Casper Suite Release Notes

Version 9.4

JAMF software

JAMF Software, LLC

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

JAMF Software
301 4th Ave S Suite 1075
Minneapolis, MN 55415-1039
(612) 605-6625

Contents

What's New in This Release

Key Features

The Casper Suite v9.4 includes the following key features:

- **Self Service Mobile**—Self Service Mobile for iOS allows you to distribute configuration profiles, apps, and eBooks to mobile devices for users to install. You can use the JSS to group configuration profiles, apps, and eBooks in categories, which makes those items easier to locate in Self Service Mobile. In addition, you can send notifications to mobile devices with Self Service Mobile installed. Self Service Mobile is available for free from the App Store.
- **Self Service enhancements for OS X**—OS X configuration profiles, eBooks from the iBookstore, in-house eBooks, and Mac App Store apps can now be made available for users to install from Self Service. In addition, notifications about new items added to Self Service can be enabled to appear in Self Service and in Notification Center in OS X.
- **Personal Device Management**—Users can now enroll personally owned iOS and Android devices with the JSS via user-initiated enrollment. This allows users to securely access institutional email, contacts, calendar, Wi-Fi, and VPN connections. In addition, managed apps can be distributed to personal iOS devices. You can also enforce device encryption and passcode settings on personal devices, and send remote commands to lock a device or wipe institutional data and settings from a device.
- **Support for network integration with Cisco ISE**—The JSS can be integrated with Cisco Identity Services Engine (ISE) to allow Cisco ISE to communicate with the JSS. This integration allows Cisco ISE to refer end users to enroll with the JSS, verify compliance of computers and mobile devices to your organization's standards using advanced searches in the JSS, and to send remote commands via the JSS.
- **VPP invitations available in Self Service**—Users can now accept all of their VPP invitations in Self Service at any time. Users are prompted to accept pending VPP invitations if they attempt to install an app or eBook that is assigned to them in a VPP assignment, ensuring that each user will register with VPP before they can receive the apps and eBooks that are assigned to them.
- **User-Initiated Enrollment enhancements**—You can customize each step of the user-initiated enrollment experience for computers and mobile devices, including the language that the enrollment steps are displayed in. In addition, you can specify the sites you want to make available to LDAP user groups during enrollment.
- **Improved enrollment capabilities**—Administrators can assign users to a computer or mobile device, and add the computer or mobile device to a site during enrollment.

Implemented Feature Requests

To view a complete list of feature requests that were implemented in v9.4, go to:

https://jamfnation.jamfsoftware.com/featureRequests.html?releaseID=65

API Improvements

Earlier versions of the JSS API returned inconsistent values, making it difficult to compare values and maintain consistency. In the JSS API v9.0 and later, the following changes have been made to improve this:

- Values are always returned as integers.
- There are new keys that provide pre-converted integer values in the associated unit of measure.
- Data is automatically converted to the appropriate integer value.

  For example, if a computer or mobile device submits data that is inconsistent with the integer values, the JSS API converts the value to the appropriate value.

The following table shows the items in the API that have changed as a result:

Item	Data Name	Previous Value	New Value	Additional Keys
Mac bus speed	bus_speed	String value in GHz (e.g., “1.07 GHz”)	Integer value in MHz (e.g., “1095”)	bus_speed_mhz
Mac processor speed	processor_speed	Integer value in MHz (e.g., “2260 MHz”)	Integer value in MHz (e.g., “2314”)	processor_speed_ mhz
Mac total memory	total_ram	Integer value in MB (e.g., “2048 MB”)	Integer value in MB (e.g., “2048”)	total_ram_mb
Mac full internal drive size Individual partition size	size	String value in GB (e.g., “500.11 GB”)	Integer value in MB (e.g., “512113”)	drive_capacity_ mb partition_ capacity_mb
Mac size of cache	Mac size of cache	String value in MB (e.g., “3 MB”)	Integer value in KB (e.g., “3072”)	cache_size_kb

Installation

Compatibility

The JSS v9.4 supports the following versions of client applications in the Casper Suite:

- Casper Admin v9.4 or later
- Casper Imaging v8.6 or later
- Casper Remote v9.2 or later
- Recon v9.2 or later

You can use any version of Composer and Casper Focus.

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

Upgrading the JSS

The easiest way to upgrade is to use a JSS Installer. There are three installers, one for each platform on which the JSS can be installed—Mac, Linux, and Windows. Use the installer for the platform on which you plan to install the JSS.

Note: The time it takes to upgrade from the Casper Suite v8.x or earlier has increased due to the number of changes and improvements in the JSS. The amount of time added depends on the number of mobile devices and computers in your inventory and the number of features utilized in the Casper Suite.

Before You Upgrade

Before you upgrade, consider the following:

- **If you are using smart groups**—The JSS v9.0 and later no longer supports smart groups that contain "Version" and "Title" criteria listed in that order. It is recommended that you switch the order to "Title" then "Version" before upgrading from v8.x to v9.0 or later. This applies to the "Title" /"Version" criteria for applications, fonts, plug-ins, and mobile device apps.

  For detailed instructions, see the following Knowledge Base article:

  Switching the Order of Smart Group Criteria
- **If you are using Managed Preferences**—There are two types of Managed Preferences that are lost when you upgrade from v8.x to v9.0 or later. For detailed information, see the following Knowledge Base article:

  Managed Preferences and Upgrading to v9.0 or Later

Mac Requirements

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

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

  You can download the latest JCE from:

  http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:

  https://www.mysql.com/downloads/
- Ports 8443 and 9006 available

Linux Requirements

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

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- One of the following operating systems:
  - Ubuntu 12.04 LTS Server (64-bit)
  - Ubuntu 14.04 LTS Server (64-bit)
  - Red Hat Enterprise Linux (RHEL) 6.4 or later
- Open Java Development Kit (OpenJDK) 6 or later

  For more information, go to http://openjdk.java.net/.
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:

  https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

Windows Requirements

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

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- Windows Server 2008 R2 (64-bit) or Windows Server 2012 (64-bit)

- Java SE Development Kit (JDK) 1.6 or 1.7 for Windows x64

  You can download the latest JDK from:

  http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7

  You can download the latest JCE from:

  http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html
- MySQL Enterprise Edition 5.5 or later (recommended), or MySQL Community Server 5.5 or later, available at:

  https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

Upgrading the JSS

1. Back up the current database using the JSS Database Utility.
2. Copy the most current version of the JSS Installer for your platform to the server.
3. Double-click the installer and follow the onscreen instructions to complete the upgrade.
4. If you scheduled database backups using the JSS Database Utility v8.2, it is recommended that you reschedule the backups using the updated version of the JSS Database Utility.

For more information, see the JSS installation and configuration guide for your platform.

After You Upgrade

After you upgrade, consider the following:

- **Migrating Users**—If you have upgraded from the Casper Suite v9.2x or earlier and want to integrate with VPP and utilize the **Users** tab, you must first complete the user migration process. This creates user inventory from the existing user information in computer and mobile device inventory.

  For more information, see the following Knowledge Base article:

  Migrating Users
- **Distributing Signed Configuration Profiles from Apple**—If you have a signed configuration profile from Apple, you can upload and distribute it to mobile devices with the Casper Suite v9.21 or later.

  For instructions, see the following Knowledge Base article:

  Distributing a Signed Configuration Profile from Apple

- **Enrolling Mobile Devices Using Enrollment Profiles**—There are two things to consider if you plan to use enrollment profiles to enroll mobile devices with the Casper Suite:
  - **Enrollment profiles downloaded from the Casper Suite v8.71 or earlier**—Enrollment profiles downloaded from the Casper Suite v8.71 or earlier cannot be used to enroll mobile devices with the Casper Suite v8.72 or later. Before enrolling devices with the upgraded version of the Casper Suite, re-download any enrollment profiles downloaded from v8.71 or earlier.
  - **Enrolling mobile devices that have iOS 7**—Enrollment profiles created using the Casper Suite v9.0 or earlier cannot be used to enroll mobile devices that have iOS 7 or later. If you plan to enroll devices that have iOS 7 or later, you will need to create a new enrollment profile using the Casper Suite v9.1 or later.

  Note: Mobile devices that were originally enrolled with the Casper Suite v9.0 or earlier using an enrollment profile do not need to be re-enrolled when the devices are upgraded to iOS 7.

  For information on creating an enrollment profile, see the "Enrollment Profiles" section in the *Casper Suite Administrator's Guide*.

- **Distributing an MDM Profile for App Management**—Distributing managed apps with the Casper Suite requires mobile devices with iOS 5 or later and an MDM profile that supports app management.

  As of the Casper Suite v8.3, devices that have iOS 5 or later when they are enrolled with the JSS automatically obtain an MDM profile that supports app management. Managed iOS 4 devices that are upgraded to iOS 5 or later do not obtain this profile.

  To update the MDM profile on devices, you must distribute an updated MDM profile using the Self Service web clip. When users install the profile on an iOS 5 device, the device has app management capabilities.

  For detailed instructions, see the following Knowledge Base article:

  Distributing Updated MDM Profiles

- **Enabling Certificate-Based Authentication**—If you are upgrading from the JSS v8.2 or earlier, it is recommended that you enable certificate-based authentication. Enabling certificate-based authentication ensures the JSS verifies that device certificates on OS X computers are valid.

  For detailed instructions, see the following Knowledge Base article:

  Certificate-Based Authentication for OS X Computers

Upgrading to OS X Server v10.9

This section explains how to upgrade the JSS host server to OS X Server v10.9.

1. Back up your current database.
2. Upgrade from OS X v10.8 to v10.9.
3. Install Java 1.7 and JCE 1.7.

   For instructions, see the Installing Java and MySQL Knowledge Base article.
4. Follow the instructions for upgrading the JSS.

Removals

Enrollment URLs ending in "/iosenroll" or "/osxenroll" can no longer be used to direct users to the enrollment portal for user-initiated enrollment. To direct users to the enrollment portal, you need to provide them with the full URL for the JSS followed by "/enroll". For example:

https://jss.mycompany.com:8443/enroll

Deprecations

The following functionality has been deprecated:

- **Policy status determined by checking script output for "error" and "fail"**—Historically, one of the ways the JSS has determined the status of a policy is by checking script output for the words "error" and "fail". As of v9.0, the JSS also uses exit codes to determine the status of a policy. This method is more reliable and accurate.

  Although the JSS v9.32 still checks script output for the words "error" or "fail", this will be removed in a future version. If you have written scripts that utilize this feature, consider implementing an alternative solution using exit codes as soon as possible.

- **Clear-text and masked password fields in the JSS Rest API**—Clear-text and masked password fields in the JSS Rest API have been deprecated and will be removed in a future version. Accordingly, new fields have been added that contain the MD5 and SHA-256 hashed versions of those fields.

  If you have any processes or applications that read clear-text or masked passwords from the JSS Rest API, consider implementing the MD5 or SHA-256 versions of those fields as soon as possible.

If you need assistance with the transition to new functionality, or if you have questions or concerns, contact your JAMF Software Account Manager.

Bug Fixes and Enhancements

Casper Admin

- [D-006956] Fixed an issue that caused Casper Admin to incorrectly delete the original copy of a script saved on the computer that uploaded the script, when the script is added to and deleted from Casper Admin before quitting the application.
- [D-007153] Fixed an issue that caused Casper Admin to incorrectly replicate all files if comparing files by checksum when replicating files between two file share distribution points.

Casper Imaging

- [D-006157] Fixed an issue that caused Casper Imaging to fail to use a non-master JDS instance as the default distribution point in a network segment.
- [D-007146] Fixed an issue that caused Casper Imaging to incorrectly create a third partition on a smart configuration that is two or more levels below a top-level configuration with two partitions.

Casper Remote

[D-007141] Fixed an issue that caused the JSS to incorrectly allow users with the "Screen Share with Remote Computers" privilege, but not the "Screen Share with Remote Computers without Asking" privilege to start a screen sharing session with a computer that is on the login screen without asking.

jamf binary

- [D-005179] Fixed an issue that caused the Activity Monitor to incorrectly show that the jamfAgent process is not responding on managed computers with OS X v10.9.
- [D-006854] Fixed an issue that caused the jamf binary to incorrectly display a deferral message and allow a user to run or defer the policy without requiring the computer to fist be unlocked when a policy configured with User Interaction is initiated on a locked computer.
- [D-006982] Fixed an issue that caused computer extension attribute scripts uploaded through the JSS API to fail to run.
- [D-007016] Fixed an issue that caused the jamf binary to incorrectly cause computers to frequently attempt to check in with a JSS that is no longer available.

JAMF Distribution Server

- [D-005464] Fixed an issue that caused the JSS to fail to display the correct hostname when a JDS on a computer with IPv6 disabled is enrolled in the JSS.
- [D-005939] Fixed an issue that caused the JDS installer for Linux (.run) to fail to run if dmidecode is not present.
- [D-006817] Fixed an issue that caused JDS instances to fail to install in environments with Ubuntu 14.04.
- [D-007117] Fixed an issue that caused the JDS inventory submission to fail on RedHat Enterprise Linux if the network configuration is using an interface other than eth0.

JAMF Software Server

- [D-005255] Fixed an issue that caused the JSS to incorrectly make changes to configuration profiles that have been uploaded to and downloaded from the JSS.
- [D-005624] Fixed an issue that caused the JSS to fail to properly encode Self Service policy description text and incorrectly execute the policy description as a script.
- [D-005838] Fixed an issue that caused Casper Imaging to fail to image computers using a JSS user account with a password that contained a percent symbol (%).
- [D-006027] Fixed an issue that caused the JSS to fail to update smart groups that contain nested smart groups when the nested smart group is renamed or deleted.
- [D-006044] Fixed an issue that caused the JSS to fail to save advance computer searches with a name that matches the name of a computer group that is included in the search criteria.
- [D-006049] Fixed an issue that caused the JSS to incorrectly exclude computers and mobile devices from smart group memberships if the smart group is based on Model criteria using the model identifier (e.g., "MacBookAir6,1") instead of the model format displayed in computer inventory information (e.g., "MacBook Air (11-inch Mid 2013)").
- [D-006114] Fixed an issue that caused the JSS to display a white page when clicking the Management tab in inventory information for a mobile device that belongs to a deleted smart mobile device group that was being used to assign students to a class that is in the scope of an eBook.
- [D-006192] Fixed an issue that caused the JSS to fail to correctly display inventory information for a computer that was enrolled with the JSS via the API.
- [D-006386] Fixed an issue that caused the JSS to fail to display the System Preferences payload in a managed preference profile after the profile is deleted and re-uploaded.
- [D-006435] Fixed an issue that caused the JSS API to fail to correctly process GET and POST commands when creating a licensed software record with only the required fields completed.
- [D-006610] Fixed an issue that caused the JSS API to fail to display the correct error message when a JSS user without create privileges for smart computer groups attempts to create a smart computer group.
- [D-006614] Fixed an issue that caused the JSS API to allow users without the **Create Smart User Groups** privilege to create smart computer groups, smart mobile device groups, and smart user groups.

- [D-006630] Fixed an issue that caused the JSS API to fail to display user information for a user assigned to a mobile device in the results of a simple user search if the mobile device was created with the location information using the JSS API.
- [D-006631] The JSS fails to associate a computer added via API POST with an existing user record.
- [D-006640] Fixed an issue that caused the jamf binary to fail to submit computer User and Location information to the JSS if the computer is enrolled by user-initiated enrollment and the **Restrict re-enrollment to authorized users only** option is selected in User-Initiated Enrollment settings.
- [D-006644] The QuickStart Guide for Managing Mobile Devices no longer displays an incorrect enrollment URL in the Enroll Mobile Devices section.
- [D-006826] Fixed an issue that caused the JSS to fail to correctly sort computers and mobile devices by date when preforming a search if there is a string value listed in a date field, and Inventory Display settings are set to show fields that include dates.
- [D-006844] Fixed an issue that caused the JSS to fail to pull information from the info.plist file for some in-house apps, requiring the information to be entered manually.
- [D-006893] Fixed an issue that caused the JSS REST API Resource Documentation page to fail to return the JSON Response Body when looking up computers and mobile devices by ID.
- [D-006902] Fixed an issue that caused the JSS to fail to save computer location information if a username has not been specified.
- [D-006936] Fixed an issue that caused the JSS to sometimes fail to update inventory information for mobile devices immediately after they enroll with the JSS.
- [D-007002] Fixed an issue that caused the JSS to incorrectly report information for all JDS instances when submitting inventory from a JDS to a JSS with a large number of JDS instances configured, causing the JSS to respond slowly or not at all.
- [D-007042] Fixed an issue that caused the JSS to fail to enroll computers if the PKI settings were configured with an external CA.
- [D-007057] After upgrading the JSS from v8.x to v9.x, the JSS incorrectly enables flush management history on re-enroll.
- [D-007067] Fixed an issue that caused the JSS to fail to allow a user to deselect the **Allow installing configuration profiles (Supervised device only)** checkbox in the Restrictions payload of an iOS configuration profile.
- [D-007072] Fixed an issue that caused the JSS to fail to display the correct model in the **Model** field when viewing the inventory information for an iMac v13,3.
- [D-007074] Fixed an issue that caused the JSS to fail to leave the **Force encrypted backups** checkbox selected in iOS configuration profiles with the Restrictions payload.
- [D-007088] Fixed an issue that caused the JSS to incorrectly reconfigure log flushing settings from "Do Not Delete" to retain logs for 0 days when the JSS is upgraded from v8.x to v9.x.
- [D-007090] Fixed an issue that caused the XML API to fail to display the **Script Contents** field when using a GET command and fail to create a script with script contents when using a POST command for a script object.
- [D-007092] Fixed an issue that caused the JSS API to fail to return correct information after performing a READ command on an advanced computer search.
- [D-007135] Fixed an issue that caused the JSS to sometimes display an error and fail to install OS X configuration profiles on multiple computers after imaging a computer that was already enrolled with the JSS.

- [D-007145] Fixed an issue that caused the JSS to fail to save the "Proxy Setup" pop-up menu in the VPN payload of OS X and iOS configuration profiles if the Proxy Setup is changed to anything other than "None".
- [D-007162] Fixed an issue that caused the JSS to incorrectly set the management account password to the value that was set for the EFI password if both the EFI password and the management Account payloads are configured in the same policy.
- [D-007167] Fixed an issue that caused the JSS to fail to display an EFI Password payload in a policy if the payload was updated using the JSS API.
- [D-007194] Fixed an issue that sometimes caused the JSS to fail to display apps and eBooks recently purchased through VPP.
- [D-007196] The XML API fails to correctly GET eBooks that were created in the JSS.
- [D-007205] Fixed an issue that caused the JSS API to fail to display user information, other than the username, in the inventory information for a computer or mobile device if the computer or mobile device was enrolled with the JSS using the JSS API.
- [D-007228] Fixed an issue that caused MDM commands to fail to send on computers and mobile devices if a configuration profile with a smart group in the scope of the profile uses user information as the criteria for inclusion in the group and a user object is updated so that a user falls into or out of the scope of the smart group.
- [D-007362] Fixed an issue that caused the JSS to fail to clone configuration profiles with the WiFi payload and more than two Certificate payloads.

JSS Installer for Linux

[D-006993] Fixed an issue that caused the JSS installer for Linux v9.31 to fail to migrate the JVM_TMP environment variable from catalina.sh to setenv.sh when upgrading the JSS. Manually adding a JVM_TMP variable to setenv.sh did not override the jamf.tomcat7 startup script.

Recon

[D-006588] Fixed an issue that incorrectly removed purchasing information from inventory on Windows computers if Recon.exe is used to submit inventory to the JSS and purchasing information was entered in Recon.exe.

Self Service

[D-006199] Fixed an issue that caused Self Service to fail to display user interaction messages when a policy is run.

Known Issues

The following are known issues in the Casper Suite v9.4:

- When users try to access the Self Service web clip on a mobile device with iOS 7.0.1 or 7.0.2, Self Service opens in Safari instead of as a web clip.
- eBooks and unmanaged apps cannot be installed from the Self Service web clip on iOS 7 devices until the Self Service web clip is updated for iOS 7. For more information, see the following Knowledge Base article:

  Updating the Self Service Web Clip for iOS 7
- Management account passwords configured using the network scanner in Recon v9.01-9.11 are not saved correctly in the JSS if they contain an "at" symbol (@). This prevents management tasks from being performed on the affected computers. For more information, see the following Knowledge Base article:

  Casper Remote Error: An Incorrect Username/Password is Entered for this Computer
- [D-003284] Disk encryption configurations fail to activate FileVault 2 on computers with Fusion Drives.
- [D-004003] OS X configuration profiles that require users to change their passwords after a specified number of days fail to prompt users to change their passwords.
- [D-004036] Newly enrolled OS X JDS instances do not immediately trust the SSL certificate if it was created from the JSS's built-in CA. This prevents the JDS instance from submitting inventory, and the JDS instance cannot be used until the SSL certificate is trusted. Trust is usually established within five minutes of enrollment.
- [D-004197] Printers mapped using an OS X configuration profile are not displayed in "Print and Scan" in System Preferences unless the **Allow printers that connect directly to user's computer** checkbox is selected in the configuration profile.
- [D-004198] OS X configuration profiles that are configured to display a heading on the login window fail to do so.
- [D-004382] Tapping the URL in an email enrollment invitation on an iOS 6 device draws a blank page. Users should copy-and-paste the URL into the Safari app instead.
- [D-005532] OS X configuration profiles with a Login Window payload that is configured to deny users and groups the ability to log in fail to do so.
- [D-005612] Casper Admin fails to compile configurations if the master distribution point is a file share distribution point hosted on Windows Server.
- [D-005736] The **Require password after sleep or screen saver begins** and **Allow user to set lock message** settings in the Security & Privacy payload of an OS X configuration profile are not applied.
- [D-005750] An iOS configuration profile with a Restrictions payload that has Media Content settings configured causes the Require Password option to be set to "Immediately" on a mobile device that was originally set to "15 minutes".
- [D-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of an OS X configuration profile is not applied at login.
- [D-005900] The JSS fails to install configuration profiles with a Web Clip payload on computers with OS X v10.9.
- [D-005921] Casper Focus sometimes fails to focus mobile devices on an app when the devices are restarted after being focused on the app.

- [D-006026] The JSS fails to restrict Game Center when the **Allow use of Game Center** checkbox is deselected in the Restrictions payload in OS X configuration profiles.
- [D-006058] User-level OS X configuration profiles with widget restrictions fail to restrict widgets.
- [D-006250] A customized Self Service web clip icon uploaded using the JSS will revert to the default Casper Suite icon on iOS 7 devices.
- [D-006266] Policies running during the DarkWake state of Power Nap fail if DarkWake is terminated before the policy finishes running.
- [D-006393] The **Start screen saver after** option in a Login Window payload of an OS X configuration profile is not applied on computers with OS X v10.8.4 or v10.8.5.
- [D-006627] When restarting a computer that has been imaged using Casper Imaging, the computer fails to enroll if attempting to connect to the JSS via an Apple Thunderbolt to Ethernet Adapter.
- [D-006636] Login and logout hooks implemented via the JSS will not run on computers with OS X v10.9.3.
- [D-006662] Installed OS X configuration profiles that include a VPN payload with the **Use Hybrid Authentication** checkbox selected append "[hybrid]" to the group name in the VPN authentication settings on the computer, which causes group authentication to fail.
- [D-006758] iOS configuration profiles with a Single App Mode payload fail to require a passcode on supervised iOS 7 devices when the devices have a passcode and are locked.
- [D-006793] Computer-level OS X configuration profiles that define options for Time Machine backups fail to do so.
- [D-007004] iOS configuration profiles with a cookies restriction fail to set the specified restriction and hide other cookies restrictions on the device. The restrictions that are hidden depend on the restriction specified in the profile.
- [D-007206] Attempting to install Self Service Mobile for iOS on an enrolled mobile device when the Self Service web clip is open causes the device to lock on the web clip. This prevents the user from accessing any other screens or content on the device.
  Workaround: Change the **Install Automatically** option to **Self Service web clip**.
- [D-007209] In clustered environments, check-in items may not be installed/applied until the second time the computer or mobile device checks in with the JSS after the item is added to the JSS.