and Casper Imaging can now mount a JDS instance on computers with OS X v10.9.2 or later.

Fixed in v9.31:

- [D-006665] Fixed an issue that prevented the JDS Installer for Linux (.run) from successfully installing a JDS instance on computers with Red Hat Enterprise Linux (RHEL).

JAMF Helper

Fixed in v9.31:

- [D-006667] Fixed an issue that prevented JAMF Helper messages from being displayed at the login window if the message is configured to display in full screen mode.

JAMF Software Server

Fixed in v9.3:

- [D-004868] The JSS no longer displays the **Fill user templates (FUT)** and **Fill existing user home directories (FEU)** options when you are configuring a policy that includes a package with the PKG format.

- [D-004995] Fixed an issue that caused the JSS to create a blank computer record when imaging a managed computer using a different name.
- [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-005421], [D-006502] The JSS now correctly processes invalid policy logs.
- [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-005854] Fixed an issue that prevented the JSS from distributing an app or iOS configuration profile if both an LDAP user and an LDAP user group are added as limitations for the scope.
- [D-006085] Fixed an issue that prevented deployment of a package to LDAP users with a space included in the username when the **Fill user templates (FUT)** or **Fill existing user home directories (FEU)** options are configured for the package.
- [D-006096] Fixed an issue that allowed the JSS to deploy policies, configuration profiles, and Managed Preferences to computers with the **Allow JSS to perform management tasks** checkbox deselected if the scope is set to "All Computers".
- [D-006126] Fixed an issue that prevented mapping a printer using a policy with the **Set as Default** checkbox selected.
- [D-006134] The JSS now handles session timeout settings correctly when the session timeout is configured to 0 or 1 minute.
- [D-006187] The JSS now correctly deletes the previously installed version of an iOS configuration profile from mobile devices when the profile is updated using the JSS API.
- [D-006235] Fixed an issue that caused the JSS to display an error when attempting to view PreStage imaging logs.
- [D-006246] The JSS API now includes a serial_number field for the basic computers subset.
- [D-006248] Fixed an issue that prevented the JSS from correctly populating FileVault 2 encryption information using the JSS API.
- [D-006249] Fixed an issue that prevented computers with duplicate names from being added to the JSS using the JSS API.
- [D-006256] Fixed an issue that prevented the JSS API from correctly parsing fields containing certain units of measure.
- [D-006282] When selecting the Security setting **Enable SSL certificate verification**, the JSS now displays a warning stating that OS X computers could be prevented from communicating with the JSS.
- [D-006294] Fixed an issue that prevented computers from being added to the JSS using the JSS API when the computer has a blank UDID and the JSS already contains a computer with a blank UDID. This issue has also been fixed for computers with blank serial numbers and MAC addresses.
- [D-006298] Fixed an issue that prevented a mobile device from being added to the JSS using the JSS API if the mobile device has a blank Wi-Fi MAC address.
- [D-006299] Fixed an issue that prevented mobile devices from being added to or edited in the JSS using the JSS API when the device model_identifier value is iPad2,4.
- [D-006310] Improved performance of computer group lookups using the JSS API.
- [D-006314] Fixed an issue that caused data including packages, scripts, and local accounts to be removed from the original Imaging PreStage when cloning a PreStage for imaging.

- [D-006330] Fixed an issue that caused a computer or mobile device to be unmanaged if an attachment is added to the computer or mobile device using the JSS API. This also resulted in the removal of most of the computer's or mobile device's inventory information from the JSS.
- [D-006354] Fixed an issue that caused headers to be displayed incorrectly and some of the text to overlap when viewing a list in the JSS on a smartphone or an iPod touch.
- [D-006370] Fixed an issue that prevented the JSS from assigning peripherals to computers via the JSS API.
- [D-006391] Fixed an issue that caused iOS configuration profiles to fail if the Per-App VPN Connection Type is set to "F5 SSL" in the VPN payload.
- [D-006397] Fixed an issue that prevented computers from being able to connect to password-protected Wi-Fi when an OS X configuration profile with the Network payload is deployed to the computer before the computer's Wi-Fi is turned on.
- [D-006411] The JSS no longer allows a signed configuration profile to be cloned.
- [D-006416] Fixed an issue that prevented the JSS from uploading a configuration profile (.mobileconfig) if the profile is an enrollment profile.
- [D-006418] Fixed an issue that caused the UDID of a configuration profile to be changed when it is downloaded and then uploaded via the JSS API. This prevented computers or mobile devices with the original profile installed from receiving updates to the profile if it is redeployed.
- [D-006439] Fixed an issue that caused the setting for requiring a password after sleep or screen saver begins to be incorrectly applied when using the JSS to install an OS X configuration profile with a Login Window payload.
- [D-006478] Fixed an issue that caused the JSS to add payload settings to a signed configuration profile that is downloaded from the JSS.
- [D-006495] Fixed an issue that prevented the JSS from saving changes made using a smartphone or an iPod touch.
- [D-006500] Fixed an issue that caused the JSS to schedule a table optimization in MySQL after modifying log flushing settings.
- [D-006547] Fixed an issue that prevented FileVault 2 from being required using an OS X configuration profile with the **Require FileVault 2** option selected in the Security & Privacy payload.
- [D-006594] Fixed an issue that caused the **Show Notification Center in lock screen** and **Show Today view in lock screen** checkboxes in the Restrictions payload of an iOS configuration profile to be reselected after saving if they were deselected.

Fixed in v9.31:

- [D-004057] The JSS now correctly displays computer and mobile device names containing multiple, consecutive spaces.
- [D-004924] Fixed an issue that prevented the Self Service web clip from displaying line breaks in eBook and app descriptions.
- [D-005188] Fixed an issue that prevented the JSS from adding or removing Dock items on OS X v10.9 computers using a policy.
- [D-005256] Fixed an issue that caused the JSS to incorrectly send notifications for violations of restricted software records that do not have email notifications enabled when email notifications for restricted software violations are enabled for a JSS user.
- [D-005508] Fixed an issue that prevented the JSS from immediately distributing an unmanaged app to mobile devices when the distribution method for the app is changed from "Make Available in Self Service Web Clip" to "Prompt User to Install" and additional devices are added to the scope.

- [D-005784] Fixed an issue that prevented some computer and mobile device users from logging in to Self Service or the Self Service web clip using credentials for an LDAP directory account.
- [D-005799] Email notifications for failed policies now include the IP address and serial number of the computer on which the policy failed.
- [D-005856] Fixed an issue that incorrectly caused the JSS to add the Finder payload to an OS X configuration profile when the Restrictions and Login Window payloads are added to the profile.
- [D-005915] Fixed an issue that caused OS X configuration profiles to display a "Not Configured" Finder payload as if it had been configured if the Security & Privacy and Restrictions payloads are configured for the profile.
- [D-005937] Fixed an issue that prevented JSS users from viewing the FileVault 2 recovery key for a computer when they have privileges to do so.
- [D-005979] Fixed an issue that required the Self Service policy **Categories** settings for "Display in" options to be saved before the associated "Feature in" options are enabled when configuring how a policy is displayed in Self Service.
- [D-006045] Fixed an issue that prevented specified folders from syncing when a user authenticates with Active Directory to a computer that has an OS X configuration profile installed with a Mobility payload.
- [D-006055] Fixed an issue that prevented the JSS from restricting AirDrop when the **Allow AirDrop** option is deselected in the Restrictions payload of an OS X configuration profile.
- [D-006064] The JSS now specifies that the **Allow use of YouTube** option in the Restrictions payload in iOS configuration profiles only works for Apple's YouTube on mobile devices with iOS 4 and 5.
- [D-006265] Fixed an issue that prevented similar settings configured in the Security & Privacy and/or Login Window payloads of an OS X configuration profile from being removed from computers when computers are removed from the scope of the profile, or when one of the payloads has been removed from the profile and the profile has been redeployed.
- [D-006278] The JSS now correctly displays dates using the date format selected in Account Preferences when looking up and populating purchasing information from Apple's Global Service Exchange (GSX).
- [D-006470] Fixed an issue that prevented the JSS from consistently adding Dock items to OS X v10.8 computers using a policy.
- [D-006493] Fixed an issue that prevented JSS users with the Auditor privilege set from changing their password.
- [D-006507] Fixed an issue that prevented the JSS from removing the password associated with the non-enterprise network encryption from a cloned OS X configuration profile that includes a Network payload with a non-enterprise security type if the new configuration profile is re-configured with an enterprise security type.
- [D-006545] Fixed an issue that prevented the JSS from respecting changes to the **Make Available Offline** setting of a policy if the changes were made using the JSS API.
- [D-006552] Fixed an issue that prevented eBooks from being added to the JSS using the JSS API.
- [D-006572] Fixed an issue that prevented the JSS from replacing the `$MACADDRESS` payload variable for an OS X configuration profile with the attribute value that is stored in the JSS for that computer.
- [D-006634] Fixed an issue that prevented access to the **Users** tab prior to the user migration process when using a JSS user account that has full JSS access and belongs to a group with the Administrator privilege set.

- [D-006649] Fixed an issue that prevented the VPP registration page from properly displaying images and text when registering with VPP using a VPP invitation if the JSS is not installed as the "ROOT" web application.
- [D-006650] Fixed an issue that prevented the JSS from including all devices assigned to a Device Enrollment Program instance if there are more than 1,000 devices associated with the instance's server token file (.p7m).
- [D-006674] Fixed an issue that caused the department, building, and room information to be reset for a computer when this information is specified for the computer in Recon or Recon.exe and the computer is enrolled.
- [D-006681] Fixed an issue that caused the building or department to be removed from the user and location information of a computer or mobile device when the same LDAP user is assigned to both the computer and the mobile device in the JSS and the building or department is changed in inventory for either the computer or the mobile device.
- [D-006696] Fixed an issue that prevented JSS users from accessing Computer and Mobile Device PreStage Enrollments when they do not have "Computer PreStage Enrollments" and "Mobile Device PreStage Enrollments" privileges.
- [D-006697] Fixed an issue that caused user and location information to be reset for a computer when the computer assignment is removed from the associated peripheral.
- [D-006702] Fixed an issue that prevented computers from installing an MDM profile if the organization name contains one of the following special characters:

  , \ " < > ;
- [D-006706] Fixed an issue that prevented the JSS from sending the JSS Summary to JAMF Software via JAMF Nation when using the **Send Summary to JAMF Software** button.
- [D-006709] Fixed an issue that caused the JSS to display an incorrect count of the computers or mobile devices that belong to a smart group if it is a nested smart group.
- [D-006741] Fixed an issue that prevented a Dock application from launching if the application was added to the user's Dock using an OS X configuration profile with a .app file specified as a Dock item in the Dock payload.
- [D-006746] Fixed an issue that caused the JSS to incorrectly require Username and Password when saving an OS X configuration profile with a Network payload if the Security Type is set to "WPA/WPA2 Enterprise" and Accepted EAP Types is set to **PEAP**.
- [D-006755] Fixed an issue that caused the JSS to incorrectly allow signed configuration profiles to become editable and remove the signature after the configuration profile is edited and saved if the JSS is hosted on a server with Java 1.7 or 1.8.
- [D-006764] Fixed an issue that caused the Security & Privacy payload settings of an OS X configuration profile to be displayed when editing the configuration profile after deleting the Security & Privacy payload.
- [D-006778] Fixed an issue that caused the JSS to incorrectly require Username and Password when saving an OS X configuration profile with a Network payload and Wi-Fi interface if the Accepted EAP Types is set to **TTLS**, **LEAP**, **PEAP**, or **EAP-FAST**.
- [D-006816] Fixed an issue that caused mobile device enrollment to fail when using a PreStage enrollment, or Apple Configurator and an Enrollment URL.
- [D-006849] Fixed an issue that prevented replication of a package to a non-root JDS instance when the package name contains a special character.
- [D-006862] Improved JSS performance for looking up mobile devices and computers associated with a PreStage Enrollment.

Fixed in v9.32:

- [D-006900] Fixed an issue that caused OS X configuration profiles to fail to be deployed to computers during enrollment.
- [D-006887] Fixed an issue that caused OS X configuration profiles with Network payloads to save incorrectly.
- [D-006906] When creating a user report by exporting the results of an advanced user search, the report's Username column is now correctly named.
- [D-005985] Fixed an issue that caused the JSS to incorrectly allow users with site access to be able to see the FileVault 2 category in the inventory information for a computer.
- [D-006030] OS X configuration profiles with a Mobility payload that includes an Account Expiry **Delete At** value are now saved properly.
- [D-006034] Fixed an issue that caused the JSS to incorrectly display a **Version** field in the **Computers** tab when performing a simple computer search if the JSS has been upgraded from v8.x to v9.x and a site has been added.
- [D-006040] Fixed an issue that caused the JSS to fail to display a complete list of configuration profiles when a non-existent smart group is in the scope of a profile.
- [D-006219] Fixed an issue that caused the JSS to fail to flush logs in the jss_audit table when log flushing is turned on for computer inventory reports.
- [D-006773] Fixed an issue that caused the JSS to fail to correctly add or remove Managed Preferences payloads in a Managed Preference profile if a configuration profile is configured with the Security & Privacy, Mobility, Energy Saver, and/or Login Window payloads and the payload settings are repeatedly edited.
- [D-006840] When performing a simple content search for an item other than "All Content" and the search returns no results, the JSS now keeps the previously selected search item.
- [D-006899] Fixed an issue that caused computer-level OS X configuration profiles to fail to display the Mobility payload.
- [D-006952] Removed an unnecessary backslash from a JSS URL shown in the QuickStart Guide for Managing Mobile Devices.
- [D-005920] Fixed an issue that caused the JSS to fail to display an error when attempting to upload an incorrectly formatted PLIST file to a custom payload.
- [D-006544] Fixed an issue that caused the JSS to fail to recognize a .pfx file as a valid file format when attempting to upload a certificate in the Certificate payload of a configuration profile.
- [D-006735] Fixed an issue that prevented the JSS API from correctly interpreting a PUT or POST operation on an account group.
- [D-006947] Fixed an issue that caused the JSS to fail to display the Self Service Web Clip tab for iOS configuration profiles that have been made available in the Self Service Web Clip.
- [D-006905] Fixed an issue that caused the results of a simple user search to fail to export correctly when creating a user report.
- [D-006725] Fixed an issue that caused the JSS to fail to correctly calculate smart computer group memberships if the smart group is based on Purchased or Leased criteria with a value other than Purchased or Leased.
- [D-006770] Fixed an issue that caused the JSS to fail to upload a custom configuration profile created by the mcxToProfile script when the management frequency is set to "Once".

- [D-006835] Fixed an issue that caused the JSS to fail to deploy user-level OS X configuration profiles or make policies available to LDAP users and LDAP user groups if the scope of the profile or policy is configured with a target of all computers and both an LDAP user and an LDAP user group are added as limitations.
- [D-006922] Fixed an issue that caused the JSS to incorrectly display categories in the inventory information for computers when logged in with a JSS account without computer update privileges.
- [D-006919] Fixed an issue that caused the JSS to incorrectly display the "Allow JSS to perform management tasks" checkbox in the inventory information for Windows computers.
- [D-006921] Fixed an issue that caused OS X Configuration Profiles with the Dock payload to be able to choose a magnification when the "Magnification" checkbox is not selected.
- [D-006994] Fixed an issue that caused a simple user search for a blank value to fail to display the message "No results found" when there are no users in the JSS.
- [D-006876] Fixed an issue that caused the JSS API to fail to populate the Site ID and the Site Name for LDAP groups with site access.
- [D-006530] Fixed an issue that caused OS X configuration profiles with two 801.2x Certificates and the Network payload to fail to finish authenticating after the profile is installed.

JSS Database Utility

Fixed in v9.3:

- [D-006043] The JSS Database Utility now displays a warning message when attempting to restore the database while Tomcat is running.

JSS Installer for Linux

Fixed in v9.3:

- [D-006437] Fixed an issue that prevented the JSS Installer for Linux from stopping Tomcat before an upgrade.

JSS Installer for Windows

Fixed in v9.31:

- [D-006648] Fixed an issue that prevented the JSS Installer for Windows from upgrading the JSS.

Recon

Fixed in v9.31:

- [D-006707] Fixed an issue that caused Recon to crash when attempting to enroll computers using the network scanner and a large number of network segments are specified.

Self Service

Fixed in v9.31:

- [D-006738] Fixed an issue that caused Self Service to display a timeout message when running a policy scoped to LDAP users or groups.
- [D-006930] Fixed an issue that, in clustered environments, caused Self Service to sometimes fail to display policies that have LDAP users or LDAP user groups added to their scope.

Known Issues

The following are known issues in the Casper Suite v9.32:

- When users try to access the Self Service web clip on a mobile device with iOS 7.0.1 or 7.0.2, Self Service opens in Safari instead of as a web clip.
- eBooks and unmanaged apps cannot be installed from the Self Service web clip on iOS 7 devices until the Self Service web clip is updated for iOS 7. For more information, see the following Knowledge Base article:

  Updating the Self Service Web Clip for iOS 7
- Management account passwords configured using the network scanner in Recon v9.01-9.11 are not saved correctly in the JSS if they contain an "at" symbol (@). This prevents management tasks from being performed on the affected computers. For more information, see the following Knowledge Base article:

  Casper Remote Error: An Incorrect Username/Password is Entered for this Computer
- [D-003284] Disk encryption configurations fail to activate FileVault 2 on computers with Fusion Drives.
- [D-004003] 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.
- [D-004036] 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.
- [D-004197] Printers mapped using an OS X configuration profile are not displayed in "Print and Scan" in System Preferences unless the **Allow printers that connect directly to user's computer** checkbox is selected in the configuration profile.
- [D-004198] OS X configuration profiles that are configured to display a heading on the login window fail to do so.
- [D-004382] Tapping the URL in an email enrollment invitation on an iOS 6 device draws a blank page. Users should copy-and-paste the URL into the Safari app instead.
- [D-005179] Activity Monitor incorrectly shows that the jamfAgent process is not responding on managed computers with OS X v10.9.
- [D-005532] OS X configuration profiles with a Login Window payload that is configured to deny users and groups the ability to log in fail to do so.
- [D-005612] Casper Admin fails to compile configurations if the master distribution point is a file share distribution point hosted on Windows Server.
- [D-005736] The **Require password after sleep or screen saver begins** and **Allow user to set lock message** settings in the Security & Privacy payload of an OS X configuration profile are not applied.
- [D-005750] An iOS configuration profile with a Restrictions payload that has Media Content settings configured causes the Require Password option to be set to "Immediately" on a mobile device that was originally set to "15 minutes".
- [D-005797] 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.
- [D-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of an OS X configuration profile is not applied at login.

- [D-005900] The JSS fails to install configuration profiles with a Web Clip payload on computers with OS X v10.9.
- [D-005921] Casper Focus sometimes fails to focus mobile devices on an app when the devices are restarted after being focused on the app.
- [D-006026] The JSS fails to restrict Game Center when the **Allow use of Game Center** checkbox is deselected in the Restrictions payload in OS X configuration profiles.
- [D-006058] User-level OS X configuration profiles with widget restrictions fail to restrict widgets.
- [D-006250] A customized Self Service web clip icon uploaded using the JSS will revert to the default Casper Suite icon on iOS 7 devices.
- [D-006266] Policies running during the DarkWake state of Power Nap fail if DarkWake is terminated before the policy finishes running.
- [D-006393] The **Start screen saver after** option in a Login Window payload of an OS X configuration profile is not applied on computers with OS X v10.8.4 or v10.8.5.
- [D-006636] Login and logout hooks implemented via the JSS will not run on computers with OS X v10.9.3.
- [D-006662] Installed OS X configuration profiles that include a VPN payload with the **Use Hybrid Authentication** checkbox selected append "[hybrid]" to the group name in the VPN authentication settings on the computer, which causes group authentication to fail.
- [D-006758] iOS configuration profiles with a Single App Mode payload fail to require a passcode on supervised iOS 7 devices when the devices have a passcode and are locked.
- [D-006793] Computer-level OS X configuration profiles that define options for Time Machine backups fail to do so.
- [D-007004] iOS configuration profiles with a cookies restriction fail to set the specified restriction and hide other cookies restrictions on the device. The restrictions that are hidden depend on the restriction specified in the profile.