Casper Suite Release Notes

Version 8.6

Contents

What's New in This Release

The following features are new in the Casper Suite v8.6:

- **Support for OS X Mountain Lion (v10.8).** The Casper Suite includes support for OS X v10.8.

- **FileVault 2 disk encryption management.** The JSS allows you to activate and report on FileVault 2 disk encryption for OS X v10.8 computers.

- **Compatibility with Gatekeeper.** All client applications in the Casper Suite are signed for compatibility with Gatekeeper. A signed JSS Installer for Mac (`JSS Installer.pkg`) is available from JAMF Software Support upon request.

  In addition, Composer allows you to create signed, flat PKGs that are compatible with Gatekeeper. Recon also allows you to create signed QuickAdd packages that are compatible with Gatekeeper.

- **Mac OS X user-initiated enrollment.** You can allow users to enroll Mac OS X computers by sending them an email invitation or providing them with an enrollment URL.

- **Certificate chains for signing certificates.** You can upload a certificate chain for a signing certificate when integrating the JSS with an external certificate authority (CA).

- **Set challenge password type.** The JSS allows you to use static or dynamic challenge passwords for Simple Certificate Enrollment Protocol (SCEP) when using an external CA or by using a configuration profile.

- **Automatic LDAP lookups for Mac OS X computers.** The JSS can automatically perform an LDAP lookup each time a computer's inventory is updated.

- **Upload package manifests to JAMF Nation.** Composer allows you to upload package manifests to JAMF Nation.

- **Import package manifests.** Composer allows you to import package manifests from your hard drive. In addition, the Update Package Manifest feature now imports package manifests from JAMF Nation.

The following feature is new in the Casper Suite v8.61:

- **Support for iOS 6.** The Casper Suite includes support for iOS 6.

- **New and updated payloads for iOS configuration profiles.** The JSS includes App Lock and Global HTTP Proxy payloads for iOS configuration profiles. In addition, the Restrictions payload includes the following new settings: Allow iBookstore, Allow adult content in iBookstore, Allow shared Photo Stream, Allow iMessage, Allow Passbook while locked, and Allow installation of certificates or unmanaged configuration profiles.

For a complete list of implemented feature requests, bug fixes, and enhancements, see the "Implemented Feature Requests" and "Bug Fixes and Enhancements" sections.

Installation

Compatibility

JAMF Software makes every effort to ensure backwards compatibility with earlier versions of the Casper Suite. Use the most current version of the Casper Suite to take full advantage of new features and bug fixes.

Security measures built into the JSS prevent earlier versions of Casper Remote from working with newer versions of the JSS. Casper Admin also requires a JSS running the same version.

Upgrading the JSS on Mac OS X Server

Use the JSS Installer for Mac to upgrade the JSS on Mac OS X Server.

Requirements

A Mac computer with:

- An Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- OS X Server v10.6 or later
- Java 1.6
- 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

Upgrading

To upgrade the JSS:

1. Back up your current database.

2. Copy the most current version of the JSS Installer for Mac to the server.

   > *Note:* The JSS Installer for Mac that is included in the product DMG (`JSS Installer.mpkg`) is unsigned. To obtain a signed version of the JSS Installer for Mac (`JSS Installer.pkg`), contact JAMF Software Support. The signed installer allows you to install or upgrade the JSS when Apple's Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

3. Double-click the installer to open it, and then click **Continue**.

4. When the Introduction pane appears, click **Continue**.

5. Read the information on the Read Me pane, and then click **Continue**.

6. Select a drive on which to install the software, and then click **Continue**.

7. If the Database pane appears, enter information about your MySQL database. Then, click **Continue**.

   The JSS Installer uses this information to connect to the existing database.

   > *Note:* This pane is only displayed if the `database.xml` file is in a custom location or contains invalid information.

8. Click **Install**.

9. Enter your administrator password when prompted, and then click **OK**.

10. When the upgrade is complete, follow the instructions on the Summary pane to access the JSS. Then, click **Close**.

    If you scheduled database backups with the JSS Database Utility v8.2, it is recommended that you reschedule the backups using the updated version of the JSS Database Utility. (See "Backing Up the Database" in the *Casper Suite Administrator's Guide* for detailed instructions.)

Enabling Certificate-Based Communication

If you are upgrading from the Casper Suite v8.2 or earlier, it is recommended that you enable certificate-based communication. Enabling certificate-based communication ensures that all messages from Mac OS X clients to the JSS are signed with a valid signature.

To enable certificate-based communication:

1. Log in to the JSS with a web browser.

2. Click the **Settings** tab.

3. Click the **Computer Management Framework Settings** link.

4. Click the **Security** tab.

5. Select the **Enable Certificate-Based Communication** checkbox.

Distributing an MDM Profile for App Management

App management with the Casper Suite is limited to devices that have an MDM profile that supports app management capabilities. Devices must be using iOS 5 to obtain this profile.

iOS 5 devices that are newly enrolled with the Casper Suite v8.3 or later automatically obtain an MDM profile with app management capabilities when they are enrolled. To update the MDM profile on devices that were enrolled with the Casper Suite v8.2 or earlier, you must distribute an updated MDM profile to the Self Service web clip. When a user installs the profile on an iOS 5 device, the device has app management capabilities.

> **Note:** Only devices that are enrolled by OTA invitation or enrollment URL can obtain an updated MDM profile via the Self Service web clip.

To distribute an updated MDM profile:

1. Log in to the JSS with a web browser.

2. Click the **Settings** tab.

3. Click the **Mobile Device Management Framework Settings** link.

4. Ensure that the **Install Self Service Web Clip** option is selected, and then select **Prompt user to update MDM profile**.

5. Click **Save**.

Upgrading to OS X Server v10.8

This section explains how to upgrade the server hosting the JSS to OS X Server v10.8.

To upgrade the server hosting the JSS to OS X Server v10.8:

1. Back up your current database.

2. Upgrade from OS X v10.7 to v10.8.

3. Install Java 1.6.

4. Follow the instructions for upgrading the JSS.

Future Deprecations

The following features are still available and functional in the Casper Suite v8.6, but they will be removed in a future version:

- **Collection of UNIX executables**—The current functionality can be better addressed by creating one or more extension attributes to collect UNIX executables. This will allow you to use the executables as criteria for creating smart computer groups and performing advanced computer searches.

- **Collection of application details**—Some application details will be collected by default with the new functionality. The collection of copyright information, modification date, and permissions will most likely be removed.

- **Collection of UNIX reports**—The collection of UNIX reports (snapshots of the command-line tools `top`, `uptime`, and `w`) will be replaced with an extension attribute. This will allow you to use UNIX reports as criteria for creating smart computer groups and performing advanced computer searches.

- **Custom reporting framework**—The ability to create custom reports using JSP (Java Server Pages) files will be removed. Many of the reporting functions that currently require custom reports will be built into the Casper Suite.

- **Display Names for packages**—The **Display Name** field for packages may be removed.

If any of these features affect your environment, consider implementing the proposed, alternative solutions as soon as possible. If you need assistance with the transition, or have questions or concerns, contact your JAMF Software Account Manager.

Implemented Feature Requests

This section lists the feature requests implemented in the Casper Suite v8.6.

Casper Imaging

[JAMF Nation FR-180] Casper Imaging accurately displays the progress when restoring a Winclone image.

Composer

- [FR-0912] [JAMF Nation FR-541] Composer allows you to add package manifests from JAMF Nation.
- [FR-1379] Composer allows you to import a package manifest.

Documentation

- [JAMF Nation FR-159] The *Casper Suite Administrator's Guide* explains that the name of the process in a restricted software record is case-sensitive and supports filename wildcards.
- [JAMF Nation FR-551] The upgrade procedure in the product documentation includes a step for backing up custom reports.

JAMF Software Server

- [FR-0102] The JSS performs an LDAP lookup every time inventory is updated.
- [FR-0693, FR-0989] The JSS allows you to activate FileVault 2 disk encryption and store recovery keys for OS X v10.8 computers.
- [FR-1381] The JSS allows you to not display available app updates in the Self Service web clip.
- [JAMF Nation FR-34] The **Reboot Immediately** option in a Self Service policy reboots clients as soon as possible and does not require user interaction.
- [JAMF Nation FR-368] The JSS allows you to use static or dynamic challenge passwords for Simple Certificate Enrollment Protocol (SCEP) when using an external CA or by using a configuration profile.

Self Service

[JAMF Nation FR-561] The Self Service icon displays at a higher resolution.

Bug Fixes and Enhancements

Casper Imaging

Fixed in v8.6:

- [D-002844] Fixed an issue that prevented Casper Imaging from respecting the specified start number for numerical naming when using Target Mode Imaging.
- [D-002894] Fixed an issue that caused Winclone images to boot improperly when a Mac OS X Installer is used to image a partition.
- [D-002927] Fixed an issue that prevented Casper Imaging from applying AirPort settings when IPv4 is configured manually.
- [D-002930] Fixed an issue that caused Casper Imaging to mount multiple distribution points when using Target Mode Imaging.
- [D-002945] Fixed an issue that caused Target Mode Imaging to result in a non-bootable partition.

Fixed in v8.61:

- [D-003067] Fixed an issue that caused Spotlight to be disabled on client computers after imaging with a method other than Target Mode Imaging (TMI).
- [D-003074] Fixed an issue that caused Casper Imaging to assign duplicate names when using a CSV file to name computers during Target Mode Imaging (TMI).
- [D-003076] Fixed an issue that prevented Casper Imaging from caching PKGs with the **This package must be installed to the boot volume at imaging time** option selected on OS X v10.8.
- [D-003083] Fixed an issue that caused Casper Imaging to create an unbootable Windows 7 partition on Thunderbolt computers when the partition was part of a configuration with OS X v10.7 and later.
- [D-003093] Fixed an issue that prevented scripts with a priority of "At Reboot" from running after imaging unless the configuration also contains a package with the **This package must be installed to the boot volume at imaging time** option selected.
- [D-003103] Fixed an issue in Casper Imaging that prevented computers from trusting certificates issued by the JSS's built-in CA after the computers are imaged with Autorun data.
- [D-003108] Fixed an issue that prevented Casper Imaging from naming computers when deploying an OS X v10.8 configuration.

Casper Remote

Fixed in v8.61:

[D-003085] Fixed an issue that caused Casper Remote to incorrectly report that packages with unmet OS requirements are successfully installed.

Composer

Fixed in v8.6:

[D-002856] Fixed an issue that prevented the contents of a package from being copied successfully if the package is renamed in Composer before building as a PKG or DMG.

JAMF Software Server

Fixed in v8.6:

- [D-002832] Fixed an issue that caused the confirmation dialog that appears when saving changes to a Mac OS X configuration profile to display that an inaccurate number of computers have the profile installed.

- [D-002833] Fixed an issue that prevented the JSS from binding computers using Centrify 4.4.3 or later when a zone is specified.

- [D-002840] Fixed an issue that caused Mac OS X configuration profiles to fail if they include a Network payload with PEAP and TTLS EAP types, MSCHAPv2 inner authentication, and the **Use as a Login Window configuration** option selected.

- [D-002847] Fixed an issue that prevented computers from being added to the JSS using the API.

- [D-002850] Fixed an issue that delayed the JSS API when returning computer details.

- [D-002851] Fixed an issue that caused the contents of the Applications folders on client computers to be deleted when the Self Service install location is set to `/Applications/` in the JSS.

- [D-002852] Fixed an issue that prevented network mounts in the Login Items payload for Mac OS X configuration profiles from being edited.

- [D-002874] Fixed an issue that caused `JAMFSoftwareServer.log` to fill up with statements about invalid device tokens.

- [D-002880] Fixed an issue that caused provisioning profiles to be removed from and then re-added to mobile devices when the scope of an in-house app is modified.

- [D-002888] Fixed an issue that caused Mac OS X configuration profiles with a Wi-Fi payload and a Security Type of "None" to fail.

- [D-002893] Fixed an issue that caused extension attributes created from the "Current AirPort Network" template to fail.

- [D-002912] Fixed an issue that caused advanced computer searches based on model criteria and any criteria in the "OS Configuration Information" category to return no results.

- [D-002935] Fixed an issue that caused advanced mobile device searches based on mobile device name and criteria of "like" to return all mobile devices.

- [D-002937] Fixed an issue that caused advanced mobile device and computer searches based on IP address with criteria of "like" to return all devices or computers.

- [D-002943] Fixed an issue that caused the JSS to return an error when adding a peripheral in computer details, and then clicking **Cancel**.

- [D-002951] Fixed an issue that prevented Mac OS X configuration profiles from installing on computers that were added to the scope if the configuration profile had already been installed on other computers in the scope.

- [D-002984] Fixed an issue that caused `JAMFSoftwareServer.log` to throw "Error parsing OS version" when a computer's inventory is updated.
- [D-002989] Fixed an issue that caused the JSS to allow computers that are not enrolled to be assigned to the scope of configuration profiles and remote commands.
- [D-003004] Fixed an issue that prevented the **Distribute to Newly Assigned Devices Only** option in iOS configuration profiles that are made available in Self Service from being applied.
- [D-003035] Added Adobe InDesign CS5 to the software definition for the "Adobe Creative Suite 5 - Design Premium" licensed software template.

Fixed in v8.61:
- [D-002947] The JSS displays the "Create" and "Update" columns for LDAP user group API privileges in the correct order.
- [D-003060] The JSS interface has been hardened against the following reported cross-site request forgery (CSRF) vulnerabilities:
  - VU#555668
  - CVE-2012-4051
- [D-003068] Fixed an issue that caused the JSS to incorrectly assign a status of "Available" to redeemed VPP codes that were used to install and reinstall a managed app.
- [D-003078] Fixed an issue that caused the JSS to display a JasperException error in Computer Details when there is an extension attribute populated by a script and the computer submits inventory that contains a percent symbol (%).
- [D-003117] Fixed an issue that prevented the JSS from displaying inventory details for computers with invalid certificates.
- [D-003118] The JSS displays the appropriate instructions on the pane for renewing an existing APNs certificate.
- [D-003124] Fixed an issue that caused Mac OS X configuration profiles with a SCEP payload and a "Dynamic-Microsoft CA" challenge password to use the same password multiple times.
- [D-003139] Line breaks in app descriptions are displayed properly in the Self Service web clip.
- [D-003139] Fixed an issue that removed purchasing information for computers already in the JSS if the computers are enrolled or re-enrolled.
- [D-003144] Fixed an issue that prevented the JSS from granting the appropriate API privileges to LDAP user groups with privileges to use Casper Imaging, add hardware, or create Recon QuickAdd packages.
- [D-003164] Fixed an issue that cleared location information for acquired computers if certificate-based communication is enabled after the acquisition and the computers are then enrolled.

Fixed in v8.62:
- [D-003188] Fixed an issue that caused the JSS to become unresponsive during periods of heavy load if mobile devices, apps, and VPP codes are in the JSS.

JSS Database Utility

Fixed in v8.6:
- [D-002848] Fixed an issue that prevented the JSS Database Utility from detecting when binary logging has been enabled.
- [D-002849] Fixed an issue that prevented the JSS Database Utility from disabling binary logging.

JSS Installer for Windows

Fixed in v8.6:

[D-002870] The JSS Installer for Windows (`JSS Installer.msi`) is now signed.

Recon.exe

Fixed in v8.6:

[D-002780] Fixed an issue that caused Recon.exe to add duplicate records to the JSS for Windows computers that submitted inventory using both a wired and a wireless network connection.

Self Service

Fixed in v8.6:

- [D-002883] Fixed an issue that caused the **Username** and **Password** fields for logging into Self Service to be displayed black when Safari v5.1.7 is running on the computer.
- [D-002898] Fixed an issue that caused Self Service to fail to initiate policies when users are forced to view the policy description.
- [D-002994] Fixed an issue that caused Self Service to incorrectly report policy failures.

/usr/sbin/jamf (jamf binary)

Fixed in v8.6:

- [D-000066] Fixed an issue that prevented computers from entering Sleep mode if application usage reporting is enabled or restricted software is configured.
- [D-001232] Fixed an issue that caused the jamf binary to submit inaccurate inventory information to the JSS for applications with a percent symbol (%) in the name.
- [D-002867] Fixed an issue that prevented the jamf binary from updating location information for computers that belong to a network segment.
- [D-002928] Fixed an issue that prevented the `PrimaryGroupID` from populating when user-level Managed Preferences are applied to directory user accounts.
- [D-003001] Fixed an issue that prevented the jamf binary from updating ByHost preference files and returning an error if the `jamf fixByHostFiles` command is executed with a ByHost file that has a malformed name.

Fixed in v8.61:

- [D-003062] Fixed an issue that prevented the jamf binary from restricting applications that are started in the background and do not have a user interface.
- [D-003066] Fixed an issue that caused users to be prompted for the JAMF keychain password when inventory submission takes longer than 5 minutes.

- [D-003073] Fixed an issue that caused account information to be displayed in plain text when binding a computer to Active Directory.
- [D-003080] Fixed an issue that sometimes prevented unicode characters from being handled properly during communication between the JSS and the jamf binary.
- [D-003081] Fixed an issue that caused the jamf binary to remove existing login/logout hooks when login/logout hooks are disabled in the JSS.
- [D-003105] Fixed an issue that prevented the jamf binary from granting administrator privileges to the user when executing the `jamf createAccount` command on OS X v10.6.8 to create a user named "admin".
- [D-003107] Fixed an issue that caused the jamf binary to incorrectly report that there is a proxy in place when attempting to run Software Update on an enrolled computer.
- [D-003114] Fixed an issue that caused the jamf binary to crash when collecting application information.
- [D-003116] Email notifications for restricted software violations include the path for where the software was launched from.
- [D-003132] Fixed an issue that prevented the jamf binary from restricting renamed applications.
- [D-003145] Fixed an issue that caused the jamf binary to create user accounts for which the passwords cannot be changed on OS X v10.7 and v10.8.
- [D-003146] Fixed an issue that caused the mount_afp binary in OS X to crash when called by the jamf binary.

Fixed in v8.63:

- [D-003399] Due to encoding issues in the JSS, the jamf binary was treating special characters as wildcards in restricted software processes. They are now read as literal question mark (?) characters.

Known Issues

The following are known issues in the Casper Suite v8.6:

- Casper Imaging fails when re-imaging computers that have FileVault 2 activated. Use Disk Utility to re-partition the disk before using Casper Imaging to re-image.

  For instructions on re-imaging computers that have FileVault 2 activated, see the following Knowledge Base article:

  https://jamfnation.jamfsoftware.com/article.html?id=228

- Casper Remote and policies fail to set or remove Open Firmware/EFI passwords on models "Late 2012" or later if the Apple "setregproptool" binary is not present on the volume(s) used to set firmware.

  For instructions on obtaining and placing the "setregproptool" binary, see the following Knowledge Base article:

  https://jamfnation.jamfsoftware.com/article.html?id=58