Casper Suite Release Notes

Version 9.98

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

Important Notice—Increased Startup Time

When upgrading from v9.97 or earlier to v9.98 or later, an additional database index will be 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. For example, the estimated startup time for an applications table with 7 million applications is around 4 minutes, whereas the estimated startup time for an applications table with 200 million applications would be close to 2 hours.

It is important that you do not stop the startup process. If you have questions or experience any issues during startup, contact Jamf Support.

Compatibility with iOS, macOS, and tvOS

The Casper Suite is now compatible with iOS 10.3, macOS v10.12.4, and tvOS 10.2.

iOS Management Capabilities

iOS Remote Commands

- Shut Down Device remote command for mobile devices (iOS 10.3 or later):
  - You can now remotely shut down a mobile device.
    To access this feature in the JSS, navigate to the Management tab of mobile device inventory information.
  - You can now use mass actions to remotely shut down mobile devices.
    To access this feature in the JSS, view mobile device group memberships or view simple or advanced search results, navigate to **Action** > **Send Remote Commands** > **Shut Down Device**.
- Passcode Lock Grace Period remote command for Shared iPad (iOS 10.3 or later):
  - You can now remotely update the passcode lock grace period for Shared iPad.
    To access this feature in the JSS, navigate to the Management tab of mobile device inventory information.
  - You can now use mass actions to remotely update the passcode lock grace period for Shared iPad.
    To access this feature in the JSS, view mobile device group memberships or view simple or advanced search results, navigate to **Action** > **Send Remote Commands** > **Update Passcode Lock Grace Period**.

- Restart Device remote command for mobile devices (iOS 10.3 or later):
  - You can now restart supervised devices.
    To access this feature in the JSS, navigate to the Management tab of mobile device inventory information.
  - You can now use mass actions to remotely restart devices.
    To access this feature in the JSS, view mobile device group memberships or view simple or advanced search results, navigate to **Action** > **Send Remote Commands** > **Restart Device**.
- Play Lost Mode Sound when configuring the Lost Mode remote command for a mobile device (iOS 10.3 or later):
  - You can now play a sound on a supervised device when Lost Mode is enabled.
    To access this feature in the JSS, navigate to the Management tab of mobile device inventory information.

iOS PreStage Enrollments

- The "Cloud Storage" skip step has been added to a mobile device PreStage enrollment.
- The **Disallow MDM Profile Removal** checkbox has been renamed to **Prevent unenrollment**.
- The **Require Authentication** checkbox has been renamed to **Require credentials for enrollment**.
  To access these features in the JSS, navigate to **Mobile Devices** > **PreStage Enrollments**.

iOS Configuration Profiles

- You can now issue Symantec certificates to mobile devices—either one certificate for each device in the scope, or one certificate for all devices in the scope.
  To access this feature in the JSS, navigate to **Mobile Devices** > **Configuration Profiles > Certificate.**
- The following Restrictions payload settings are now available for supervised devices with iOS 10.3 or later:
  - Allow modifying the AirPlay and View Screen permissions for managed classes
    Selecting this restriction prevents students from blocking screen observation and from changing AirPlay settings on their device.
  - Allow dictation
    Selecting **Allow dictation** prevents users from dictating text.
  - Allow connection to unmanaged Wi-Fi networks
    Selecting this restriction prevents users from connecting to any Wi-Fi networks not deployed through the JSS.
    Warning: If left unchecked, and if at least one Wi-Fi payload is not configured on scoped devices through a configuration profile, devices may lose all network connectivity.

macOS Management Capabilities

macOS Configuration Profiles

- The following new restrictions have been added to the Functionality tab of the Restrictions payload in macOS configuration profiles:
  - Allow Touch ID to unlock device
  - Allow iCloud Desktop & Documents

  To access these features in the JSS, navigate to **Computers** > **Configuration Profiles** > **Restrictions**.
- The SmartCard payload has been added for macOS configuration profiles. The SmartCard payload controls restrictions and settings for SmartCard pairing.
  To access this feature in the JSS, navigate to **Computers** > **Configuration Profiles** > **SmartCard**.
- You can now issue Symantec certificates to computers in macOS configuration profiles—either one certificate for each device in the scope, or one certificate for all devices in the scope.
  To access this feature in the JSS, navigate to **Computers** > **Configuration Profiles** > **Certificate.**

tvOS Management Capabilities

tvOS Remote Commands

- Restart Device remote command for Apple TV devices (tvOS 10.2 or later):
  - You can now restart supervised devices.
    To access this feature in the JSS, navigate to the Management tab of mobile device inventory information.
  - You can now use mass actions to remotely restart tvOS devices.
    To access this feature in the JSS, view mobile device group memberships or view simple or advanced search results, navigate to **Action > Send Remote Commands > Restart Device**.
- Wipe Device remote command for Apple TV devices:
  - You can now remotely wipe tvOS devices.
    To access this feature in the JSS, navigate to the Management tab of mobile device inventory information.
  - You can now use mass actions to remotely wipe tvOS devices.
    To access this feature in the JSS, view mobile device group memberships or view simple or advanced search results, navigate to **Action** > **Send Remote Commands** > **Wipe Device**.

tvOS PreStage Enrollments

You can now enroll Apple TV devices with tvOS 10.2 or later via a PreStage enrollment.

PreStage enrollment options for tvOS include:

- Make MDM Profile Mandatory
  Selecting **Make MDM Profile Mandatory** will require users to apply the MDM profile for enrollment.
  Note: This payload is not required for Auto Advance to work, but will temporarily show onscreen before automatically advancing past it.
- Auto Advance through Setup Assistant
  Selecting this option automatically sets up all available steps in the Setup Assistant for tvOS devices.
  Note: Ethernet connection required.
  When using automatic setup, do not use the Siri Remote, as it will disrupt enrollment.
  Your Siri Remote is not automatically paired with your Apple TV when using Auto Advance.
- Skip Setup Assistant Options
  Selected items are not deployed in the Setup Assistant during enrollment.

To access this feature in the JSS, navigate to **Mobile Devices** > **PreStage Enrollments**.

tvOS Configuration Profiles

The following configuration profile payloads are compatible with tvOS 10.2 or later:

- General
- Restrictions
- Wi-Fi
- Certificate
- SCEP
- Single App Mode
- Global HTTP Proxy
- Conference Room Display

Note: A configuration profile will deploy containing both the iOS and tvOS selected options to all devices in scope. Devices will ignore the restrictions that do not pertain to their device type.

To access this feature in the JSS, navigate to **Mobile Devices** > **Configuration Profiles**.

Single App Mode payload settings for Apple TV devices

You can now set supervised tvOS devices to Single App Mode. Single App Mode locks scoped devices to a selected app. Apple TV devices in Single App Mode can still use AirPlay, unless restricted via the Restrictions payload.

Note: Attempting to lock Apple TV devices to an in-house or third-party app that does not yet exist on the devices will cause an error. To avoid this issue, ensure the app is installed on scoped devices before configuring Single App Mode.

The following settings can be enforced when in Single App Mode:

- Touch
  When enforced, all touch input is disabled on the device including Siri Remote and any paired iOS devices.
- Auto-Lock
  When enforced, Auto-Lock is disabled, preventing the tvOS screen saver from appearing.

The following settings can be enforced or set to allow users to change when in Single App Mode:
Note: When enforced, these settings are disabled.

- VoiceOver
- Zoom
- Invert Colors

Restrictions payload settings for Apple TV devices

Added tvOS restrictions available through configuration profiles include:

- Disable AirPlay (supervised devices only)
  Selecting **Disable AirPlay** prevents AirPlay on scoped tvOS devices. Scoped tvOS devices will not appear in a list of available devices when attempting to AirPlay on Apple TV.
- Require passcode on first AirPlay pairing
  You can now select **Require passcode on first AirPlay pairing** for tvOS devices to require devices to provide the AirPlay password.
  Note: Does not require tvOS 10.2 or later.
- Disable control using Remote app
  Selecting **Disable control using Remote app** prevents iOS devices from using the Remote app, and instead requires the use of the remote provided by Apple.
  Note: This restriction does not prevent the use of the Siri Remote.
- Allow keyboard continuation
  Selecting **Allow keyboard continuation** prevents iOS keyboards from inputting text on Apple TV.

Conference Room Display payload settings for Apple TV devices

You can now set supervised tvOS devices to Conference Room Display mode from the JSS. Conference Room Display locks scoped Apple TV devices to a black wallpaper screen, downloads a default screen saver, and displays a message if configured.

Note: If a tvOS device is running Single App Mode, or if Single App Mode is deployed with Conference Room Display, Conference Room Display will override Single App Mode.

Apple Education Support

- You can now configure a class naming format in the JSS when importing classes from Apple School Manager. This prevents editing of a class display name after the class has been imported to the JSS.
- Improved deployment of EDU profiles.

- The JSS now includes the following user information in the Roster category of user inventory information for users imported from Apple School Manager:
  - Last Sync
  - Status
  - User Number
  - First Name
  - Middle Name
  - Last Name
  - Grade

In addition, if you import a user from Apple School Manager, you can no longer edit the Passcode Requirement field in the user's inventory information.

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

AirPlay Permissions

- You can now map AirPlay Permissions to any User and Location inventory field or extension attribute.
- AirPlay Permissions information is now included in inventory information for mobile devices.
- The JSS now displays an error for a mobile device extension attribute if the attribute is used to map to AirPlay and is being edited in the device's inventory information.

To access this feature in the JSS, navigate to **Settings > Global Management > AirPlay Permissions**.

Public Key Infrastructure

- You can now integrate with Symantec, as a third-party certificate authority (CA).
- Using the PKI Certificates settings, you can now do the following:
  - View a list of certificates in your environment (Active, Expiring, Inactive, All)
  - Add a PKI certificate authority to the JSS dashboard
  - View all certificates issued by a CA
  - Choose a custom name for each managed certificate
  - View details of a specific certificate that was issued
  - Export a certificate list for a CA

To access this feature in the JSS, navigate to **Settings > System Settings > PKI Certificates**.

Self Service Mobile for iOS

Self Service Mobile for iOS now displays a default app icon while the assigned icon loads to improve performance.

Self Service Mobile v9.98 will be available from the App Store when it is approved by Apple.

Single Sign-On

You can now configure enrollment access for any group or identity provider user when enabling Single Sign-On for user-initiated enrollment.

To access this feature in the JSS, navigate to **Settings** > **System Settings** > **Single Sign-On**.

SSL Certificate Verification

The **Enable SSL certificate verification** checkbox located in the Security settings in the JSS has been changed to the **SSL Certificate Verification** pop-up menu with the options: "Always", "Always except during enrollment", and "Never".

If you are performing a fresh install of the Casper Suite v9.98 or later, the SSL Certificate Verification setting is set to "Always except during enrollment" by default.

If you are upgrading from the Casper Suite v9.97 or earlier to the Casper Suite v9.98 or later and you previously enabled SSL certificate verification, the setting is set to "Always" by default. If you did not enable SSL certificate verification before upgrading, the setting is set to "Always except during enrollment" by default.

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

Jamf Infrastructure Manager

- You can now delete an Infrastructure Manager instance from the JSS.
- Improved the usability of the API for the Infrastructure Manager.

To access this feature in the JSS, navigate to **Settings** > **Server Infrastructure** > **Infrastructure Manager Instances**.

For instructions on how to install and configure the Infrastructure Manager, see the *Jamf Infrastructure Manager Installation Guide*.

Healthcare Listener

- You can now specify IP addresses or a range of IP addresses to accept incoming ADT messages from.
- You can now view the history of a Healthcare Listener.
- You can now track the changes that happen in the JSS via the Change Management logs for the Healthcare Listener.
- The JSS now clears the Activation Lock before sending a Wipe Device remote command to a mobile device via the Healthcare Listener.
- You can now configure email notifications to be sent to specified users when a remote command sent via the Healthcare Listener fails to send or is in a pending state.
- The JSS now displays an error for a mobile device extension attribute if the attribute is used to map to the Healthcare Listener and is being edited in the device's inventory information.
- Improved the usability of the API for the Healthcare Listener.
- Improved the communication with the Healthcare Listener and the JSS.

To access this feature in the JSS, navigate to **Settings** > **Server Infrastructure** > **Infrastructure Manager Instances** > Click the Infrastructure Manager instance that is hosting a Healthcare Listener.

Note: To take full advantage of the features and enhancements available in the Healthcare Listener, you must install the latest version of the Jamf Infrastructure Manager that hosts a Healthcare Listener.

File Extension Whitelist

- The file extension whitelist has been added to increase and enhance security for files uploaded to the web interface.
- The feature is enabled by default. You can interact with the file extension whitelist using the JSS API.

For more information on how to use the file extension whitelist, see the following Knowledge Base article:

Managing the File Extension Whitelist

Other Enhancements

- You can now change or reset the management account password when administering the management account using a policy.
- Renamed "LDAP Proxy Server" to "LDAP Proxy" in the JSS.
- Renamed "PKI" to "PKI Certificates" in the JSS.
- You can now issue Symantec certificates to personal devices—either one certificate for each device in the scope, or one certificate for all devices in the scope.

- The JSS now contains a "Server Infrastructure" settings section.
- You can now add a description to classes in the JSS.
- The Exchange Device ID is now collected in mobile device inventory information.
- All configuration profiles now appear in a device's inventory report, regardless of the device's installation method.
- You can now create smart groups and advanced searches using configuration profile names and identifiers.

Memcached Future Requirement for Clustered Environments

In the Casper Suite v9.98, Memcached is recommended, but not yet required. In future versions of the Casper Suite, Memcached will be required for clustered environments. To prepare for this change, it is recommended that you review the following information:

- Memcached Configuration for Clustered JSS Environments
- Securing Your JSS

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 v9.98, go to:

https://www.jamf.com/jamf-nation/feature-requests/versions/168/casper-suite-9-98

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
v9.98	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 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.
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.
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.

Starting with...	Change or Consideration	Description
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.
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

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 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

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 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

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 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:

- **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. If you need assistance or have questions, contact Jamf Support.
- **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 Jamf Support.

Bug Fixes and Enhancements

Jamf Infrastructure Manager

[PI-002936] You can now delete an Infrastructure Manager instance from the JSS.

Jamf Software Server

- Fixed an issue that caused a warning message to be displayed incorrectly when editing attributes in mobile device inventory information.
- Fixed an issue that caused the JSS to send a Wipe Device remote command to the wrong mobile device when the Healthcare Listener receives a Patient Transfer (ADT-A02) message.
- Fixed an issue where Apple TV devices incorrectly received the Self Service web clip.
- Fixed an issue where the Disable App Store restriction failed to install on tvOS devices when selected in a mobile device configuration profile. This caused future remote commands to remain in a pending state..
- [D-008296] The JSS now requires that a master web application be defined when enabling a clustered environment.
- [D-008932] Fixed an issue that caused the JSS Installer for Windows to incorrectly include "${catalina.home}" instead of "${catalina_home}" in the server.xml file when performing a fresh installation of the JSS.
- [D-009503] Fixed an issue where configuring the Login Window payload for a computer configuration profile also caused the **Require password immediately after sleep or screen saver begins** checkbox in the Security & Privacy payload to be incorrectly enforced.
- [D-009974] Fixed an issue where the supervision requirements text in the Restrictions payload of a mobile device configuration profile did not match the text in Profile Manager.
- [PI-002199] Fixed an issue that caused a computer's keyboard to sometimes become unresponsive when the Login Window payload of a configuration profile was configured.
- [PI-002312] Fixed an issue that caused the user and location information of a computer to be removed after enrollment via a PreStage enrollment.
- [PI-002503] Fixed an issue that prevented the JSS from supporting the use of signed URLs created with Amazon CloudFront.
- [PI-002645] Fixed an issue where mobile device profiles for macOS Server accounts did not allow username fields to be populated on devices that were left blank.
- [PI-002791] Fixed an issue where out-of-date App Store apps were not automatically updated after a recalculation.
- [PI-002847] Fixed an issue where the PreStage enrollment process failed when the Accounts payload was configured for a computer PreStage enrollment.
- [PI-002889] Fixed an issue where communication failed between Jamf Nation and the JSS when renewing a push certificate using the **Download CSR and sign later using Jamf Nation** option.

- [PI-002909] Fixed an issue that prevented advanced criteria options from displaying when creating an advanced user search.
- [PI-002917] Fixed an issue where VPP app auto import fails for apps with names exceeding 255 characters.
- [PI-002931] Fixed an issue that prevented the Set Wallpaper remote command from being sent to a device that was re-enrolled.
- [PI-002932] Fixed an issue where the value of the Screen Lock Timeout setting couldn't be changed if the Login or Security and Privacy payload already existed.
- [PI-002963] Fixed an issue that caused the Certificates payload to break the Security and Privacy payload.
- [PI-002965] Fixed an issue that prevented computers from enrolling via user-initiated enrollment when using an SSL certificate signed by the JSS's built-in CA and the **Enable SSL certificate verification** checkbox is selected.
- [PI-003045] Fixed an issue that prevented all classes from displaying when switching from the full JSS to a site in the JSS, and then back to the full JSS.
- [PI-003080] Fixed an issue that prevented some users from logging in using Single Sign-On authentication unless a matching user or group was in the JSS User Accounts and Settings.
- [PI-003087] Fixed an issue that redirected users to the default context root path when working in a multi-context environment in the JSS and logging in with Single Sign-On credentials.
- [PI-003112] Fixed an issue where the JSS would not consider versions to match if the app version and iTunes version differed.
- [PI-003116] Fixed an issue where smart computer groups containing the Application Title and Operation System Version criteria could not be saved.
- [PI-003127] Fixed an issue that caused the JSS to display "MESSAGE_SITE_WARNING_TITLE" when changing the site of a class that was imported from Apple School Manager.
- [PI-003209] Fixed an issue that caused "Compliant" to be returned for the "Passcode Compliance with Configuration Profile" mobile device inventory information when there are no mobile device configuration profiles installed on the device.
- [PI-003211] Fixed an issue that prevented access to the Apple Education Support settings and the classes imported from Apple School Manager when the Apple School Manager Sync Time is set to the 31st of the month.
- [PI-003301] Fixed an issue where smart user groups would sometimes lose their link with Classes.
- [PI-003304] Fixed an issue that caused the JSS to use more memory than necessary when storing replication information for a cloud distribution point.
- [PI-003331] The JSS no longer times out when large packages are being uploaded.
- [PI-003394] Fixed multiple cross-site scripting (XSS) vulnerabilities in the JSS web application.
- [PI-003395] Fixed issues with LDAP group authentication.
- [PI-003435] Fixed an issue that caused the JSS to continue syncing with Apple School Manager after the Apple School Manager Sync Time is set to "Never" from a previously configured sync time.
- [PI-003514] Fixed an issue that caused the JSS to display the incorrect value for "Available Storage" and "Battery Level" in a mobile device inventory record for an iPad that is enabled as Shared iPad.

- [PI-003524] Fixed an issue that prevented classes from being displayed on all JSS web application instances in a clustered environment after importing classes from Apple School Manager to one JSS instance.
- [PI-003551] Fixed an issue that caused the **Autopopulate** checkbox to be automatically selected if a VPP token is saved to the JSS from another server.
- [PI-003558] Fixed an issue that prevented the last enrollment date from being populated for Apple TV devices when they were re-enrolled.
- [PI-003562] Fixed an issue where the clustered JSS environment failed to start if no Master Node was selected.
- [PI-003589] Fixed an issue that prevented a scope based on user information from updating when the user's Full Name or Email Address was edited in mobile device inventory records.
- [PI-003645] Fixed an issue that prevented APNs serial numbers from being displayed in the JSS.

jamf binary

Fixed an issue that prevented an API PUT command from working for the Healthcare Listener.

JSS Installer for Linux

[PI-003358] Fixed an issue that prevented an external CA certificate from being restored when upgrading the JSS to v9.97 using the JSS Installer for Linux.

Self Service Mobile for iOS

[PI-002769] Self Service Mobile for iOS now displays a default app icon while the assigned icon loads to improve performance.

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.
- When switching PreStage enrollments and re-enrolling an Apple TV, the Apple TV may be present in two smart groups if **Enrollment Method: PreStage enrollment** is selected as smart group criteria. To avoid this issue, delete the Apple TV device record prior to re-enrollment.
- 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.

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.
- [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.