Casper Suite Release Notes

Version 9.99.0

jamf

© copyright 2002-2017 Jamf. All rights reserved.

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

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of Jamf.

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

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

The CASPER SUITE, COMPOSER®, the COMPOSER Logo®, Jamf, the Jamf Logo, JAMF SOFTWARE®, the JAMF SOFTWARE Logo®, RECON®, and the RECON Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC 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 product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

Contents

What's New in This Release

New Casper Suite Versioning Schema

This release of the Casper Suite introduces a new versioning schema that is based on the Semantic Versioning specification (semver.org). This schema will be used for all Casper Suite applications, including those distributed through the App Store.

The new versioning schema uses the following incremental numbering format:

MAJOR.MINOR.MAINTENANCE

For example, based on v9.99.0 as the current release, the next incremental version will be one of the following:

- Major: **10**.0.0
- Minor: 9.**100**.0
- Maintenance: 9.99.**1**

This change is being made in an effort to standardize how version numbers are assigned so that they can be incremented and compared properly. In addition, with the MAJOR.MINOR.MAINTENANCE format, a specific type of increment to a version number will clearly indicate the level of changes introduced in that version. For example, if a version number is incremented from 10.0.0 to 10.0.1, this indicates a MAINTENANCE-level release.

Before You Upgrade: If you have configured smart groups, advanced searches, or extension attributes based on Casper Suite version number criteria, you will need to update that information to reflect the new versioning schema. In addition, you may need to update API scripts or other custom logic created outside the Casper Suite.

iOS Management Capabilities

Lost Mode Enhancements

- The following Lost Mode parameters are now available to collect information from supervised mobile devices with iOS 10.3 or later: Horizontal Accuracy, Vertical Accuracy, Altitude, Speed, Course, and Timestamp.
  When Lost Mode is enabled, this information is displayed in the Security category in the Management tab of mobile device inventory information.
- You can now ensure Lost Mode is re-enabled after an enrollment event has completed for supervised mobile devices with iOS 10.3 or later.
  To access this feature in the JSS, navigate to the Security category in the Management tab of mobile device inventory information and select the **Always enforce Lost Mode** checkbox.
  Note: This option is selected by default.

- Lost Mode parameters have been removed from the General category and now are available in the Security category in inventory information for a mobile device.

iOS Remote Command Enhancements

You can now choose to clear the passcode on a device when sending a Restart or Shut Down remote command to a mobile devices with iOS 10.3 or later. To access this feature in the JSS, navigate to **Action** > **Send Remote Command s** , and then click **Shut Down Device** or **Restart Device** to view the **Clear Passcode on the device** checkbox.

iOS Configuration Profile Enhancements

You can now configure Default and Data Access Point Name (APN) settings in the Cellular payload of the mobile device configuration profile for mobile devices with iOS 10.3 or later. To access this feature in the JSS, navigate to **Mobile Devices** > **Configuration Profiles > Cellular.**

Computer Management Capabilities

Added Reporting Capabilities for Apple macOS Security Features

- You can now view the status for the following security settings:
  - System Integrity Protection (for computers with macOS 10.11 or later)
  - Gatekeeper (for computers with macOS 10.9 or later)

  To access these features in the JSS, navigate to the Security category in the Management tab of computer inventory information.
- You can now create an advanced computer search with the following criteria:
  - System Integrity Protection
  - Gatekeeper

  To access these features 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 following criteria:
  - System Integrity Protection
  - Gatekeeper

  To access these features in the JSS, navigate to **Computers** > **Smart Computer Groups,** and click **New** to create a smart computer group.

Apple Education Support Enhancements

- You can now specify a class description format. This is applied to all classes imported from Apple School Manager. The description is displayed in Apple's Classroom app.
  To access this feature in the JSS, navigate to **Settings** > **Mobile Device Management** > **Apple Education Support**.

- Classes now display information from Apple School Manager.
  To access this feature in the JSS, navigate to **Mobile Devices** > **Classes**.
- You can now integrate the JSS with more than one instance of Apple School Manager. Integrating with more than one instance allows you to choose the instance of Apple School Manager when performing a class or user import. In addition, the JSS can perform multiple instances of force syncing.
  To access this feature in the JSS, navigate to **Settings** > **Mobile Device Management** > **Apple Education Support**.

Network Integration Enhancements

Added support for the Cisco MDM API v2 when integrating the JSS with Cisco Identity Services Engine (ISE) in the Network Integration settings in the JSS.
To access network integration in the JSS, navigate to **Settings** > **Network Organization** > **Network Integration**.

PKI Certificates Enhancements

You can now view a list of devices/usernames associated with "Other" Certificate Authorities.
To access this feature in the JSS, navigate to **Settings** > **Global Management** > **PKI Certificates** . Next, go to the **Certificate Authority** tab, click "All" in the " Other" row in the Certificate Authority table, and click the certificate you want to view the associated configuration profile for. Details are displayed for certificates with 100 or fewer devices.

Other Enhancements

- Packages uploaded to an Apple Filing Protocol (AFP) or Server Message Block (SMB) share can now be validated with the SHA-512 algorithm. Existing packages with an MD5 checksum are not automatically upgraded to SHA-512. To upgrade existing packages, see Calculating a Checksum in the "Managing Packages" section of the *Casper Suite Administrator's Guide*.
- Package validation now occurs after the package has been downloaded. Packages will be validated if you choose "Always" or "When checksum is present" from the **Package Validation** pop-up menu.
  To access this feature in the JSS, navigate to **Settings > Computer Management > Security**.
- The hashing algorithm has now been improved for JSS user account passwords that are stored on the JSS server.

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 v9.99.0, go to:

https://www.jamf.com/jamf-nation/feature-requests/versions/170/casper-suite-9-99-0

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
v9.99.0	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	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 Jamf Support.
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

Starting with...	Change or Consideration	Description
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**.
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.

Starting with...	Change or Consideration	Description
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—**Jamf will stop distributing Recon.exe in a future version of the Casper Suite and will end support for Recon.exe at the end of 2017. Jamf will continue to offer technical support for existing Recon.exe customers until December 31, 2017. This change is specific to Recon.exe. Recon features and functionality outside of Recon.exe 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

- The JSS now correctly displays the list of "Patch Reporting Software Title" criteria values in descending order with the latest version at the top of the list when creating a smart computer group or advanced computer search.
- Improved JSS performance when importing classes to the JSS from Apple School Manager.
- Fixed an issue that prevented the JSS from correctly displaying the Class Naming Format setting in the Apple Education Support settings.
- Fixed an issue that caused Apple TV devices to be present in two smart groups when switching PreStage enrollments and re-enrolling an Apple TV if **Enrollment Method: PreStage enrollment** was selected as smart group criteria.
- [D-010269] Fixed an issue that prevented a computer configuration profile with a Passcode or Directory payload from displaying in a computer's inventory information when the computer was enrolled with the JSS via a PreStage enrollment. This issue was fixed in v9.98.
- [PI-001048] Fixed an issue resulted in a syntax error if a smart computer group containing both a "Filevault2 Partition Encryption State" criteria and an OR operator was saved.
- [PI-001350] The JSS now retains the names of mobile devices in the Mobile Device Names tab after adding new devices and refreshing the PreStage Enrollments settings.
- [PI-001393] Fixed an issue that caused a smart mobile device group or an advanced search to fail to return results if an OR operator was used for a bundle identifier.
- [PI-001746] Fixed an issue that caused the JSS to sometimes incorrectly display the enrollment date for a new computer or mobile device as "Today" instead of "Yesterday", if the JSS was hosted in a different time zone than the JSS admin.
- [PI-002163] Fixed an issue that prevented the default number of policy log and advanced computer search entries shown from being changed.
- [PI-002171] Fixed an issue that resulted in some packages failing to upload from Casper Admin to a JAMF Cloud Distribution Service (JCDS) or an Amazon cloud distribution point.
- [PI-002179] Fixed an issue that caused a targeted Apple TV device assigned to a site to not display in the smart mobile device group view.
- [PI-002241] Fixed an issue that changed OR operators to AND operators when deleting criteria from a smart group and did not generate a new operator menu between search criteria.
- [PI-002314] Fixed an issue that caused the JSS to become unresponsive in large environments (e.g., 40,000 devices) when determining device compliance to a network access management service.
- [PI-002487] Fixed an issue that caused local users to be incorrectly listed as MDM capable in the computer's inventory record when re-enrolling a computer.
- [PI-002705] Fixed an issue that prevented the JSS from displaying a "Content-Type" header.
- [PI-002721] Fixed an issue that prevented a warning message from being displayed if an extension attribute associated with a smart group was deleted.

- [PI-002792] Fixed an issue that prevented the Last Enrollment date from populating for computers enrolled via DEP.
- [PI-003005] The JSS no longer allows information in the Roster category of user inventory information imported from Apple School Manager to be edited in the JSS.
- [PI-003027] Fixed an issue in Jamf Cloud environments that caused search results to not be returned if the search criteria contained special characters, including comma-separated values.
- [PI-003131] Fixed an issue that caused two calculations to be performed for each smart group if changes were made to a computer record that included inventory updates.
- [PI-003192] Fixed an issue that caused navigation to fail to load for computer configuration profiles when uploading certain custom property list (.plist) files.
- [PI-003223] Fixed an issue that sometimes prevented users from being imported to the JSS from Apple School Manager if the matching criteria used an operator of "contains" or "ends with".
- [PI-003345] Fixed an issue that resulted in the criteria view of a smart mobile device group or smart computer group to not display if the name of the group was the same as the search criteria.
- [PI-003348] Fixed an issue that caused the JSS to become unresponsive when updating several (e. g., 60) App Store apps simultaneously if the **Automatically update app** checkbox was selected for mobile device or computer apps.
- [PI-003384] Fixed an issue that could result in the unauthorized remote disclosure of Extension Attribute information.
- [PI-003446] Fixed an issue that caused Self Service Mobile for iOS to sometimes fail to connect to the JSS if an in-house eBook is made available in Self Service.
- [PI-003474] Fixed an issue that sometimes incorrectly allowed patch services to run when the JSS was reconfigured as a child instance in a clustered environment.
- [PI-003484] Fixed an issue that caused syncing from Apple School Manager to the JSS to remain in a pending state.
- [PI-003544] Fixed an issue that caused the OS update process and other commands to fail if an OSUpdateStatus command was present before the ScheduleOSUpdate command completed.
- [PI-003545] Fixed an issue that caused no results to be returned if multiple OR operators in a smart computer group for "Enrollment Method: PreStage enrollment" were used.
- [PI-003565] Fixed an issue that prevented the JSS from returning to Personal Device Profile settings after deleting a personal device profile with no certificates configured.
- [PI-003572] Fixed an issue that caused Self Service Mobile for iOS and the Self Service web clip to become unresponsive if apps made available in Self Service have special characters in the app description and the environment is hosted on Jamf Cloud.
- [PI-003630] Fixed an issue with error logging when scoping an eBook or in-house app to an iOS device with Self Service.
- [PI-003637] Fixed an issue with in-house apps that caused the hosting location to default to external when the App URL was left blank. Due to modifications in the Customer API, the hosting location now defaults to internal when the App URL is left blank.
- [PI-003642] The JSS now performs patch reporting and patch notifications for McAfee Endpoint Security for Mac. (The McAfee Endpoint Protection for Mac software title has been removed from the JSS.)
- [PI-003651] Improved the performance of smart group queries that contain extension attribute criteria.

- [PI-003653] Fixed an issue to prevent cache settings in Jamf Cloud instances from being modified via the Universal Application Programming Interface (UAPI).
- [PI-003659] Fixed an issue that prevented an operator precedence from being added via the API to a smart computer group search.
- [PI-003664] Fixed an issue that caused a smart computer group to not retain membership if the name of an extension attribute was changed.
- [PI-003667] Fixed an issue that caused the JSS to display an "Out of Memory" error when loading the dashboard view for a policy with a large amount of history data.
- [PI-003710] Fixed an issue that caused the `jamfsoftwareserver.log` to unnecessarily display a “Thread starvation or clock leap detected” warning messages.
- [PI-003744] Fixed an issue that increased error logging in the JSS when inventory records were updated. This issue is limited to customers who had previously run v8.0 or v8.1 of the Casper Suite.
- [PI-003754] The JSS now uses updated Apple payload type specifications for the SmartCard payload of a macOS configuration profile.
- [PI-003756] Fixed an issue that allowed unauthorized access to objects in sites.
- [PI-003763] Fixed an issue that prevented in-house apps from updating despite editing the version and app archive (.ipa) file in the JSS.
- [PI-003769] Fixed an issue that prevented the `InstallApplication` command from running if the **Automatically update app** checkbox was selected for mobile device apps, causing the apps to not update.
- [PI-003781] Fixed an issue that caused the JSS to become unresponsive when updating several (e. g., 60) iOS apps simultaneously.
- [PI-003798] Fixed an issue that prevented apps made available in Self Service Mobile for iOS from loading quickly.
- [PI-003819] Fixed an issue that caused a policy to fail to run on macOS v10.9 when containing a package hosted on an HTTP distribution point.
- [PI-003839] Fixed an issue that caused an "InvalidDataAccessApiUsageException" error to show up repeatedly in the `JAMFSoftwareServer.log`.
- [PI-003934] Fixed an issue that caused GSX connection to fail for the Casper Suite v9.99.0 or later. For the Casper Suite v9.98 or earlier, users must upgrade to Java 1.8 to maintain GSX connection.
- [PI-003935] Fixed an issue in the JSS that caused some information (e.g., Full Name, Grade, Status, etc.) to be missing from the Students or Teachers payload of Classes in Mobile Devices if the information was imported from Apple School Manager (ASM).

Jamf Software Server Installer for Linux

[PI-002927] Fixed an issue that caused the JSS Installer for Linux to incorrectly remove files and directories from `/jss/location/tomcat/webapps` that are not installed by the installer when upgrading.

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.
- 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.
- The JSS may become unresponsive when assigning or un-assigning several (e.g., 1000) VPP licenses simultaneously.
- [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-009355] Starting with the Casper Suite v9.98, a significant delay occurs when using Casper Focus to focus student devices that are in a class. Until the issue is resolved, Jamf does not recommend using Casper Focus with devices that are managed by the Casper Suite v9.98 or later.

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

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.
- [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.
- [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.