Casper Suite Release Notes

Version 9.100.0

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

Initial Compatibility with macOS 10.13, iOS 11, and tvOS 11

The Casper Suite v9.100.0 provides initial compatibility with macOS 10.13, iOS 11, and tvOS 11. Full compatibility and key feature support for these OS versions will be available in a future version of the Casper Suite.

In preparation for the release of macOS 10.13, consider the following changes:

- Starting with macOS 10.13, Apple has deprecated the use of Apple Filing Protocol (AFP) on computers formatted with Apple File System (APFS). If you are using a file share distribution point, be prepared to change the sharing protocol to SMB before upgrading computers to macOS 10.13. If you need assistance or have questions, contact your Jamf account representative.
- When using a policy to upgrade computers with macOS 10.9 or earlier to macOS 10.12.4 or later, be prepared to upgrade the computers to a version between macOS 10.10 and 10.12.3 first.

iOS Management Capabilities

Option to Require Tethered Connection for App Installation

Setup and Requirements:

- Mobile devices with iOS 10.3 or later
- Computers with macOS 10.12.4 or later, must be connected to the Internet via Ethernet and have Wi-Fi turned off
- Portable computers must be plugged in to a power source because the tethered caching service prevents computers from going to sleep.

Feature Details:

Apps can now be set to require a tethered connection to a Mac computer to install the app. The computer will share its Ethernet connection and cache app downloads, allowing you to install apps on a large number of iOS devices faster than installing apps via a Wi-Fi connection. App updates will not require tethering; this setting is for initial installations of an app only.

To access this feature in the JSS, navigate to **Mobile Devices** > **Mobile Device Apps**, and select the **Require tethered network connection for app installation** checkbox on the General tab. This checkbox is only displayed if "Install Automatically/Prompt Users to Install" is chosen in the **Distribution Method** pop-up menu.

Note: It is recommended that you ensure iOS devices are plugged in to the computer. In addition, ensure an Update Inventory command is completed to update the tethered status. This guarantees app installations do not hang in a pending state.

Computer Management Capabilities

Added Reporting Capabilities for Apple's XProtect Security Feature

- You can now view the version of XProtect Definitions installed on a computer (for computers with macOS 10.9 or later).
  To access this feature in the JSS, navigate to the Security category in the Inventory tab of computer inventory information.
- You can now create an advanced computer search with the "XProtect Definitions Version" criteria.
  To access this feature in the JSS, navigate to **Computers** > **Search Inventory,** and click **New** to create an advanced computer search.
- You can now create a smart group with the "XProtect Definitions Version" criteria.
  To access this feature in the JSS, navigate to **Computers** > **Smart Computer Groups,** and click **New** to create a smart computer group.

Re-enrollment Settings for Computers and Mobile Devices

The JSS now allows you to choose settings that clear inventory information for computer and mobile devices during re-enrollment with the JSS. You can choose to clear the information from the following categories of a device's inventory information:

- User and Location category
- User and Location History category
- Policy Logs category
  In addition, when you clear the information in the Policy Logs category, the logs for a policy that are specific to the computer being re-enrolled are also cleared.
- Management History category

To access this feature in the JSS, navigate to **Settings** > **Re-enrollment**.

Healthcare Listener Enhancements

The JSS now allows you to add rules for the Healthcare Listener. Rules are a group of settings that enable the JSS to automatically send remote commands to mobile devices when the Healthcare Listener receives an ADT message. When adding a rule, you specify the following:

- The remote command you want to automatically send to mobile devices
- The ADT message the Healthcare Listener can receive
- The fields in the ADT message you want to map to an attribute in mobile device inventory information

In addition, you can now enable an email notification for each rule.

You can now choose the following remote commands:

- Lost Mode

- Clear Passcode
- Lock Device

You can now choose the following ADT message types:

- Admit/Visit Notification (ADT-A01)
- Cancel Admit/Visit Notification (ADT-A11)
- Cancel Transfer (ADT-A12)
- Cancel Discharge/End Visit (ADT-A13)

To access the new features in the Healthcare Listener, navigate to **Settings** > **Infrastructure Managers** > select the Infrastructure Manager that hosts a Healthcare Listener.

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 v9.100.0, go to:

https://www.jamf.com/jamf-nation/feature-requests/versions/171/casper-suite-9-100-0

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

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
v9.100.0	Change to SSL certificates issued by the JSS built-in CA	SSL certificates issued by the JSS built-in CA now include a "Subject Alternative Name" (SAN) extension to meet the updated requirements for SSL certificates from Google Chrome. As of Chrome 58, SSL certificates must include a "Subject Alternative Name" (SAN) extension.
v9.100.0	Removed product documentation from the JSS Installers	The following PDF files have been removed from the JSS Installers: *Casper Suite Release Notes* *Casper Suite Administrator's Guide* *QuickStart Guide for Managing Computers* *QuickStart Guide for Managing Mobile Devices* *Jamf Software Server Installation and Configuration Guide for Mac* *Jamf Software Server Installation and Configuration Guide for Windows* *Jamf Software Server Installation and Configuration Guide for Linux* *Manually Installing the Jamf Software Server* Links to this documentation in web-based format are now available on the JSS Installer download page on Jamf Nation. To access this page, log in to Jamf Nation and go to: https://www.jamf.com/jamf-nation/my/products
v9.100.0	Incremental upgrade required when using a policy to upgrade computers with macOS 10.9 or earlier t o macOS 10.12.4 or later	When using a policy to upgrade computers with macOS 10.9 or earlier to macOS 10.12.4 or later, you must first perform an incremental upgrade to any version between macOS 10.10 and macOS 10.12.3 . You cannot upgrade a computer with macOS 10.9 or earlier directly to macOS 10.12.4 or later without first performing this incremental upgrade. If you have questions or experience any issues during an upgrade, contact your Jamf account representative.

Starting with...	Change or Consideration	Description
v9.99.0	Connection to Apple GSX requires TLS 1.2	The Casper Suite v9.99.0 and later use TLS 1.2 for GSX by default, regardless of Java version. For the Casper Suite v9.98 or earlier, you must upgrade to Java 1.8 to maintain GSX connection.
v9.99.0	Removed support for Home Screen Layout web clips for mobile device configuration profiles	Web clips can no longer be set for the Dock or page layouts in the Home Screen Layout payload for mobile device configuration profiles. After upgrading to v9.99.0 or later, previously set web clips will no longer display when viewing mobile device configuration profiles in the JSS.
v9.98	Change to trust settings of Tomcat SSL certificates for user-initiated enrollment	As a result of an Apple security feature, beginning with iOS 10.3, during user-initiated enrollment of a device, the JSS built-in certificate authority (CA) signed Tomcat SSL certificate is not trusted by default, causing the MDM profile installation to fail. This is also true of any Tomcat SSL certificates that are self-signed or issued from a CA that the device does not trust by default. In previous versions of iOS, installing the CA certificate during enrollment caused the device to trust the CA but this is no longer the case. This is the result of intended behavior by Apple to avoid significant security vulnerabilities and will not be resolved. It is recommended that you obtain a publicly trusted web server certificate to avoid security vulnerabilities. For a list of trusted certificates for iOS devices, see the following Apple Knowledge Base article: https://support.apple.com/en-us/HT204132
v9.98	Extended startup time when upgrading (one-time impact)	When upgrading from v9.97 or earlier to v9.98 or later, an additional database index is added during the initial server startup to improve performance of applications table queries. This one-time extended startup could take anywhere from a few additional minutes to several additional hours, depending on the size of your applications table and the hardware used in your environment. It is important that you do not stop the startup process. If you have questions or experience any issues during startup, contact your Jamf account representative.

Starting with...	Change or Consideration	Description
v9.98	Change to the SSL Certificate Verification Setting	The **Enable SSL certificate verification** checkbox has been changed to the **SSL Certificate Verification** pop-up menu with the options "Always", "Always except during enrollment", and "Never". For more information on this change and instructions on how to safely configure SSL certificate verification in the JSS, see the following Knowledge Base articles: ▪ Change to the SSL Certificate Verification Setting in the Casper Suite v9.98 or Later ▪ Safely Configuring SSL Certificate Verification
v9.96	Removed support for macOS 10.5 and 10.6	The Casper Suite v9.96 removes support for macOS 10.5 and 10.6. For information on removing unsupported computers from the JSS, see the Removing the Management Framework from Multiple Computers Knowledge Base article.
v9.96	Deprecated support for macOS 10.7 and 10.8	Features implemented in the Casper Suite v9.96 or later are no longer supported on computers with macOS 10.7 and 10.8. Workflows implemented prior to v9.96 will continue to function, but they may require earlier versions of the client applications.
v9.96	Change to JDS instance installation	JDS instances are no longer installed during fresh installations of the JSS.
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.
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.
v9.93	Change to `database.xml`	The Database Driver in the `database.xml` is now set to `org.mariadb.jdbc.Driver` during JSS upgrades.
v9.92	Criteria name change	The advanced search and smart group criteria **Subscriber MCC** will now be listed as **Current Carrier Network**.
v9.92	Criteria name change	The advanced search and smart group criteria **Subscriber MNC** will now be listed as **Home Carrier Network**.

Starting with...	Change or Consideration	Description
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.
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.

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.

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 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

The JSS Installer for Mac requires the following:

- Minimum operating systems:

    - macOS 10.7
    - macOS 10.8
    - macOS 10.9
- Recommended operating systems:
    - macOS 10.10
    - macOS 10.11
    - macOS 10.12

In addition, you need the following:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- macOS 10.7 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 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  https://www.mysql.com/downloads/
- Ports 8443 and 9006 available

JSS Installer for Linux

The JSS Installer for Linux requires the following:

- Minimum operating systems:
    - Ubuntu 12.04 LTS Server (64-bit)
    - Red Hat Enterprise Linux (RHEL) 6.4, 6.5, 6.6, or 7.0
- Recommended operating systems:
    - Ubuntu 14.04 LTS Server (64-bit)
    - Ubuntu 16.04 LTS Server (64-bit)
    - Red Hat Enterprise Linux (RHEL) 6.8
    - Red Hat Enterprise Linux (RHEL) 7.3

In addition, you need the following:

- 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 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

JSS Installer for Windows

The JSS Installer for Windows requires the following:

- Minimum operating systems:
  - Windows Server 2008 R2 (64-bit)
  - Windows Server 2012 (64-bit)
- Recommended operating systems:
  - Windows Server 2012 R2 (64-bit)
  - Windows Server 2016 (64-bit)

In addition, you need the following:

- 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 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  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

The following functionality has been deprecated:

- **Recon.exe—**Starting with v9.100.0, Jamf is no longer distributing Recon.exe as part of the Casper Suite. Jamf will end support for Recon.exe at the end of 2017 and continue to offer technical support for existing Recon.exe customers until December 31, 2017. Note that this change is specific to *Recon.exe*. *Recon.app* features and functionality will stay intact.
- **Self Service Plug-in Bundles**—Support for Self Service Plug-in bundles will be removed in a future version of the Casper Suite.
- **Managed Preferences**—Support for managed preferences will be removed in a future version of the Casper Suite. It is recommended that you start using macOS configuration profiles to define settings and restrictions for computers and users.
- **Provisioning Profiles**—The ability to upload and deploy provisioning profiles using the JSS will be removed in a future version of the Casper Suite. It is no longer necessary to manually upload provisioning profiles to authorize the use of in-house apps. For more information, see the following documentation from Apple:
  Creating Your Team Provisioning Profile

  If you need assistance or have questions, contact your Jamf account representative.

Bug Fixes and Enhancements

Jamf Software Server

- Fixed an issue that caused unnecessary logging in the JSS when the JSS is integrated with a network access management service.
- Fixed several performance issues in the standard Jamf Cloud environment.
- [PI-000078] Fixed an issue that caused the QuickAdd.pkg to be signed by a previously uploaded certificate when replacing the signing certificate used for enrollment.
- [PI-002230] Fixed an issue that caused the number of Smart Groups to be reported inaccurately on the JSS dashboard.
- [PI-002312] The JSS no longer removes user and location information from computer or mobile device inventory information when the device is enrolled with the JSS via a PreStage enrollment with the **Require Authentication** option selected.
- [PI-002380] Fixed an issue that prevented certificates from displaying in device inventory records when the certificate's Common Name field was left blank.
- [PI-002485] Fixed an issue that caused the local users to be incorrectly listed as MDM capable in the computer's inventory. (If the **Allow MDM Profile Removal** checkbox in the PreStage Enrollments is deselected, the `sudo jamf mdm -userLevelMdm` command will not work for any additional local users. This is the expected behavior.)
- [PI-002509] Fixed an issue that caused a blank page to display when adding VPP Store apps in the JSS.
- [PI-002795] The JSS now gives you the option to clear the management history for computers and mobile devices during re-enrollment.
- [PI-002821] Fixed an issue that resulted in some information not being returned when using the JSS API to get mobile device data.
- [PI-002905] Fixed an issue that caused the External CA to be active after disabling it in the JSS.
- [PI-002981] Fixed an issue that caused the "Reveal in Finder" option to fail in Capser Admin v9.96.
- [PI-003139] Fixed an issue that caused the Restricted Software policy to fail to run if a Shutdown or Restart command was waiting for a user response.
- [PI-003225] Fixed an issued that resulted in multiple email notifications being sent for Restricted Software violations.
- [PI-003277] Fixed an issue that caused incorrect data in the Managed App Configuration when in clustered environments.
- [PI-003352] Fixed an issue that sometimes caused MDM-related information to be deleted from the JSS during enrollment of macOS devices.
- [PI-003576] Fixed an issue that prevented user and location information from being entered in computer and mobile device inventory information during re-enrollment with the JSS via a PreStage enrollment with the **Require Authentication** and **Use existing location information, if applicable** options selected.

- [PI-003601] Fixed an issue that prevented any information from being displayed on the Lock screen of a mobile device with Lost Mode enabled. As a result, the JSS now limits the number of characters to 255 in the **Phone Number** field in the Enable Lost Mode pane.
- [PI-003674] Fixed an issue that prevented email addresses from displaying in debug logs when sending VPP invitations. This issue was fixed in v9.99.0.
- [PI-003718] Fixed an issue that resulted in the Jamf binary reporting a failure even if the password update policy was successful.
- [PI-003724] The JSS no longer displays database errors when certain emoji characters are used. An unknown character symbol is displayed instead.
- [PI-003726] Fixed an issue with the Restricted Software scope.
- [PI-003752] Fixed an issue that caused upgrades for Casper Suite v9.98 to fail if duplicate jss_cluster_settings tables existed.
- [PI-003860] Fixed an issue that resulted in a warning the JAMFSoftwareServer.log if the JSS had a large number of users (e.g., 50,000).
- [PI-003870] Fixed an issue that caused communication to fail with Apple TV devices when certain configuration profiles were removed.
- [PI-003903] Fixed an issue that resulted in Tomcat needing to be restarted before certain Smart Mobile Device Groups could be deleted.
- [PI-003924] Fixed an issue that cleared the selection of the **Operating System** pop-up menu in the JSS when a Customer API update request was sent to the /mobiledeviceapp resource.
- [PI-003955] Fixed an issue that caused a significant delay when using Casper Focus to focus student devices in a class.
- [PI-003961] Fixed an issue that caused the JSS to incorrectly send a remote command via the Healthcare Listener to a mobile device that is not enrolled with the JSS. The command would fail causing unnecessary email notifications.
- [PI-003973] The JSS now returns correct results for a smart group or advanced search with the "System Integrity Protection" or "Gatekeeper" criteria when using invalid or unsupported values.
- [PI-003975] Fixed an issue that prevented the JSS from deploying a computer configuration profile that was manually created using Apple’s Profile Manager if the configuration profile contained a payload that was not available in the JSS.
- [PI-004005] Fixed an issue that caused details for a second LDAP user group to not populate correctly when importing from Active Directory.
- [PI-004008] Fixed an issue that prevented an installed certificate from displaying in device inventory records when two certificates were incorrectly considered equivalent in the JSS.
- [PI-004031] Fixed an issue that caused t he JSS to become unresponsive when assigning or un-assigning several (e.g., 1000) VPP licenses simultaneously.
- [PI-004050] The JSS now correctly displays email notifications in the Healthcare Listener.
- [PI-004071] Additional model identifiers for iOS devices have been added to the JSS.
- [PI-004083] Fixed an issue that incorrectly caused computer configuration profiles to redeploy multiple times.
- [PI-004087] Fixed an issue that prevented communications with Apple’s Volume Purchase Program when using an HTTP proxy server.

- [PI-004111] The JSS now correctly maps LDAP extension attributes for computers and mobile devices.
- [PI-004112] Fixed an issue that resulted in user extension attribute information being removed if users imported by class in Apple School Manager already existed in the JSS.
- [PI-004115] Fixed an issue that caused the JSS to send unnecessary requests to the Jamf Cloud Distribution Service (JCDS) during package uploads.
- [PI-004102] Fixed an issue that caused the networkStateChange trigger to block communication with the jamf agent until the policy completed.
- [PI-004093] Fixed an issue that caused a policy limited to a site to become unable to be edited or removed.

JSS Installer for Windows

[PI-004049] Fixed an issue that prevented Tomcat from starting after upgrading the JSS to v9.98 or later using the JSS Installer for Windows.

Recon

[PI-004096] Fixed an issue that caused a connection error when attempting to enroll clients.

Known Issues

Third-party Software

The following issues are the result of bugs that have been found in third-party software. Jamf has filed defects for these bugs and is awaiting their 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.
- [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-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-009450] A macOS configuration profile with a Password payload incorrectly enforces a number of complex characters equal to the last value used.

Jamf Software Server

The following issues are known in the JSS:

- 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.
- To install applications on Apple TV devices, tvOS 10.2 or later is required. Although earlier versions do not support app installation, the **Apps** tab displays in the JSS for all mobile device records.
- When Apple TV devices are in Single App Mode, users cannot install apps.
- [PI-003614] Apple TV devices do not properly clear from the scope column when the device record is deleted. If scoped to a configuration profile, the profile will still list the removed devices in the number of targeted devices.
- [PI-003940] Beginning with the Casper Suite v9.98, Android devices do not update after first enroll. The following commands are also unable to complete: Install Personal Device Profile, Wipe Institutional Device, and Lock Device.
- [PI-003952] Attachments added to Apple TV devices during enrollment do not display in the devices’ inventory information.
- [PI-004196] When Single Sign-On authentication is enabled in the JSS, sometimes administrators are not able to reliably configure which sites are visible to a user during user-initiated enrollment.
- [PI-004205] When using AirPlay Permissions, the JSS fails to automatically send Apple TV passwords to iOS devices.
  Workaround: Use a configuration profile to send an Apple TV password to iOS devices.

Casper Focus

Due to the issues known in Casper Focus, Jamf does not recommend using Casper Focus with iOS 9.3.2 or later or the Casper Suite v9.96 or later. For the best iOS classroom management experience, Jamf recommends using Apple Classroom.

The following issues are known in Casper Focus:

- [D-008567] When a student device with iOS 8 is focused on a website, multiple icons with the website link are displayed.
- [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.
- [PI-002319] Changing the focus from one app to another fails on student devices with iOS 9.3.2 to 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.
- [PI-002359] Focus commands fail on student devices with iOS 10 until the devices are reset.

- [PI-002858] Changing the focus from an app to a website fails on student devices with iOS 9 or 10.
- [PI-004106] Focusing student devices on an app or the attention screen fails.
- [PI-004107] Focusing student devices with iOS 11 on iBooks or Safari fails.

If you need assistance or have questions, contact your Jamf account representative.