



Casper Suite Release Notes

Version 9.61

 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.

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
4	API Improvements
5	Supported OS X Operating Systems
6	Installation
6	Compatibility
6	Upgrading the JSS
10	Upgrading to OS X Server v10.10
11	Removals
11	Deprecations
12	Bug Fixes and Enhancements
12	Casper Admin
12	Casper Remote
12	jamf binary
12	JAMF Distribution Server
13	JAMF Software Server
13	Recon
13	Self Service for iOS
14	Self Service for OS X
15	Known Issues

What's New in This Release

Key Features

There are no key features for the Casper Suite v9.61. The Casper Suite v9.6 includes the following key features:

- **Support for OS X Yosemite (v10.10)**—The Casper Suite now includes support for OS X v10.10.
- **Additions to OS X configuration profiles**—New payloads and settings have been added to OS X configuration profiles. This includes but is not limited to: AirPlay payload, Xsan payload, and additional settings in the Passcode, Restrictions, and AD Certificate payloads.
- **Mac App Store apps**—Mac App Store apps purchased through Apple's Volume Purchase Program (VPP) and assigned to users via VPP-managed distribution can now be installed automatically on computers with OS X v10.9 or later.
- **Device Enrollment Program**—When the JSS is integrated with the Apple's Device Enrollment Program, computers with OS X v10.10 can be managed automatically when added to the JSS using a PreStage enrollment.

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

For information about the operating systems that are supported with this version of the Casper Suite, see the [Supported OS X Operating Systems](#) section.

Implemented Feature Requests

There are no implemented feature requests for the Casper Suite v9.61. To view a complete list of feature requests that were implemented in v9.6, go to:

<https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=82>

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

Supported OS X Operating Systems

As of the Casper Suite v9.6 or later, the following operating systems are fully supported:

- OS X v10.7
- OS X v10.8
- OS X v10.9
- OS X v10.10

If you have computers with OS X v10.5 and v10.6 in your environment, new features will not be implemented for these computers. All existing workflows will continue to function, however you may need an older version of the client applications. For more information about client application versions, see the "Requirements" section in the *Casper Suite Administrator's Guide*.

Installation

Compatibility

The JSS v9.61 supports the following versions of client applications in the Casper Suite:

- Casper Admin v9.4 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, Casper Focus, and Self Service Mobile.

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

Upgrading the JSS

The easiest way to upgrade is to use a JSS Installer. There are three installers, one for each platform on which the JSS can be installed—Mac, Linux, and Windows. Use the installer for the platform on which you plan to install the JSS. (For more information, see the [Preparing to Upgrade the JSS](#) Knowledge Base article.)

The JSS Installer installs the JSS web application, JSS Database Utility, and Apache Tomcat on your computer. For more information about the version of Tomcat installed by the JSS Installer, see the [Apache Tomcat Version Installed by the JSS Installer](#) Knowledge Base article.

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 use the JSS Installer for Mac, you need a Mac computer with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- OS X Server v10.7 or later
- Server.app (recommended)
- Java 1.6 or 1.7
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7

You can download the JCE from:

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:
<https://www.mysql.com/downloads/>
- Ports 8443 and 9006 available

Linux Requirements

To use the JSS Installer for Linux, you need a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- One of the following operating systems:
 - Ubuntu 12.04 LTS Server (64-bit)
 - Ubuntu 14.04 LTS Server (64-bit)
 - Red Hat Enterprise Linux (RHEL) 6.4 or later

- Open Java Development Kit (OpenJDK) 6 or 7

For more information, go to <http://openjdk.java.net/>.

- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:
<https://www.mysql.com/downloads/>
- Ports 8443 and 8080 available

Windows Requirements

To use the JSS Installer for Windows, you need a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available

- Windows Server 2008 R2 (64-bit) or Windows Server 2012 (64-bit)
- Java SE Development Kit (JDK) 1.6 or 1.7 for Windows x64
You can download the JDK from:
<http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html>
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7
You can download the JCE from:
<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:
<https://www.mysql.com/downloads/>
- Ports 8443 and 8080 available

Upgrading the JSS

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.

If you are upgrading from the JSS v9.6 or earlier using the Windows installer, you must modify the HTTPS connector for port 8443 in the `server.xml` file:

- a. Open the `server.xml` file in a text editor.
The `server.xml` file is located in `/path/to/JSS/Tomcat/conf/`.
 - b. Add the following attribute to the `Connector` element for `port="8443"` after the `sslProtocol="TLS"` attribute:
`sslEnabledProtocols="TLSv1.2, TLSv1.1, TLSv1"`
 - c. Save and close the `server.xml` file.
 - d. Restart Tomcat.
For instructions, see the following Knowledge Base article:
[Starting and Stopping Tomcat](#)
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:

- **Distributing Apps to Mobile Devices with App Store Restrictions**—As of the Casper Suite v9.5, you can distribute apps to mobile devices with iOS 7 or later even when the App Store is restricted on the devices. To implement this functionality after upgrading to v9.5, you need to redistribute any existing iOS configuration profiles that have the Allow installing apps checkbox deselected in the Restrictions payload.

For more information, see the following Knowledge Base article:

[Distributing Apps to Mobile Devices with App Store Restrictions After Upgrading to the JSS v9.5 or Later](#)

- **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 v10.10

This section explains how to upgrade the JSS host server to OS X Server v10.10.

1. Back up your current database.
2. Upgrade from OS X v10.9 to v10.10.
3. Install Java 1.7 and JCE 1.7.
For instructions, see the [Installing Java and MySQL](#) Knowledge Base article.
4. Follow the instructions for upgrading the JSS.

Removals

The following functionality has been removed:

- **Enrollment URLs ending in “/iosenroll” or “/osxenroll”**—Enrollment URLs ending in “/iosenroll” or “/osxenroll” can no longer be used to direct users to the enrollment portal for user-initiated enrollment. To direct users to the enrollment portal, you need to provide them with the full URL for the JSS followed by “/enroll”. For example:
`https://jss.mycompany.com:8443/enroll`
- **Clear-text password fields in the JSS Rest API**—Processes or applications that use the clear-text password field must be modified to use the MD5 and SHA-256 hashed versions instead. For assistance or if you have questions or concerns, contact your JAMF Software Account Manager.

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.

The JSS still checks script output for the words “error” or “fail”, but 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.

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 v9.6:

- [D-007005] Fixed an issue that prevented Casper Admin from mounting the JDS instance if the “Enable Certificate-Based Authentication” checkbox is selected and the JDS instance is set as the master distribution point.
- [D-007428] Fixed an issue that caused Casper Admin to display an error when adding the Install OS X v10.10 Developer Preview.app.

Casper Remote

Fixed in v9.6:

[D-006231] Fixed an issue that prevented Casper Remote from logging out of the SSH connection on the target computer after ending the screen sharing session by closing the app.

jamf binary

Fixed in v9.6:

- [D-007510] Fixed an issue that prevented the jamf binary from running policies successfully if there is an unexpected log file in /Library/Application Support/JAMF/logs/.
- [D-007778] Self Service for OS X now clears the ~/Library/Caches/com.jamfsoftware.selfservice/ cache after it has been upgraded.

JAMF Distribution Server

Fixed in v9.6:

- [D-006396] Fixed an issue that prevented the JDS instance from being installed if the computer’s UDID contains a non-hex character.
- [D-007526] Fixed an issue that prevented a master JDS instance installed on Linux from applying the correct permissions to the package if umask was present when the package was uploaded. This caused the package to become unreadable.
- [D-007570] Fixed an issue that caused JDS instances to be incompatible with Apache 2.4.

Fixed in v9.6.1:

[D-007874] The jamfds binary now uses Transport Layer Security (TLS) instead of Secure Sockets Layer (SSL) v3.0.

JAMF Software Server

Fixed in v9.6:

- [D-005832] Fixed an issue that prevented users with full access to the JSS from adding items to Casper Admin when they are viewing a specific site in the JSS.
- [D-006527] Fixed an issue that caused the JSS to report incorrect FileVault 2 information in the Storage and Disk Encryption categories in computer inventory information if a non-boot partition is encrypted.
- [D-007482] Fixed an issue that caused the JSS to fail to start if Tomcat 8.0 is installed on the JSS host server.
- [D-007593] Fixed an issue that prevented the JSS from allowing JSS users with site access to change the password of their JSS account.
- [D-007776] Fixed an issue that caused a manual upgrade of the JSS to fail when Tomcat 6 is installed on the JSS host server.
- [D-007787] Fixed an issue that prevented the JSS from removing a managed app from a mobile device if the device was removed from the scope of the app while the device's Wi-Fi was turned off and the app was then deleted from the JSS. This caused the JSS to display a RemoveApplication command indefinitely in the list of pending management commands, and subsequent MDM commands sent to the device to fail.
- [D-007803] Fixed an issue that caused a JSS in debug mode to recalculate smart user group memberships when verifying the content for VPP-managed distribution.
- [D-007836] Fixed an issue that sometimes caused the JSS to incorrectly calculate smart group memberships if multiple smart groups are updated at the same time.

Fixed in v9.61:

- [D-007873] RC4 cipher suites are now disabled in the default server .xml file when performing a fresh installation.
- [D-007876] The default server .xml file now only supports Transport Layer Security (TLS) and disables support for Secure Sockets Layer (SSL) v3.0.

Recon

Fixed in v9.6:

[D-007681] Fixed an issue that prevented Composer and Recon from being opened on an OS X v10.9.5 computer that has Apple's Gatekeeper feature set to only allow applications downloaded from the Mac App Store and identified developers.

Self Service for iOS

Fixed in v9.6:

[D-007772] Fixed an issue that caused Self Service Mobile for iOS to display an "Unable to Connect to Server" error instead of directing the user to the JAMF Software website when Self Service Mobile is opened after it is downloaded from the App Store.

Self Service for OS X

Fixed in v9.6:

[D-007674] Fixed an issue that caused Self Service to crash when a user attempts to accept a VPP invitation using Self Service on a computer with OS X v10.7 or v10.8.

Known Issues

The following are known issues in the Casper Suite v9.61:

- 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-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-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-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of an OS X configuration profile is not applied at login.
- [D-005900] The JSS fails to install configuration profiles with a Web Clip payload on computers with OS X v10.9.
- [D-006026] The JSS fails to restrict Game Center when the **Allow use of Game Center** checkbox is deselected in the Restrictions payload in OS X configuration profiles.
- [D-006058] User-level OS X configuration profiles with widget restrictions fail to restrict widgets.
- [D-006250] A customized Self Service web clip icon uploaded using the JSS will revert to the default Casper Suite icon on iOS 7 devices.

- [D-006266] Policies running during the DarkWake state of Power Nap fail if DarkWake is terminated before the policy finishes running.
- [D-006393] The **Start screen saver after** option in a Login Window payload of an OS X configuration profile is not applied on computers with OS X v10.8.4 or v10.8.5.
- [D-006627] When restarting a computer that has been imaged using Casper Imaging, the computer fails to enroll if attempting to connect to the JSS via an Apple Thunderbolt to Ethernet Adapter.
- [D-006662] Installed OS X configuration profiles that include a VPN payload with the **Use Hybrid Authentication** checkbox selected append “[hybrid]” to the group name in the VPN authentication settings on the computer, which causes group authentication to fail.
- [D-006758] iOS configuration profiles with a Single App Mode payload fail to require a passcode on supervised iOS 7 devices when the devices have a passcode and are locked.
- [D-006793] Computer-level OS X configuration profiles that define options for Time Machine backups fail to do so.
- [D-007004] iOS configuration profiles with a cookies restriction fail to set the specified restriction and hide other cookies restrictions on the device. The restrictions that are hidden depend on the restriction specified in the profile.
- [D-007087] Mobile devices fail to enroll properly using a PreStage enrollment when they are powered off from the Login page after being restored to an iCloud backup.
- [D-007163] Casper Focus sometimes incorrectly removes the focus from a student device if the home button on the student device is pressed while the device is being focused.
- [D-007206] Attempting to install Self Service Mobile for iOS on an enrolled mobile device when the Self Service web clip is open causes the device to lock on the web clip. This prevents the user from accessing any other screens or content on the device.
Workaround: Change the **Install Automatically** option to **Self Service web clip**.
- [D-007245] The configuration page fails to display correctly when enrolling a mobile device via PreStage enrollment.
- [D-007386] Mobile devices fail to enroll using a PreStage enrollment if an LDAP user has **User must change password at next logon** selected in Active Directory.
- [D-007447] Casper Admin is unable to replicate to a local, non-external partition.
- [D-007486] SMB shares sometimes fail to mount on a computer with OS X v10.9.
- [D-007508] Apps assigned to users for VPP-managed distribution sometimes fail to install completely on mobile devices that have Automatic Downloads enabled.
- [D-007511] If the option to skip the Restore page is selected for a PreStage enrollment in the JSS, the Restore page is not skipped during enrollment if the enrollment process is restarted during the Setup Assistant.
- [D-007537] Location Services are incorrectly disabled when the **Allow modifying Find My Friends settings (Supervised devices only)** checkbox is deselected in the Restrictions payload of an iOS configuration profile.
- [D-007568] The Activation Lock bypass code is not collected by the JSS v9.4.
- [D-007628] iOS configuration profiles made available in Self Service cannot be removed manually from mobile devices with iOS 8 even when the profiles are configured to allow removal.
Workaround: Remove the mobile device from the scope of the profile.
- [D-007638] An in-house eBook set to the **Install Automatically** distribution method will display as “Untitled” until it is opened on a mobile device.

- [D-007641] Samsung Galaxy Pocket Plus devices with Android v4.0.4 fail to enroll with the JSS.
- [D-007721] iOS configuration profiles with a Mail payload configured to log in to the app using a specified password fail to require a password after the configuration profile has been removed and redistributed to require a password on mobile devices with iOS 6.
- [D-007823] Policies configured to require users to enable FileVault 2 in a disk encryption payload fail to do so on a computer with OS X v10.10.
- [D-007825] OS X configuration profiles with a Software Update payload configured to allow installation of OS X beta releases fail to make OS X beta releases available to users.
- [D-007860] When the User value in the Exchange payload of an OS X configuration profile is an email address, an OS X Mail app user cannot authenticate and access their email on OS X v10.10 computers.
- [D-007898] If a PreStage enrollment is configured with the **Make MDM Profile Mandatory** checkbox selected and a user skips the Wi-Fi configuration step during the OS X Setup Assistant process, the computer will not be enrolled with the JSS.