



Casper Suite Release Notes

Version 9.3

 JAMF Software, LLC

© 2014 JAMF Software, LLC. All rights reserved.

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

Apache Tomcat and Tomcat are trademarks of the Apache Software Foundation.

Apple, the Apple logo, and Mac OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

Casper Admin, Casper Imaging, Casper Remote, the Casper Suite, Composer, JAMF Software, the JAMF Software logo, JAMF Software Server (JSS), and Self Service are trademarks of JAMF Software, LLC, registered in the U.S. and other countries.

Intel is a registered trademark of the Intel Corporation in the U.S. and other countries.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

Maker's Mark is a registered trademark of Beam Global Spirits & Wine, Inc.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

All other products and service names mentioned are the trademarks of their respective companies.

Contents

4	What's New in This Release
4	Key Features
4	Implemented Feature Requests
5	API Improvements
6	Installation
6	Compatibility
6	Upgrading the JSS
10	Upgrading to OS X Server v10.9
11	Removals
11	Deprecations
12	Bug Fixes and Enhancements
12	Casper Admin
12	Casper Focus
12	Casper Imaging
12	Casper Remote
12	jamf binary
13	JAMF Distribution Server
13	JAMF Software Server
15	JSS Database Utility
15	JSS Installer for Linux
16	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.

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

Casper Focus v9.3 will be available from the App Store when it is approved by Apple.

Implemented Feature Requests

To view a complete list of feature requests that were implemented in v9.3, go to:

<https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=57>

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 v9.3 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 v9.3 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 v9.3 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 v9.3 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.

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.

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 or iPod touch, 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**.

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 or iPod touch, 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**.

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 v9.3 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

[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.

Casper Focus

[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

- [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.

Casper Remote

- [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.

jamf binary

- [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.

JAMF Distribution Server

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

JAMF Software Server

- [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.

JSS Database Utility

[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

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

Known Issues

The following are known issues in the Casper Suite v9.3:

- 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-005577] OS X configuration profiles with an Energy Saver payload set incorrect startup and shutdown times on OS X v10.8 computers.
- [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] Some 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-005903] Casper Focus crashes on iPads connected to a Bluetooth keyboard if the escape key is pressed.
- [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-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-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-006582] An “Enrollment successful” message displays after failing to re-enroll a computer if the **Restrict re-enrollment to authorized users only** option is selected in User-Initiated Enrollment settings.