Casper Suite Release Notes

Version 9.101.0

jamf

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

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Contents

What's New in This Release

Apple Compatibility

The Casper Suite is now compatible with macOS 10.13, iOS 11, and tvOS 11.

To prepare for updates in your environment, see the following Apple Knowledge Base articles:

- Prepare your institution for iOS 11, macOS High Sierra, or macOS Server 5.4
- Prepare for changes to kernel extensions in macOS High Sierra
- Prepare for changes to Content Caching in macOS High Sierra

Imaging Considerations with macOS 10.13

Starting with macOS 10.13, Apple does not recommend or support monolithic system imaging when updating or upgrading macOS. To prepare for this change, see Apple's Knowledge Base article: Upgrade macOS on a Mac at your institution

In a future release of the Casper Suite, Casper Imaging will support re-provisioning a macOS 10.13 computer with up-to-date firmware using an imaging workflow.

Deprecation of Shared APFS-Formatted Volumes Using AFP

Starting with macOS 10.13, Apple has deprecated the ability to share Apple File System (APFS)-formatted volumes using Apple Filing Protocol (AFP). Computers formatted with APFS can still mount AFP shares but cannot share over AFP.

When preparing to upgrade your file share server to macOS 10.13, change the sharing protocol to SMB and update the protocol set for that distribution point in the JSS. If you need assistance or have questions, contact your Jamf account representative.

For additional information regarding APFS, see Apple's Knowledge Base article: Prepare for APFS in macOS High Sierra

Configuration Profiles

Computer Configuration Profile Enhancements

The following table provides an overview of the computer configuration profile enhancements in this release, organized by payload:

Setting	OS Requirements	Description
Certificate and SCEP		
Certificate Preference	macOS 10.12 or later	You can now set a certificate preference for user level configuration profiles in the Certificate or SCEP payload. Setting a certificate preference automatically selects the correct certificate in a user's keychain, preventing users from needing to manually select the correct certificate after a new certificate is installed on the user's device. Multiple preferences per payload may be specified.
Login Window		
Disable Siri setup during login	macOS 10.13 or later	
Network		
TLS Minimum and Maximum Version	macOS 10.13 or later	You can now define minimum and maximum TLS network security versions using a configuration profile. Selecting a minimum and maximum TLS version allows you to define a range of protocols for the security levels that are appropriate for your network or to meet compatibility requirements for your environment.
Ethernet	macOS	You can now select an Ethernet network option based on status, for example, first, second, first active, second active, and so on.
Fast Lane Quality of Service (QoS) Marking	macOS 10.13 or later	You can now use Cisco Fast Lane Quality of Service (QoS) Marking for macOS apps.
Restrictions		
Allow Content Caching	macOS 10.13 or later	You can now control if Content Caching is allowed. Content caching can be used to store content on one computer that sends content to other computers. This can save bandwidth since each computer does not need to download and install content separately.

Setting	OS Requirements	Description
Defer software update notifications for 90 days	macOS 10.13 or later	You can now defer software update notifications from displaying for 90 days after the date that the software updates became available. After 90 days, the software update notifications will appear. Users will still be able to manually install the software updates using the App Store during the 90-day deferment period.
Allow AirPrint	macOS 10.13 or later	The following AirPrint settings are now available: ▪ Disallow AirPrint to destinations with untrusted certificates ▪ Allow discovery of AirPrint printers using iBeacons
Security & Privacy		
FileVault tab	macOS 10.13 or later	New options have been added to the FileVault tab on the Security & Privacy payload to enable and manage the personal FileVault recovery key. In addition, you can use the new Recovery Key Encryption Method option to choose the method the JSS will use for encrypting and decrypting the personal recovery key. For more information, see the following Knowledge Base article: Configuration Profiles Reference. **Note:** On macOS 10.13 or later, you must use these options instead of the FileVault Recovery Key Redirection payload which is not supported on macOS 10.13. However, you must continue to use the FileVault Recovery Key Redirection payload to manage the personal FileVault recovery key for computers with macOS 10.12 or earlier.
System Migration		
	macOS 10.12 or later (target computer)	You can now configure the System Migration payload on computers and customize the source and target path pairs when data is transferred to a computer using Apple's Migration Assistant. You can migrate data from both Mac and Windows (Windows XP or later) computers. The target folder is created if not present. For more information about moving data from a Windows PC to a Mac computer, see the following Apple Knowledge Base article: Move your data from a Windows PC to your Mac

Mobile Device Configuration Profile Enhancements

The following table provides an overview of the mobile device configuration profile enhancements in this release, organized by payload:

Setting	OS Requirements	Description
AirPlay Security		
	tvOS 11 or later	You can now control tvOS password requirements and access methods using the new AirPlay Security payload for configuration profiles.
Home Screen Layout		
Dock Layout	Supervised devices with iOS 10.3.2 or later	You can configure the Home Screen Layout to display folders in the Dock. This helps you organize the application content on a device. If an application configured in the Home Screen Layout payload is not installed on a device, it will not display, or download and install automatically.
	Supervised devices with tvOS 11 or later	You can now configure the Home Screen Layout on supervised Apple TV devices using the JSS. The content of the Home Screen can include applications and folders. They are displayed on the screen in the same order as configured in the profile payload. If an application configured in the Home Screen Layout payload is not installed on a device, it will not display, or download and install automatically. **Note:** Any existing Home Screen Layout configuration profiles will be automatically set to iOS when upgrading to the JSS v9. 101.0. You will need to update the setting manually to the reflect the new payload configuration. For more information on how to manage Apple TV devices with tvOS 10.12 or later, see the Managing Apple TV Devices with tvOS 10.2 or Later Using the Casper Suite technical paper.
Restrictions		
Allow AirPrint	Supervised devices with iOS 11 or later	The following AirPrint settings are now available: ▪ Disallow AirPrint to destinations with untrusted certificates ▪ Allow discovery of AirPrint printers using iBeacons ▪ Allow storage of AirPrint credentials in Keychain
Allow adding VPN configurations	Supervised devices with iOS 11 or later	

Setting	OS Requirements	Description
Allow removing system apps	Supervised devices with iOS 11 or later	
Allow Classroom app to lock student devices to an app and lock device screens without prompting	Supervised devices with iOS 11 or later	This restriction applies to manually created classes in Apple's Classroom app only. Classes managed in the JSS automatically have this feature.
Automatically join Classroom classes without prompting	Supervised devices with iOS 11 or later	This restriction applies to manually created classes in Apple's Classroom app only. Classes managed in the JSS automatically have this feature.
Allow modifying device name	tvOS 11 or later	
Media Content	tvOS 11 or later	
Restrict App Usage	Supervised devices with tvOS 11 or later	You can now restrict app usage by creating an allowed or disallowed app list. When searching for apps to add to the list, the bundle ID can help differentiate between tvOS (e.g., com.apple.TVappname) and iOS (e.g., com.apple.appname) apps. Devices will ignore the bundle IDs that do not pertain to their device type.
Wi-Fi		
TLS Minimum and Maximum Version	▪ iOS 11 or later ▪ tvOS 11 or later	You can now define minimum and maximum TLS network security versions using a configuration profile. Selecting a minimum and maximum TLS version allows you to define a range of protocols for the security levels that are appropriate for your network or to meet compatibility requirements for your environment.

Remote Commands

The following remote commands have been added in this release:

Command	OS Requirements	Description
Remove User	macOS 10.13 or later enrolled via a PreStage enrollment	You can now remotely delete a local or mobile user account on computers. To access this feature in the JSS, navigate to the Local User Accounts category in inventory information for the computer. Click **Manage** in the respective row of the Local User Accounts table to view the available commands for this user. **Note:** If the JSS cannot identify the type of a user account, the Type value in the Local User Accounts table is blank.
Unlock User	macOS 10.13 or later enrolled via a PreStage enrollment	You can now remotely unlock a local user account on computers. To access this feature in the JSS, navigate to the Local User Accounts category in inventory information for the computer. Click **Manage** in the respective row of the Local User Accounts table to view the available commands for this user. **Note:** If the JSS cannot identify the type of a user account, the Type value in the Local User Accounts table is blank.
Retain cellular data plan	iOS 11 or later	You can now retain cellular data plans on mobile devices when sending the Wipe Device remote command. To access these remote commands in the JSS, view mobile device group memberships or view simple or advanced search results, and navigate to **Action** > **Send Remote Commands**. The retaining cellular data plan option can also be selected when sending the Wipe Device command as a mass action.

In addition, for supervised devices with iOS 10.3 or later, enrollment via a PreStage is not required for the **Update iOS Version on supervised devices** command to work.

Re-enrollment Settings Enhancements

You can now clear or retain the values for extension attributes for computers and mobile devices during re-enrollment with the JSS.

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

JSON Web Token (JWT) Option for In-House App Distribution

You can now secure in-house app downloads with JWT. JWT configurations can be enabled or disabled to allow you to troubleshoot your web server setup without deleting the setup.

This feature requires in-house apps configured in the JSS and a web server configured to require JSON Web Token authentication.

Note: If your web server is not set up to require tokens, apps will download as usual. If your web server is set up to require tokens and the token expires, the next push of the app installation will retrieve a new token with a new expiration time.

This feature is located in **Settings** > **Global Management** > **PKI Certificates** > **JSON Web Token** tab.

Jamf Self Service for iOS

The following enhancements have been made to Jamf Self Service for iOS:

- "Self Service Mobile" has been renamed "Jamf Self Service" in the App Store.
- Jamf Self Service is now compatible with iOS 11.

Jamf Self Service v9.101.0 will be available from the App Store when it is approved by Apple.

Healthcare Listener Enhancements

The following functionality has been added to the Healthcare Listener rules:

- You can choose to apply a rule to either tvOS or iOS.
- You can enter a custom field from the ADT message to use to map to an attribute in mobile device inventory information.
- You can now send an email notification in the event that a remote command is sent to an unsupported device.

To access these enhancements in the JSS, navigate to **Settings** > **Service Infrastructure** > **Infrastructure Managers** > Click the Healthcare Listener on the Infrastructure Manager instance.

Other Changes and Enhancements

The following additional changes and enhancements have been added in this release:

- The JSS Installer for Mac no longer requires credentials for the MySQL database connection step in the assistant.

- You can now select "Google" from the Identity Provider pop-up menu when configuring Single Sign-On in the JSS.
- Added the **Disable SAML token expiration** checkbox for users using Google or Okta as an Identity Provider for Single Sign-On.
- Renamed the "WEP Enterprise" security type to "Dynamic WEP" in the Wi-Fi payload in the JSS.
- A JSS user account with the "Casper Imaging - PreStage Imaging and Autorun Imaging" privilege is now required for PreStage imaging and Autorun imaging workflows.
  For more information on the permissions required for imaging computers, see the following Knowledge Base article:
  Imaging Computer Permission Requirements
- New skip steps have been added to PreStage enrollments: **iCloud Diagnostics** for computers, and **New Feature Highlights**, **Keyboard**, and **Watch Migration** for mobile devices. To select or deselect all skip steps, use the dynamic **All/None** button.

Memcached Future Requirement for Clustered Environments

Starting with the future release of Jamf Pro 10.0.0, Memcached will be required for clustered environments.

To prepare for this change, see the following Knowledge Base article:
Memcached Installation and Configuration for Clustered JSS Environments

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
v9.101.0	Change to FileVault personal recovery key settings for macOS 10.13 or later	On computers with macOS 10.13 or later, you must use the FileVault options in the Security & Privacy payload to enable and manage the FileVault personal recovery key. The FileVault Recovery Key Redirection payload is no longer supported on macOS 10.13 or later. However, you must continue to use the FileVault Recovery Key Redirection payload to manage the FileVault personal recovery key for computers with macOS 10.12 or earlier.
v9.101.0	Additional privileges required for PreStage imaging and Autorun imaging workflows	A JSS user account with the "Casper Imaging - PreStage Imaging and Autorun Imaging" privilege is now required for PreStage imaging and Autorun imaging workflows. For more information on the permissions required for imaging computers, see the following Knowledge Base article: Imaging Computer Permission Requirements
v9.101.0	Apple has deprecated the ability to share APFS-formated volumes using AFP starting with macOS 10.13	Starting with macOS 10.13, Apple has deprecated the ability to share Apple File System (APFS)-formatted volumes using Apple Filing Protocol (AFP). Computers formatted with APFS can still mount AFP shares, but cannotshare over AFP. When preparing to upgrade your file share server to macOS 10.13, change the sharing protocol to SMB and update the protocol set for that distribution point in the JSS. If you need assistance or have questions, contact your Jamf account representative.
v9.100.0	Change to SSL certificates issued by the JSS built-in CA	SSL certificates issued by the JSS built-in CA now include a "Subject Alternative Name" (SAN) extension to meet the updated requirements for SSL certificates from Google Chrome. As of Chrome 58, SSL certificates must include a "Subject Alternative Name" (SAN) extension.

Starting with...	Change or Consideration	Description
v9.100.0	Removed product documentation from the JSS Installers	The following PDF files have been removed from the JSS Installers: *Casper Suite Release Notes* *Casper Suite Administrator's Guide* *QuickStart Guide for Managing Computers* *QuickStart Guide for Managing Mobile Devices* *Jamf Software Server Installation and Configuration Guide for Mac* *Jamf Software Server Installation and Configuration Guide for Windows* *Jamf Software Server Installation and Configuration Guide for Linux* *Manually Installing the Jamf Software Server* Links to this documentation in web-based format are now available on the JSS Installer download page on Jamf Nation. To access this page, log in to Jamf Nation and go to: https://www.jamf.com/jamf-nation/my/products You can also access documentation in PDF and web-based format at: https://www.jamf.com/resources.
v9.100.0	Incremental upgrade required when using a policy to upgrade computers with macOS 10.9 or earlier to macOS 10.12.4 or later	When using a policy to upgrade computers with macOS 10.9 or earlier to macOS 10.12.4 or later, you must first perform an incremental upgrade to any version between macOS 10.10 and macOS 10.12.3. You cannot upgrade a computer with macOS 10.9 or earlier directly to macOS 10.12.4 or later without first performing this incremental upgrade. If you have questions or experience any issues during an upgrade, contact your Jamf account representative.
v9.99.0	Connection to Apple GSX requires TLS 1.2	The Casper Suite v9.99.0 and later use TLS 1.2 for GSX by default, regardless of Java version. For the Casper Suite v9.98 or earlier, you must upgrade to Java 1.8 to maintain GSX connection.
v9.99.0	Removed support for Home Screen Layout web clips for mobile device configuration profiles	Web clips can no longer be set for the Dock or page layouts in the Home Screen Layout payload for mobile device configuration profiles. After upgrading to v9.99.0 or later, previously set web clips will no longer display when viewing mobile device configuration profiles in the JSS.

Starting with...	Change or Consideration	Description
v9.98	Change to trust settings of Tomcat SSL certificates for user-initiated enrollment	As a result of an Apple security feature, beginning with iOS 10.3, during user-initiated enrollment of a device, the JSS built-in certificate authority (CA) signed Tomcat SSL certificate is not trusted by default, causing the MDM profile installation to fail. This is also true of any Tomcat SSL certificates that are self-signed or issued from a CA that the device does not trust by default. In previous versions of iOS, installing the CA certificate during enrollment caused the device to trust the CA but this is no longer the case. This is the result of intended behavior by Apple to avoid significant security vulnerabilities and will not be resolved. It is recommended that you obtain a publicly trusted web server certificate to avoid security vulnerabilities. For a list of trusted certificates for iOS devices, see the following Apple Knowledge Base article: Lists of available trusted root certificates in iOS
v9.98	Extended startup time when upgrading (one-time impact)	When upgrading from v9.97 or earlier to v9.98 or later, an additional database index is added during the initial server startup to improve performance of applications table queries. This one-time extended startup could take anywhere from a few additional minutes to several additional hours, depending on the size of your applications table and the hardware used in your environment. It is important that you do not stop the startup process. If you have questions or experience any issues during startup, contact your Jamf account representative.
v9.98	Change to the SSL Certificate Verification Setting	The **Enable SSL certificate verification** checkbox has been changed to the **SSL Certificate Verification** pop-up menu with the options "Always", "Always except during enrollment", and "Never". For more information on this change and instructions on how to safely configure SSL certificate verification in the JSS, see the following Knowledge Base articles: ▪ Change to the SSL Certificate Verification Setting in the Casper Suite v9.98 or Later ▪ Safely Configuring SSL Certificate Verification
v9.96	Removed support for macOS 10.5 and 10.6	The Casper Suite v9.96 removes support for macOS 10.5 and 10.6. For information on removing unsupported computers from the JSS, see the Removing the Management Framework from Multiple Computers Knowledge Base article.
v9.96	Deprecated support for macOS 10.7 and 10.8	Features implemented in the Casper Suite v9.96 or later are no longer supported on computers with macOS 10.7 and 10.8. Workflows implemented prior to v9.96 will continue to function, but they may require earlier versions of the client applications.
v9.96	Change to JDS instance installation	JDS instances are no longer installed during fresh installations of the JSS.

Starting with...	Change or Consideration	Description
v9.93	Loss of certain customizations when upgrading to Tomcat 8	When upgrading from Tomcat 7 to Tomcat 8 on Windows, any customizations to CATALINA_OPTS or JAVA_OPTS will be lost. To keep your customizations, when upgrading your JSS, click **Custom** in the Setup Type pane. Click **Next** and then click **Upgrade**. In the Summary pane, click **Open Settings** to review and set your customizations.
v9.93	Change to `server.xml`	In Tomcat 8 or later, JasperListener prevents the JSS from starting and must be removed. The JSS Installer automatically makes the necessary changes to Tomcat's `server.xml` by removing the `<Listener className="org.apache.catalina.core.JasperListener" />` line.
v9.93	Change to `database.xml`	The Database Driver in the `database.xml` is now set to `org.mariadb.jdbc.Driver` during JSS upgrades.
v9.92	Criteria name change	The advanced search and smart group criteria **Subscriber MCC** will now be listed as **Current Carrier Network**.
v9.92	Criteria name change	The advanced search and smart group criteria **Subscriber MNC** will now be listed as **Home Carrier Network**.
v9.8	New location for jamf binary	The jamf binary is automatically moved from `/usr/sbin/jamf` to its new location, `/usr/local/jamf/bin/jamf` , during an upgrade to the Casper Suite v9.8. During the upgrade, the database is scanned for packages, scripts, and extension attributes that reference the previous location of the binary. If items are found, notifications are displayed in the JSS after the upgrade is complete. These items need to be modified to reference the new location of the binary, which can be done in the JSS by clicking the notifications. Items that are not stored in the database and reference the previous location of the binary need to be modified to reference the new location.
v9.8	Change in the removal of devices from DEP	The JSS can no longer be used to remove a device from Apple's Device Enrollment Program (DEP). Go to the Apple Deployment Programs website to remove the device.

Installation

Preparing to Upgrade

To ensure the upgrade goes as smoothly as possible, review the best practices, tips, and considerations explained in the following Knowledge Base articles:

- Preparing to Upgrade the JSS—Explains the best practices for evaluating and preparing for an upgrade.
- Upgrading the JSS in a Clustered Environment—Provides step-by-step instructions for upgrading the JSS in a clustered environment.

It is also recommended that you review the Functionality Changes and Other Considerations section to determine if changes made to the Casper Suite since your last upgrade could impact your environment or require you to take action.

Upgrading the JSS

This section explains how to upgrade the JSS using the JSS Installers. If the JSS host server does not meet the JSS Installer requirements, you can install the JSS manually using the instructions in the " Manually Installing the Jamf Software Server" technical paper.

Jamf tests upgrades from v9.8 through the current version.

Installed Components

The following components are installed on the JSS host server by the JSS Installer:

- JSS web application
- JSS Database Utility
- Apache Tomcat

To find out which version of Tomcat will be installed, see the Apache Tomcat Version Installed by the JSS Installer Knowledge Base article.

Note: To take full advantage of all new features, bug fixes, and enhancements available in the Casper Suite, it is recommended that you use the latest version of the JSS and the client applications. To upgrade the client applications, simply replace the existing applications with the latest version.

JSS Installer Requirements

JSS Installer for Mac

The JSS Installer for Mac requires the following:

- Minimum operating systems:

    - macOS 10.7
    - macOS 10.8
    - macOS 10.9
- Recommended operating systems:
    - macOS 10.10
    - macOS 10.11
    - macOS 10.12
    - macOS 10.13

In addition, you need the following:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- macOS 10.7 or later
- macOS Server (recommended)
- Java SE Development Kit (JDK) 1.7 or 1.8 for Mac
  You can download the JDK from:
  http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.7 or 1.8
  You can download the JCE from:
  http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html
- MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  https://www.mysql.com/downloads/
- Ports 8443 and 9006 available

JSS Installer for Linux

The JSS Installer for Linux requires the following:

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

In addition, you need the following:

- A 64-bit capable Intel processor

- 2 GB of RAM
- 400 MB of disk space available
- One of the following operating systems:
  - Ubuntu 12.04 LTS Server (64-bit)
  - Ubuntu 14.04 LTS Server (64-bit)
  - Red Hat Enterprise Linux (RHEL) 6.4, 6.5, 6.6, or 7.0
- Open Java Development Kit (OpenJDK) 7 or 8
  For installation information, go to http://openjdk.java.net/install/.
- MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

JSS Installer for Windows

The JSS Installer for Windows requires the following:

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

In addition, you need the following:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), or Windows Server 2012 R2 (64-bit)
- Java SE Development Kit (JDK) 1.7 or 1.8 for Windows x64
  You can download the JDK from:
  http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.7 or 1.8
  You can download the JCE from:
  http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html
- MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  https://www.mysql.com/downloads/
- Ports 8443 and 8080 available

Upgrading the JSS

Use the following instructions to upgrade a JSS hosted on Mac or Linux. To upgrade a JSS hosted on Windows, see "Upgrading the JSS" in the *JSS Installation and Configuration Guide for Windows*.

1. Back up the current database using the JSS Database Utility.
2. Copy the most current version of the JSS Installer for your platform to the server.
3. Double-click the installer and follow the onscreen instructions to complete the upgrade.

Deprecations and Removals

The following functionality has been deprecated and will be removed starting with v10.0.0:

- **Java 1.7 compatibility—**Compatibility with Java 1.7 will be removed. It is recommended that you start using a later version of Java.
  If you need assistance with the transition to Java 1.8, or if you have questions or concerns, contact your Jamf account representative.
- **Localization for the JSS**—The Jamf Software Server (JSS) will no longer be available in Simplified Chinese and Spanish.
- **Localization for Self Service for macOS**—Self Service for macOS will no longer be available in Simplified Chinese.
- **Peripherals**—Support for peripherals will be removed.
- **Self Service Plug-in Bundles**—Support for Self Service Plug-in bundles will be removed.
- **Managed Preferences**—Support for managed preferences will be removed. It is recommended that you start using macOS configuration profiles to define settings and restrictions for computers and users.
- **Provisioning Profiles**—The ability to upload and deploy provisioning profiles using the JSS will be removed. 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

The following functionality has been removed:

Recon.exe—As of v9.100.0, Jamf is no longer distributing Recon.exe as part of the Casper Suite. Jamf will end support for Recon.exe at the end of 2017 and continue to offer technical support for existing Recon.exe customers until December 31, 2017. Note that this change is specific to *Recon.exe*. *Recon.app* features and functionality will stay intact.

Bug Fixes and Enhancements

Jamf Infrastructure Manager Instances

[PI-003831] Fixed an issue that caused the Jamf Infrastructure Manager instance hosting the LDAP Proxy to run out of memory.

Jamf Software Server

- You can now configure Lost Mode settings via the API using the following fields: lost_mode_message, lost_mode_phone, lost_mode_footnote, always_enforce_lost_mode, and lost_mode_with_sound. You may need to update API scripts or other custom logic created outside the Casper Suite.
- [PI-001952] Fixed an issue that prevented computers from downloading QuickAdd packages during DEP enrollment in a JSS limited to computers only.
- [PI-002103] Fixed an issue that prevented scoped devices from being assigned to a PreStage enrollment when switching between two DEP tokens existing on the same JSS.
- [PI-002402] Fixed an issue that prevented the Building and Department values in the User and Location payload from being reset to "None" when a value had been previously assigned in a PreStage enrollment.
- [PI-002506] Fixed an issue that caused the description of a Mac App Store app made available in Self Service to incorrectly display as "Null" if the **Automatically update app** checkbox was selected.
- [PI-002584] Fixed an issue that prevented computers with revoked device certificates to be re-enrolled with the JSS.
- [PI-002585] Fixed an issue that caused the jamf binary to not truncate large policy logs, resulting in performance issues.
- [PI-002634] Fixed an issue that resulted in pending commands not clearing correctly if locking or wiping a computer via the API.
- [PI-002639] Fixed an issue that caused a DataTables warning to appear when certain apps were added to the App Catalog.
- [PI-002766] Fixed an issue that caused upgrades to not completely successfully if incomplete computer records were contained in the database.
- [PI-002801] Fixed an issue that caused Mac App Store apps and user level configuration profiles to attempt to install for users who were not MDM capable. This issue was fixed in v9.100.0.
- [PI-002893] Fixed an issue that caused the Policy History to not automatically flush upon re-imaging the device.
- [PI-002924] Fixed an issue that caused a user assignment to remain in user inventory information after the mobile device has been wiped and re-enrolled with the JSS.
- [PI-003108] Fixed an issue that caused upgrades to not completely successfully if incomplete mobile records were contained in the database.

- [PI-003136] Fixed an issue that caused app installation commands to be sent repeatedly to iOS devices if a device did not meet an app's minimum requirements and the **Automatically update app** checkbox was selected.
- [PI-003222] Fixed an issue that prevented the Username value for MDM capable users from updating in the JSS when the LDAP username changed, and the user logged in to the managed computer again.
- [PI-003270] Fixed an issue that caused app installation commands to be sent repeatedly to iOS devices if an app failed to install, due to the JSS incorrectly not reporting failed installations.
- [PI-003336] The JSS now displays an error if the button name for an item made available in Self Service for macOS exceeds 31 characters.
- [PI-003469] Fixed an issue that caused an incorrect error response when attempting to disassociate a VPP license.
- [PI-003706] Fixed an issue that caused devices to become unmanaged if Active Directory names were longer than 31 characters.
- [PI-003792] Fixed an issue that caused some macOS 10.12.4 upgrades to fail.
- [PI-003793] Fixed an issue that resulted in MDM commands not being sent properly if some required computer information was not available.
- [PI-003840] Fixed an issue that prevented the JSS from successfully completing the iOS Update Action when the "Download and install the update, and restart devices after installation" option was selected.
- [PI-003866] Fixed an issue that caused download failures on HTTPS file share distribution points if the password contained an asterisk.
- [PI-003868] Fixed an issue that caused expiring certificates issued via a configuration profile with the SCEP payload to be continuously reissued to computers and mobile devices.
- [PI-003960] Fixed an issue that caused many pending commands to be sent to multiple mobile devices, resulting in performance issues.
- [PI-003968] Fixed an issue that caused some iOS and macOS devices to not enroll properly due to slowly-running queries.
- [PI-004055] Fixed an issue that caused the JSS to display incorrect table headers when importing classes from Apple School Manager. As a result, the "Class Source ID" variable in the JSS is now relabeled "Class ID", and the "Course Source ID" variable has been removed from the JSS.
- [PI-004148] Fixed an issue that prevented personally owned devices with iOS 11 from enrolling in the JSS if previously enrolled as an institutionally owned device.
- [PI-004183] Fixed an issue that prevented the custom messaging from displaying on a mobile device when the Enable Lost Mode remote command was sent via the Healthcare Listener.
- [PI-004184] Fixed an issue that prevented the JSS from displaying the correct version of the Healthcare Listener.
- [PI-004205] Fixed an issue that prevented the JSS from automatically sending Apple TV passwords to iOS devices when using AirPlay Permissions.
- [PI-004216] Fixed an issue that caused the Accepted EAP Types in the Network payload to not save when all of the checkboxes were selected.
- [PI-004219] The JSS now correctly processes the membership recalculation for smart mobile device groups when the smart group criteria are changed.

- [PI-004241] Fixed an issue that prevented enrollment of devices with iOS 10.3.3 due to an inability to click the profile instillation prompt. This issue was fixed in v9.100.0.
- [PI-004265] Fixed a vulnerability regarding LDAP. If you have questions or need more information, contact your Jamf account representative.
- [PI-004271] Fixed an issue that caused the Casper Remote icon to be missing.
- [PI-004401] Fixed an issue that prevented Update Inventory commands from being automatically generated for iPhones.

Self Service for macOS

[PI-002085] Fixed an issue that caused Mac App Store apps and eBooks to automatically display in Self Service regardless of the distribution method selected.

Known Issues

Third-party Software

The following issues are the result of bugs that have been found in third-party software. Jamf has filed defects for these bugs and is awaiting their resolution.

- The "Allow all" or "Prevent all" cellular data usage and data roaming usage settings cannot be edited after they have been set on a mobile device with iOS 9.
- [D-004382] Tapping the URL in an email enrollment invitation on an iOS 6 device draws a blank page. Users should copy-and-paste the URL into the Safari app instead.
- [D-005532] macOS configuration profiles with a Login Window payload that is configured to deny users and groups the ability to log in fail to do so.
- [D-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of a macOS configuration profile is not applied at login.
- [D-005900] The JSS fails to install configuration profiles with a Web Clip payload on computers with macOS v10.9.
- [D-006026] The JSS fails to restrict Game Center when the **Allow use of Game Center** checkbox is deselected in the Restrictions payload in macOS configuration profiles.
- [D-006250] A customized Self Service web clip icon uploaded using the JSS will revert to the default Casper Suite icon on iOS 7 devices.
- [D-006393] The Start screen saver after: option in a Login Window payload of a macOS configuration profile is not applied on computers with macOS v10.8.4 or v10.8.5.
- [D-006662] Installed macOS configuration profiles that include a VPN payload with the Use Hybrid Authentication checkbox selected append "[hybrid]" to the group name in the VPN authentication settings on the computer, which causes group authentication to fail.
- [D-006758] iOS configuration profiles with a Single App Mode payload fail to require a passcode on supervised iOS 7 devices when the devices have a passcode and are locked.
- [D-006979] When enrolling a computer using a QuickAdd package, the QuickAdd installer incorrectly prompts users for local administrator credentials twice if the **Restrict re-enrollment to authorized users only** checkbox is selected.
- [D-007004] iOS configuration profiles with a cookies restriction fail to set the specified restriction and hide other cookies restrictions on the device. The restrictions that are hidden depend on the restriction specified in the profile.
- [D-007245] The configuration page fails to display correctly when enrolling a mobile device via PreStage enrollment.
- [D-007486] SMB shares sometimes fail to mount on a computer with macOS v10.9.
- [D-007511] If the option to skip the Restore page is selected for a PreStage enrollment in the JSS, the Restore page is not skipped during enrollment if the enrollment process is restarted during the Setup Assistant.

- [D-007537] Location Services are incorrectly disabled when the **Allow modifying Find My Friends settings (Supervised devices only)** checkbox is deselected in the Restrictions payload of an iOS configuration profile.
- [D-007628] iOS configuration profiles made available in Self Service cannot be removed manually from mobile devices with iOS 8 even when the profiles are configured to allow removal. Workaround: Remove the mobile device from the scope of the profile.
- [D-007638] An in-house eBook set to the "Install Automatically" distribution method will display as "Untitled" until it is opened on a mobile device.
- [D-007721] iOS configuration profiles with a Mail payload configured to log in to the app using a specified password fail to require a password after the configuration profile has been removed and redistributed to require a password on mobile devices with iOS 6.
- [D-007823] Policies configured to require users to enable FileVault 2 in a disk encryption payload fail to do so on a computer with macOS v10.10.
- [D-007825] macOS configuration profiles with a Software Update payload configured to allow installation of macOS beta releases fail to make macOS beta releases available to users.
- [D-007860] When the User value in the Exchange payload of a macOS configuration profile is an email address, a macOS Mail app user cannot authenticate and access their email on macOS v10.10 computers.
- [D-007898] If a PreStage enrollment is configured with the **Make MDM Profile Mandatory** checkbox selected and a user skips the Wi-Fi configuration step during the OS X Setup Assistant process, the computer will not be enrolled with the JSS.
- [D-007969] Compiled configurations created with Casper Admin using the {{InstallESD.dmg}} file for macOS v10.10 fail to create a “Recovery HD” partition when the configuration is used to image computers.
- [D-008018] The JSS cannot connect to an Open Directory server hosted on macOS Server v10.10 using CRAM-MD5 authentication.
- [D-008152] End users are incorrectly prompted for an Airplay password when attempting to Airplay to a device for which an AirPlay password has been specified using a macOS configuration profile.
- [D-008167] When multiple Casper Suite disk images are mounted, the JSS Installer installs the version of the Casper Suite included in the disk image that was mounted first.
- [D-008212] If a mobile device is enrolled using a PreStage enrollment and is then re-added to the server token file (.p7m), the device becomes unassigned and the JSS incorrectly displays the device as still being in the scope of the PreStage enrollment.
- [D-008286] When VMware Fusion is closed on a client computer, the computer loses its connection with the JSS.
- [D-008309] A guest user is able to log in from the FileVault 2 login window when a configuration profile was used to disallow guest users and FileVault 2 is configured for the current or next user.
- [D-008688] macOS configuration profiles that include a Network payload configured with 802.1X authentication and the **Auto Join** checkbox selected fail to automatically connect a computer to the network after the computer leaves sleep mode.
- [D-008806] The dsconfigad binary fails to bind a computer to a directory service if the service account password contains an exclamation point (!).
- [D-008920] A policy that contains an macOS v10.10.3 installer causes a computer with macOS v10. 10.2 or earlier to become unresponsive.

- [D-009110] Configuration profiles with the “Internal Disks: Allow” option disabled do not prevent the use of memory cards.
- [D-009450] A macOS configuration profile with a Password payload incorrectly enforces a number of complex characters equal to the last value used.

Jamf Software Server

The following issues are known in the JSS:

- Computers with macOS 10.13 using the Apple File System (APFS) and encrypted with FileVault, when FileVault Escrow is enabled, incorrectly report a null user in the JSS.
- Entering incorrect credentials on the JSS login page redirects to /logout.html which causes the next login attempt to fail unless the URL is changed manually.
- To install applications on Apple TV devices, tvOS 10.2 or later is required. Although earlier versions do not support app installation, the **Apps** tab displays in the JSS for all mobile device records.
- When Apple TV devices are in Single App Mode, users cannot install apps.
- When using the AirPlay Security payload in mobile device configuration profiles to set a password, if using a replacement variable, the replacement variable is recorded in device inventory instead of the updated password.
- [PI-003356] The JSS may incorrectly display placeholder text in Settings.
  Workaround: Clear your web browser cache.
- [PI-003614] Apple TV devices do not properly clear from the scope column when the device record is deleted. If scoped to a configuration profile, the profile will still list the removed devices in the number of targeted devices.
- [PI-003771] When the Account Settings payload is configured for a computer PreStage enrollment, the MDM profile is installed on the computer, but the jamf binary may not install due to a timeout.
- [PI-003940] Beginning with the Casper Suite v9.98, Android devices do not update after first enroll. The following commands are also unable to complete: Install Personal Device Profile, Wipe Institutional Device, and Lock Device.
- [PI-003952] Attachments added to Apple TV devices during enrollment do not display in the devices’ inventory information.
- [PI-004196] When Single Sign-On authentication is enabled in the JSS, sometimes administrators are not able to reliably configure which sites are visible to a user during user-initiated enrollment.
- [PI-004375] When using the AirPlay Security payload in mobile device configuration profiles to set a password, if using a replacement variable, the replacement variable is recorded in device inventory instead of the updated password.

Casper Focus

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

The following issues are known in Casper Focus:

- [D-008567] When a student device with iOS 8 is focused on a website, multiple icons with the website link are displayed.
- [D-009443] Casper Focus fails to focus a student device with iOS 7 on the attention screen if the device was being focused on an app or website.
- [PI-002319] Changing the focus from one app to another fails on student devices with iOS 9.3.2 to later. The following error message is displayed as a result: "Focus failed: the device may not be connected to a network." As a workaround, remove the focus from the student devices. Then, after a message displays indicating that the focus was removed, focus the devices on the desired app.
- [PI-002359] Focus commands fail on student devices with iOS 10 until the devices are reset.
- [PI-002858] Changing the focus from an app to a website fails on student devices with iOS 9 or 10.
- [PI-004106] Focusing student devices on an app or the attention screen fails.
- [PI-004107] Focusing student devices with iOS 11 on iBooks or Safari fails.

Casper Admin

The following issues are known in Casper Admin:

- In-place upgrades fail on computers previously formatted with macOS 10.13 on APFS-formatted drives.
- Due to changes in the way Casper Admin manages macOS 10.12.4, 10.12.5, and 10.12.6 installation files for imaging, the `InstallerEDS.dmg` is no longer automatically extracted from the `Installer.app` update file.

  Workaround: Manually extract the `InstallESD.dmg` from the `Installer.app` update file and upload it to Casper Admin. On the **General** tab, select the **Item is a DMG with an OS X Installer, or Adobe Updater/Installer for CS3 or CS4** checkbox, and click **OK**.

Casper Imaging

The following issues are known in Casper Imaging:

- Casper Imaging does not populate information saved in a PreStage imaging configuration if using the List of Names method for naming computers.
- [PI-004382] Computers with APFS-formatted drives cannot be imaged. At this time, only HFS+ formatted drives can be imaged.

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