Casper Suite Release Notes

Version 9.97

jamf

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

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Contents

What's New in This Release

The Casper Suite v9.97 includes the following features:

Single Sign-On Enhancements

- You can now specify a custom SAML attribute for User Mapping, instead of the default `NameID` attribute. To access this feature in the JSS, navigate to **Settings > Single Sign-On > User Mapping: SAML** .
- When adding a JSS Signing Certificate, the metadata `use="signing"` attribute in `KeyDescriptor` element is now optional.
- While configuring User-initiated enrollment settings, the JSS now displays a message that the custom Login page is not visible to users when Single Sign-On is enabled.

AirPlay Permissions

You can now use the JSS to create AirPlay Permissions, which allow you to automatically associate Apple TV devices with mobile devices. To access this feature in the JSS, navigate to **Settings > Global Management > AirPlay Permissions**.

Smart Mobile Device Group Enhancements

- You can now deploy automated management commands on a schedule. To access this feature in the JSS, navigate to **Mobile Devices > Smart Mobile Device Groups > Automated Management** tab.
- The list of available smart groups now includes information on automated management commands.
- Information about management commands sent via the Automated Management tab is now displayed in the inventory information for mobile devices.

Apple Configurator Enrollment Enhancements

- You can now choose Apple Configurator Enrollment as an enrollment method. To access this feature in the JSS, navigate to **Mobile Devices > Enrollment Invitations >** click **New**.
- You can choose to send a dynamic enrollment URL via email, SMS, or choose to make the URL viewable in the JSS.
- New template text is available when sending the URL via email or SMS to specify that the received URL is intended for use with Apple Configurator.
- The Apple Configurator Enrollment settings now provide links to edit enrollment invitations and sites.

iOS Configuration Profile Enhancements

- You can now use the Network Usage Rules payload to allow or prevent cellular data usage and data roaming usage for managed apps.
- The IKEv2 option is now available in the VPN payload for iOS configuration profiles when using Per-App VPN.

Volume Purchase Program (VPP) Enhancements

- The JSS now displays the total combined content purchased and total combined content in use for device-based VPP-managed distribution for mobile devices and user-based VPP-managed distribution when viewing the details of a single App Store app. In addition, you can view if the app was purchased with VPP licenses or redeemable VPP codes.
  To access this feature in the JSS, navigate to **Mobile Devices** > **Mobile Device Apps** > click the app you want to view details for.
- The JSS now displays the total combined content purchased and total combined content in use for device-based VPP-managed distribution for computers and user-based VPP-managed distribution when viewing the details of a single Mac App Store app. In addition, you can view if the app was purchased with VPP licenses or redeemable VPP codes.
  To access this feature in the JSS, navigate to **Computers** > **Mac App Store Apps** > click the app you want to view details for.

Apple Education Support Enhancments

Improved performance when syncing the JSS with Apple School Manager.
To access this feature in the JSS, navigate to **Settings** > **Mobile Device Management** > **Apple Education Support** > click the **Apple School Manager** tab.

Cloud Distribution Point Enhancements

- Improved handling of content that has been uploaded to a Cloud Distribution Point.
- Improved performance when uploading packages to JAMF Cloud Distribution Service (JCDS).

To access this feature in the JSS, navigate to **Settings** > **Computer Management** > **Cloud Distribution Point**.

Healthcare Listener—Remotely Manage Mobile Devices in Healthcare

The Casper Suite now includes the ability to automatically send remote commands to mobile devices in the healthcare industry using the Healthcare Listener. The Healthcare Listener is a secure service that receives ADT messages from a healthcare management system. When the Healthcare Listener has received an ADT message, the JSS interprets the message to automatically send remote commands to mobile devices. As of the Casper Suite v9.97, the remote command that is automatically sent to a mobile device is the Wipe Device remote command. (For more information about the communication process of the Healthcare Listener, see the Healthcare Listener Communication Knowledge Base article.)

You can use the Casper Suite to enable and configure the Healthcare Listener after an Infrastructure Manager instance is installed.
To access this feature in the JSS, navigate to **Settings** > **Computer Management** > **Infrastructure Manager Instances** > Click the Infrastructure Manager instance that is hosting a Healthcare Listener.

For more information about the Healthcare Listener, see the Installing and Configuring the Healthcare Listener technical paper.

For a complete list of deprecations, removals, bug fixes, and enhancements, see the Deprecations and Removals and the Bug Fixes and Enhancements sections.

To view a complete list of the feature requests implemented in v9.97, go to:

https://www.jamf.com/jamf-nation/feature-requests/versions/154/casper-suite-9-97

Note: New privileges associated with new features in the Casper Suite are disabled by default.

Installation

Preparing to Upgrade

To ensure the upgrade goes as smoothly as possible, review the best practices, tips, and considerations explained in the following Knowledge Base articles:

- Preparing to Upgrade the JSS—Explains the best practices for evaluating and preparing for an upgrade.
- Upgrading the JSS in a Clustered Environment—Provides step-by-step instructions for upgrading the JSS in a clustered environment.

It is also recommended that you review the Functionality Changes and Other Considerations section to determine if changes made to the Casper Suite since your last upgrade could impact your environment or require you to take action.

Functionality Changes and Other Considerations

Depending on the version you are upgrading from, changes made to the Casper Suite since your last upgrade could impact your current environment setup or workflows.

The following table explains key changes and additions to the Casper Suite, the versions in which they were implemented, and where to get more information.

Starting with...	Change or Consideration	Description	Additional Resources
v9.96	Removed support for macOS v10.5 and v10.6	The Casper Suite v9.96 removes support for macOS v10.5 and v10.6. For information on removing unsupported computers from the JSS, see the Removing the Management Framework from Multiple Computers Knowledge Base article.	N/A
v9.96	Deprecated support for macOS v10.7 and v10.8	Features implemented in the Casper Suite v9.96 or later are no longer supported on computers with macOS v10.7 and v10.8. Workflows implemented prior to v9.96 will continue to function, but they may require earlier versions of the client applications.	N/A
v9.96	Change to JDS instance installation	JDS instances are no longer installed during fresh installations of the JSS.	N/A

Starting with...	Change or Consideration	Description	Additional Resources
v9.93	Loss of certain customizations when upgrading to Tomcat 8	When upgrading from Tomcat 7 to Tomcat 8 on Windows, any customizations to CATALINA_OPTS or JAVA_OPTS will be lost. To keep your customizations, when upgrading your JSS, click **Custom** in the Setup Type pane. Click **Next** and then click **Upgrade**. In the Summary pane, click **Open Settings** to review and set your customizations.	N/A
v9.93	Change to `server.xml`	In Tomcat 8 or later, JasperListener prevents the JSS from starting and must be removed. The JSS Installer automatically makes the necessary changes to Tomcat's `server.xml` by removing the `<Listener className="org.apache.catalina.core.JasperListener" />` line.	N/A
v9.93	Change to `database.xml`	The Database Driver in the `database.xml` is now set to `org.mariadb.jdbc.Driver` during JSS upgrades.	N/A
v9.92	Criteria name change	The advanced search and smart group criteria **Subscriber MCC** will now be listed as **Current Carrier Network**.	N/A
v9.92	Criteria name change	The advanced search and smart group criteria **Subscriber MNC** will now be listed as **Home Carrier Network**.	N/A
v9.8	New location for jamf binary	The jamf binary is automatically moved from `/usr/sbin/jamf` to its new location, `/usr/local/jamf/bin/jamf`, during an upgrade to the Casper Suite v9.8. During the upgrade, the database is scanned for packages, scripts, and extension attributes that reference the previous location of the binary. If items are found, notifications are displayed in the JSS after the upgrade is complete. These items need to be modified to reference the new location of the binary, which can be done in the JSS by clicking the notifications. Items that are not stored in the database and reference the previous location of the binary need to be modified to reference the new location.	N/A
v9.8	Change in the removal of devices from DEP	The JSS can no longer be used to remove a device from Apple's Device Enrollment Program (DEP). Go to the Apple Deployment Programs website to remove the device.	N/A

Upgrading the JSS

This section explains how to upgrade the JSS using the JSS Installers. If the JSS host server does not meet the JSS Installer requirements, you can install the JSS manually using the instructions in the "Manually Installing the JAMF Software Server" technical paper.

JAMF Software tests upgrades from v9.8 through the current version.

Installed Components

The following components are installed on the JSS host server by the JSS Installer:

- JSS web application
- JSS Database Utility
- Apache Tomcat

To find out which version of Tomcat will be installed, see the Apache Tomcat Version Installed by the JSS Installer Knowledge Base article.

Note: To take full advantage of all new features, bug fixes, and enhancements available in the Casper Suite, it is recommended that you use the latest version of the JSS and the client applications. To upgrade the client applications, simply replace the existing applications with the latest version.

JSS Installer Requirements

JSS Installer for Mac

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
- macOS v10.7 or later
- macOS Server (recommended)
- Java SE Development Kit (JDK) 1.7 or 1.8 for Mac
  You can download the JDK from:
  http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.7 or 1.8
  You can download the JCE from:
  http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html
- MySQL Enterprise Edition 5.5.x or 5.6.x (recommended), or MySQL Community Server 5.5.x or 5.6.x, available at:https://www.mysql.com/downloads/
- Ports 8443 and 9006 available

JSS Installer for Linux

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, 6.5, 6.6, or 7.0
- Open Java Development Kit (OpenJDK) 7 or 8
  For installation information, go to http://openjdk.java.net/install/.
- MySQL Enterprise Edition 5.5.x or 5.6.x (recommended), or MySQL Community Server 5.5.x or 5.6.x, available at:https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

JSS Installer for Windows

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), Windows Server 2012 (64-bit), or Windows Server 2012 R2 (64-bit)
- Java SE Development Kit (JDK) 1.7 or 1.8 for Windows x64
  You can download the JDK from:
  http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.7 or 1.8
  You can download the JCE from:
  http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html
- MySQL Enterprise Edition 5.5.x or 5.6.x (recommended), or MySQL Community Server 5.5.x or 5.6.x, available at:
  https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

Upgrading the JSS

Use the following instructions to upgrade a JSS hosted on Mac or Linux. To upgrade a JSS hosted on Windows, see "Upgrading the JSS" in the JSS Installation and Configuration Guide for Windows.

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.

Deprecations and Removals

There are no deprecations or removals in this release.

Bug Fixes and Enhancements

Composer

[PI-002622] Fixed XML external entity (XXE) vulnerabilities in the Jamf Binary, Composer and Recon.

Documentation

[PI-003079] The “Group Attribute Statement” URL has been corrected in the Configuring Single Sign-On with Okta Knowledge Base article.

JAMF Software Server

- The patch notification lookup process has been optimized to eliminate the collection of excessive data.
- Fixed an issue that caused a NullPointerException in the logs during startup regarding policy class definition.
- Fixed an issue that caused the patch reporting process to generate inventory information for all computers instead of inventory information for a single computer when generating a patch report for a software title not configured on the computer.
- Fixed an issue that could result in MySQL database connection deadlocks.
- Fixed an issue where MySQL would write errors in the *JamfSoftwareServer.log* when using client-side Prepared Statements.
- Fixed an issue where packages with failing postinstall scripts showed up in logs with completed status.
- Fixed an issue where SoftwareTitleMonitor was not reporting its cycle performance to the debug logs.
- Fixed an issue where the JSS API returned a status of 200 during startup when the JSS was not yet available.
- [D-006652] Fixed an issue where the Enrollment Method field in a search or smart group would not return results if an OR operator was used.
- [D-007748] Fixed an issue where policies set to run **Once Per Computer** would sometimes run multiple times on the same computer.
- [PI-000365] Fixed an issue where the *do_not_upgrade_jamf* flag was being set to true on some machines.
- [PI-002045] Fixed an issue where applications installed via a Personal Device Profile would report as failed.
- [PI-002150] Fixed an issue where newly enrolled computers would sometimes be unable to install software via Self Service.

- [PI-002223] Fixed an issue where some Bluetooth Low Energy capable computers would not show as Bluetooth Low Energy capable.
- [PI-002382] Fixed an issue where deferred policies did not respect the deferral time set.
- [PI-002394] Fixed an issue where VPP licenses in a clustered environment would duplicate if the VPP License monitor process was kicked off from a child node when it was already running on the master node.
- [PI-002475] Fixed an issue where a single node JSS instance would duplicate VPP licenses and apps in the app catalog when updating purchased content.
- [PI-002508] Fixed an issue where the cache error page had the wrong title.
- [PI-002573] Fixed an issue where computers with macOS v10.11 that were bound with Centrify would not report inventory correctly.
- [PI-002580] Fixed an issue where a user would bypass the customized login text when logged in with an SSO provider.
- [PI-002635] Fixed an issue where apps were removed and reinstalled when a user was moved to a new smart group with a lower ID than their pervious smart group.
- [PI-002663] Fixed an issue where the SSO and Self Service logout did not function properly.
- [PI-002689] Fixed an issue where Computer User level MDM broke if the user was not in the JSS and there were Self Service Notifications scoped to them.
- [PI-002718] Fixed an issue where an outdated logout screen was sometimes displayed on Self Service.
- [PI-002759] Fixed an issue where the current site in the frontend was not set before requesting a switch to a new site, causing a 403 forbidden error to be returned from the API.
- [PI-002771] Fixed an issue where policies with a Maintenance Payload and Fix Disk Permissions checked would fail on computers with macOS v10.12.
- [PI-002826] Fixed an issue that prevented the JSS from saving user preferences while using Single Sign-On authentication.
- [PI-002829] Fixed an issue where the "Forgot your password?" link did not display.
- [PI-002869] Fixed an issue that prevented the JSS from correctly displaying a setting in the Mail payload of macOS configuration profiles.
- [PI-002902] Fixed an issue that prevented the JSS from correctly syncing class names with Apple School Manager.
- [PI-002946] Fixed an issue where only one computer record would display available Software Updates at a time.
- [PI-002949] Fixed an issue where macOS packages could not be indexed and were removed from indexing during upgrade.
- [PI-002975] Fixed an issue where AD binding would fail until the Domain Admin password was stored as unencrypted.
- [PI-002984] Fixed an issue that caused the JSS to become unresponsive when multiple patch reporting software titles are configured in rapid succession.
- [PI-003012] Fixed an issue where apps set to Install Automatically on devices with iOS 10 or later could get stuck in an installation loop when enrolled in DEP and not using VPP.
- [PI-003068] Fixed an issue where the JSS did not differentiate between a department ID and the display name.

- [PI-003151] Fixed an issue where an "Incorrect username and password" error occurred when creating a Push Proxy token.

Jamf Binary

- [D-010148] Fixed an issue that sometimes caused the jamf binary to be deleted during an upgrade to the jamf binary. **Note:** This fix will not take effect until a subsequent upgrade is performed (e.g. v9.97 is upgraded to a later version).
- [PI-002622] Fixed XML external entity (XXE) vulnerabilities in the Jamf Binary, Composer and Recon.
- [PI-003001] Fixed an issue where upgrading the binary resulted in a 0 byte binary that was not owned by the root user.

Recon

- [PI-001389] Fixed an issue where submitting inventory with Recon would sometimes result in an error, "Message could not be parsed".
- [PI-002396] Fixed an issue where Recon would crash when SSH was disabled when performing local enrollment.
- [PI-002622] Fixed XML external entity (XXE) vulnerabilities in the Jamf Binary, Composer and Recon.

Known Issues

The following issues are known in the Casper Suite:

Entering incorrect credentials on the JSS login page redirects to /logout.html which causes the next login attempt to fail unless the URL is changed manually.

The following issues are a result of bugs in third-party software. Defects have been filed for these bugs and are awaiting resolution.

- The "Allow all" or "Prevent all" cellular data usage and data roaming usage settings cannot be edited after they have been set on a mobile device with iOS 9.
- [PI-002319] In Casper Focus, changing the focus from one app to another fails on student devices with iOS 9.3.2 or later. The following error message is displayed as a result: "Focus failed: the device may not be connected to a network." As a workaround, remove the focus from the student devices. Then, after a message displays indicating that the focus was removed, focus the devices on the desired app.
- [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] macOS 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-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of a macOS configuration profile is not applied at login.
- [D-005900] The JSS fails to install configuration profiles with a Web Clip payload on computers with macOS 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 macOS configuration profiles.
- [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 a macOS configuration profile is not applied on computers with macOS v10.8.4 or v10.8.5.
- [D-006662] Installed macOS 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-006979] When enrolling a computer using a QuickAdd package, the QuickAdd installer incorrectly prompts users for local administrator credentials twice if the **Restrict re-enrollment to authorized users only** checkbox is selected.
- [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-007245] The configuration page fails to display correctly when enrolling a mobile device via PreStage enrollment.
- [D-007486] SMB shares sometimes fail to mount on a computer with macOS v10.9.
- [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-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-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 macOS v10.10.
- [D-007825] macOS configuration profiles with a Software Update payload configured to allow installation of macOS beta releases fail to make macOS beta releases available to users.
- [D-007860] When the User value in the Exchange payload of a macOS configuration profile is an email address, a macOS Mail app user cannot authenticate and access their email on macOS 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.
- [D-007969] Compiled configurations created with Casper Admin using the {{InstallESD.dmg}} file for macOS v10.10 fail to create a “Recovery HD” partition when the configuration is used to image computers.
- [D-008018] The JSS cannot connect to an Open Directory server hosted on macOS Server v10.10 using CRAM-MD5 authentication.
- [D-008152] End users are incorrectly prompted for an Airplay password when attempting to Airplay to a device for which an AirPlay password has been specified using a macOS configuration profile.
- [D-008167] When multiple Casper Suite disk images are mounted, the JSS Installer installs the version of the Casper Suite included in the disk image that was mounted first.
- [D-008212] If a mobile device is enrolled using a PreStage enrollment and is then re-added to the server token file (.p7m), the device becomes unassigned and the JSS incorrectly displays the device as still being in the scope of the PreStage enrollment.
- [D-008286] When VMware Fusion is closed on a client computer, the computer loses its connection with the JSS.
- [D-008309] A guest user is able to log in from the FileVault 2 login window when a configuration profile was used to disallow guest users and FileVault 2 is configured for the current or next user.

- [D-008567] When a student device with iOS 8 is focused on a website, multiple icons with the website link are displayed.
- [D-008688] macOS configuration profiles that include a Network payload configured with 802.1X authentication and the **Auto Join** checkbox selected fail to automatically connect a computer to the network after the computer leaves sleep mode.
- [D-008806] The dsconfigad binary fails to bind a computer to a directory service if the service account password contains an exclamation point (!).
- [D-008920] A policy that contains an macOS v10.10.3 installer causes a computer with macOS v10.10.2 or earlier to become unresponsive.
- [D-009110] Configuration profiles with the “Internal Disks: Allow” option disabled do not prevent the use of memory cards.
- [D-009443] Casper Focus fails to focus a student device with iOS 7 on the attention screen if the device was being focused on an app or website.
- [D-009450] A macOS configuration profile with a Password payload incorrectly enforces a number of complex characters equal to the last value used.