jamf | PRO

Jamf Pro Release Notes

Version 10.0.0

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

Name Change from Casper Suite to Jamf Pro

The Casper Suite is now named Jamf Pro. Starting with version 10.0.0, you'll see this change in addition to other new product names in the interface, documentation, and email notifications.

Previous Name	New Name
Casper Suite	Jamf Pro
Casper Admin	Jamf Admin
Casper Imaging	Jamf Imaging
Casper Remote	Jamf Remote
Jamf Software Server (JSS)	Jamf Pro server
JSS API	Jamf API

For additional information and answers to frequently asked questions, see the Changes to Product Names with Jamf Pro 10.0.0 Knowledge Base article.

Redesign of the Jamf Pro Interface

The Jamf Pro interface has been completely restyled and contains the following enhancements:

- **Jamf Pro Dashboard**—The Jamf Pro dashboard has been redesigned to provide an easy to understand visual overview of the status of your environment.
- **Breadcrumbs**—Jamf Pro now includes breadcrumbs for easier navigation around the interface.
- **Expert Mode Navigation**—You can now collapse the sidebar navigation to navigate Jamf Pro in "expert mode".
- **Contextual Warning and Informal Messaging**—Jamf Pro now includes improved warning and information messaging throughout the interface to help you troubleshoot common issues.
- **Keyboard Shortcuts**—Jamf Pro now includes several new keyboard shortcuts. For more information, see the Jamf Pro Keyboard Shortcuts Knowledge Base article.
- **Jamf Pro Server Logs**—You can now view and download the Jamf Pro Server log directly from the Jamf Pro web app. You can also use the Jamf Pro Server Logs settings to enable debug mode and statement logging. For more information, see the Jamf Pro Server Logs section in the *Jamf Pro Administrator's Guide*.

Note: The redesign of Jamf Pro only includes an update to the look and feel of the interface. There have been no changes made to the majority of workflows in Jamf Pro. Any changes that impact existing workflows are outlined in this document.

Patch Management Enhancements

Jamf Pro now includes patch policies for third-party macOS software titles. Patch policies rely on an automatically generated list of computers that are eligible for the software title update. Scope eligibility is based on the requirements for the update as well as the settings on the policy's General tab. As a result, you no longer need to create a smart computer group to remotely perform software updates on managed computers.

You can also make software updates available in Self Service for users to run on their computers. After you have configured a patch reporting software title, you can create a patch policy to automate the distribution of software updates.

Note: Patch Reporting has been renamed Patch Management in the Jamf Pro interface.

For additional information, see the Patch Policies section in the *Jamf Pro Administrator's Guide* and the Jamf Knowledge Base video: Patch Reporting and Patch Policies in Jamf Pro.

New Jamf Self Service for macOS

The Jamf Self Service for macOS application has been completely redesigned to provide users with an intuitive interface and enhanced user experience.

The following features and enhancements have been added to Jamf Self Service for macOS:

- **Self Service Branding**—You can now customize how Self Service displays to users by replacing the default icon, header image, and application name with custom branded elements.
- **Self Service Notifications**—You can display notifications for items and software title updates in Self Service only or in both Self Service and Notification Center.
- **Self Service Bookmarks**—Self Service URL plug-ins have been renamed to Self Service Bookmarks. You can now specify which computers display a bookmark and which users can access them. In addition, you can now customize the display name for the bookmarks category in Self Service to meet the needs of your organization.
- **Self Service Item URLs**—After making an item (other than patch policies) available in Self Service, you can now provide an item URL to your users so they can install the item or view the item description without having to search for it in Self Service.
- **Self Service Item Display Name**—You can now customize the name for the item that displays in Self Service. For example, if you create a policy with the name "Install Office 2011 with Service Pack 3", you may want an abbreviated name to display to users in Self Service (such as "Office 2011").
- **Self Service User Login**—You can now display a **Remember Me** checkbox on the Self Service Login page. This allows users to save their Self Service login credentials in Keychain Access.
- **VPP Invitation Distribution via Self Service**—Users can now access VPP invitations in Self Service by clicking the disclosure triangle next to their username. If a user attempts to install VPP content before accepting a VPP invitation, the invitation appears now appears in a dialog window in Self Service.

Self Service 10.0.0 can run on macOS 10.10.x or later. Computers with macOS 10.9 or earlier must use Self Service 9.101.0 or earlier. For more information, see the Jamf Pro Compatibility Reference for macOS Knowledge Base article.

For additional information on these features and enhancements, see the About Jamf Self Service for macOS section in the *Jamf Pro Administrator's Guide*.

Jamf Pro SCEP Proxy

Jamf Pro can now proxy communication between a SCEP server and the computers and mobile devices in your environment so that devices do not need to access the SCEP server. With Jamf Pro enabled as SCEP Proxy, Jamf Pro communicates directly with the SCEP server to obtain certificates and install them directly on devices.

You can now enable Jamf Pro as SCEP proxy for the following:

- **Configuration profiles—**Enabling Jamf Pro as SCEP proxy for configuration profiles allows you to create profiles that contain a certificate that Jamf Pro obtains from the SCEP server and installs on devices. For example, you can distribute a configuration profile that contains a VPN certificate, and Jamf Pro obtains the certificate from the SCEP server and installs it directly on devices.
- **Device enrollment—**If your environment uses an external CA that supports SCEP, you can use Jamf Pro to obtain device management certificates from the SCEP server and install them on devices during enrollment.
  Important: Changing from Jamf Pro's built-in CA to an external CA requires you to re-enroll all devices with Jamf Pro.

Additional Documentation Available in Japanese

The Jamf Pro Administrator's Guide, Jamf Pro Release Notes, and select Knowledge Base articles are now available in Japanese.

- *Jamf Pro Administrator's Guide*
  This guide contains overviews of features and instructions for performing administrative tasks using Jamf Pro.
- *Jamf Pro Release Notes*
  The release notes include a list of new features, bug fixes, and known issues. They also explain how to upgrade Jamf Pro, and what you need to do to take advantage of new features.
- Network Ports Used by Jamf Pro
  This article describes the network ports used for connections with Jamf Pro, the Jamf Pro server, and Jamf Pro applications. In addition, this article describes network ports that are commonly used when connecting or integrating Jamf Pro with third-party products.
- Installing Java and MySQL
  This article explains how to install and configure Java and MySQL on supported Mac, Linux, and Windows operating systems.
- Components Installed on Mobile Devices
  This article lists the components that are installed on mobile devices during enrollment.
- Jamf Pro Keyboard Shortcuts
  This article contains a list of the keyboard shortcuts available in Jamf Pro.

For a complete list of deprecations, removals, bug fixes, and enhancements, see the Deprecations and Removals and the Bug Fixes and Enhancements sections.

Note: It is recommended that you clear your browser's cache after upgrading Jamf Pro to ensure that the Jamf Pro interface displays correctly.

To view a complete list of the feature requests implemented in Jamf Pro 10.0.0, go to:

https://www.jamf.com/jamf-nation/feature-requests/versions/139/jamf-pro-10-0-0

Note: New privileges associated with new features in Jamf Pro are disabled by default.

What's Changed

Changes and Considerations for This Release

Review the following information before upgrading to prepare for changes that may impact your environment.

Jamf Pro Compatibility Levels by macOS Version

Starting with Jamf Pro 10.0.0, if Self Service is configured to install automatically, computers in your environment will receive a specific version of the Self Service application depending on the computer's macOS version. Computers in your environment will also receive specific versions of some Jamf utilities based on the computer's macOS version.

For more information, see the following Knowledge Base article:
Jamf Pro Compatibility Reference for macOS

Apache Tomcat Upgraded to 8.0.47 in the Jamf Pro Installers

To mitigate a potential security risk, the Jamf Pro Installers now install Apache Tomcat 8.0.47.

Tomcat PermGen Sizes No Longer Need to be Set

With the deprecation of Java 1.7, PermGen sizes no longer need to be set in the Tomcat settings. PermGen sizes do not need to be configured with Java 1.8.

Memcached Recommended for Clustered Environments

Based on customer feedback regarding the time required for testing and implementation of Memcached, this service is recommended for Jamf Pro 10.0.0, but not yet required. Memcached will be required for clustered environments in a future version of Jamf Pro.

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

Change History

Depending on the version you are upgrading from, changes made to Jamf Pro since your last upgrade could impact your current environment setup or workflows.

The following table provides a historical list of key changes and additions to Jamf Pro, and the versions in which they were implemented.

Starting with version...	Change or Consideration	Description
9.101.0	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.
9.101.0	Additional privileges required for PreStage imaging and Autorun imaging workflows	A Jamf Pro user account with the "Jamf 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
9.101.0	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 Jamf Pro. If you need assistance or have questions, contact your Jamf account representative.
9.100.0	Change to SSL certificates issued by the Jamf Pro built-in CA	SSL certificates issued by the Jamf Pro 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 version…	Change or Consideration	Description
9.100.0	Removed product documentation from the Jamf Pro Installers	Documentation is no longer included in the Jamf Pro Installers. Links to documentation in web-based format are available on the Jamf Pro 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.
9.100.0	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.
9.99.0	Connection to Apple GSX requires TLS 1.2	Jamf Pro 9.99.0 and later use TLS 1.2 for GSX by default, regardless of Java version. For the Jamf Pro 9.98 or earlier, you must upgrade to Java 1.8 to maintain GSX connection.
9.99.0	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 version 9.99.0 or later, previously set web clips will no longer display when viewing mobile device configuration profiles in Jamf Pro.

Starting with version...	Change or Consideration	Description
9.98	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 Jamf Pro 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 article from Apple's support website: Lists of available trusted root certificates in iOS
9.98	Extended startup time when upgrading (one-time impact)	When upgrading from 9.97 or earlier to 9.98 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.
9.98	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 Jamf Pro, see the following Knowledge Base articles: ▪ Change to the SSL Certificate Verification Setting in Jamf Pro 9.98 or Later ▪ Safely Configuring SSL Certificate Verification

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

It is also recommended that you review the What's Changed section to determine if changes made to Jamf Pro since your last upgrade could impact your environment or require you to take action.

Upgrading Jamf Pro

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

Jamf tests upgrades from the most recent major or minor version release to the current version.

Installed Components

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

- Jamf Pro web app (formerly the JSS web app)
- Jamf Pro database utility (formerly the JSS database utility)
- Apache Tomcat

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

Note: To take full advantage of all new features, bug fixes, and enhancements available in Jamf Pro, it is recommended that you use the latest version of the Jamf Pro server and Jamf Pro apps. To upgrade the Jamf Pro apps, simply replace the existing apps with the latest version.

Jamf Pro Installer Requirements

Jamf Pro Installer for Mac

The Jamf Pro 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) 1.8 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 1.8
  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

Jamf Pro Installer for Linux

The Jamf Pro 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) 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

Jamf Pro Installer for Windows

The Jamf Pro 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) 1.8 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 1.8
  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 Jamf Pro

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

1. Back up the current database using the Jamf Pro database utility.
2. Copy the most current version of the Jamf Pro 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:

- **Jamf Distribution Server (JDS)—**The JDS will be discontinued at the end of 2017 due to the following issues:
  - Reliance on TLS 1.0
  - Incompabilitiy with InnoDB for MySQL
  - Incompatibility with Jamf Pro 9.100.0 and later
    Jamf does not recommend using the JDS in its current state, and the installers have been removed from Jamf Nation. For questions or assistance in migrating away from the JDS, contact your Jamf account representative.
- **Support for Android devices—**Support for Andriod devices will be discontinued in a future release due to low adoption and our desire to focus on helping organizations succeed with Apple. We recommend that customers who are managing Andriod devices move those devices to an alternative solution. Note that this deprecation is specific to Android devices. Management of personally owned iOS devices will remain intact.
- **Support for Apple's iPhone Configuration Utility (iPCU)**—The ability to install enrollment profiles on mobile devices using Apple's iPCU will be removed in a future version of Jamf Pro. It is recommended that you use Apple Configurator to install enrollment profiles.

The following functionality has been removed:

- **Java 1.7 compatibility**—Jamf Pro 10.0.0 is incompatible with Java 1.7. In addition, with the deprecation of Java 1.7, PermGen sizes no longer need to be set in the Tomcat settings.
  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 Jamf Pro**—Jamf Pro is no longer available in Simplified Chinese and Spanish.
- **Localization for Jamf Self Service for macOS**—Self Service for macOS is no longer available in Simplified Chinese.
- **Self Service Plug-in Bundles**—Support for Self Service Plug-in bundles has been removed.
- **Peripherals**—Support for peripherals has been removed.
- **Managed Preferences**—Support for managed preferences has been removed. It is recommended that you use macOS configuration profiles to define settings and restrictions for computers and users.
- **Provisioning Profiles**—The ability to upload and deploy provisioning profiles using Jamf Pro has been 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

Bug Fixes and Enhancements

Jamf Pro Server

Updated 31 October 2017 with the following additions:

- [PI-004200] Fixed multiple cross-site scripting (XSS) vulnerabilities in the Jamf Pro web app.
- [PI-004623] Collapsing the Jamf Pro sidebar menu no longer causes navigation issues.
- [PI-004762] Fixed an issue that caused raw HTML tags to incorrectly display in the Apache Tomcat Settings in Jamf Pro.

- Fixed an issue that caused Jamf Pro to incorrectly save only the final patch management software title when configuring more than one title using multiple web browser tabs simultaneously.
- Fixed an issue on the **FileVault** tab of the Security & Privacy payload that prevented error indicators from appearing when required fields were left blank.
- [D-009875] Fixed an issue that caused the cursor to be incorrectly located when creating a new supervision identity for Apple Configurator 2 enrollments.
- [PI-002286] Fixed an issue that caused user photos to display broken borders in Apple School Manager when viewing with Safari.
- [PI-002427] Fixed an issue that caused the Jamf Pro side navigation bar to occasionally disappear.
- [PI-002450] Fixed a display issue that occurred in Jamf Pro when an object was clicked while the page was still rendering.
- [PI-002472] Fixed an issue that caused the `JAMFSoftwareServer.log` to display multiple unnecessary log messages.
- [PI-002488] Fixed an issue that caused site selection to not be respected when accessing Jamf Pro on mobile devices or via Responsive Design Mode.
- [PI-002492] Fixed an issue that caused the Jamf Pro side navigation bar to display incorrectly when viewed on mobile devices.
- [PI-002516] Fixed an issue that prevented button labels in Jamf Pro from displaying correctly while the page loads.
- [PI-002582] Fixed an issue that prevented the **Redistribute Profile** option from displaying in a configuration profile with a SCEP payload.
- [PI-002612] Fixed an issue that caused Jamf Pro to display a blank page when a user who does not have the "Patch Management Software Titles" privilege attempts to view patch management software titles for a computer.
- [PI-002785] Fixed an issue that prevented a Jamf Pro administrator from creating a smart computer group for a site using the "Patch Reporting Software Title" criteria when the site is created after enabling patch management.
- [PI-002793] Fixed an issue that caused an `EventLogQueue` message to display in the `JAMFSoftwareServer.log` when an In-House e-Book was deleted.

- [PI-002794] Fixed an issue that caused Jamf Pro to incorrectly convert special characters to HTML encoded characters in inventory searches.
- [PI-002886] Fixed an issue that caused descriptions for eBooks made available in Self Service to incorrectly display raw markdown tags.
- [PI-003004] Fixed an issue that prevented tables in Jamf Pro from displaying correctly when viewed on a mobile device.
- [PI-003046] Fixed an issue that prevented users from accessing the End User License Agreement (EULA) in Jamf Pro.
- [PI-003071] Fixed an issue that prevented users from logging in to Jamf Pro on the first attempt after previously being logged out due to inactivity.
- [PI-003156] Fixed an issue that resulted in the Login Keychain not updating correctly when using the `-updateLoginKeychain` flag with the `jamf resetPassword` command.
- [PI-003330] Fixed an issue that caused student photos to be distorted in Jamf Pro when rectangular photos were used.
- [PI-003361] Fixed an issue that caused the Jamf Pro user interface to become unusable after uploading a script that contains any combination of double curly brackets ({}) and less than three sets of double quotes (").
- [PI-003365] Fixed an issue that resulted in values not displaying in Criteria view if ellipses were used in the Advanced VPP content search.
- [PI-003741] Fixed an issue that caused Jamf Pro to retain previously populated values of extension attributes having the "LDAP Attribute Mapping" input type when updating the extension attribute with a space character or leaving an empty value.
- [PI-004044] Fixed an issue that prevented user-level configuration profiles with certificates issued by Symantec PKI from deploying to computers.
- [PI-004138] Fixed an issue that caused Jamf Pro to fail to recognise a user at login or as part of a scope limitation if the user was a member of an LDAP user group and the LDAP server was manually configured.
- [PI-004252] Fixed an issue that caused in-house apps or eBooks to install on devices after first failing.
- [PI-004253] The JCDS no longer requires user interaction to repair a connectivity issue.
- [PI-004254] Fixed an issue that caused Jamf Pro to display a successful package upload for packages that fail to upload when the master distribution point is a cloud distribution point.
- [PI-004354] Fixed an issue that prevented the AvailableOSUpdates command from queuing for computers with macOS.
- [PI-004401] Fixed an issue that prevented Update Inventory commands from being automatically generated for iPhones.
- [PI-004408] Fixed that issue that caused APFS-formatted drives to fail to be imaged.
- [PI-004441] Fixed an issue that caused Jamf Pro to become unresponsive during automatic inventory updates of mobile devices with iOS. This issue was observed when the **Clustering** and **A utomatically update app** options were selected, and over 500 apps were deployed to over 1,000 mobile devices.
- [PI-004481] Fixed an issue that caused performance issues when the number of threads attempting to access LDAP connections exceeded the maximum pool size.

- [PI-004523] Fixed an issue that caused the `jamf manage` command to fail to restart the jamf daemon.

Jamf Self Service for macOS

- Autocorrect is no longer enabled on the Self Service Login page.
- [PI-000865] Self Service for macOS now displays badges for notifications on the Notification icon in the Self Service toolbar instead of on the Dock icon.
- [PI-002322] Fixed an issue that prevented macOS configuration profiles from being installed through Self Service for macOS.
- [PI-002328] Fixed an issue that caused Mac App Store Apps to incorrectly display in Self Service for macOS when "Install Automatically/Prompt Users to Install" is selected from the **Distribution Method** pop-up menu.
- [PI-002679] The Self Service for macOS application is now owned by `root:wheel`.
- [PI-003810] Fixed an issue that caused Self Service for macOS to incorrectly convert quotes to smart quotes on the Self Service Login page if the **Use smart quotes and dashes** option is enabled in the Keyboard settings.

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.

- iOS 11 does not support 32-bit apps. If you deploy a 32-bit app and a VPP license to a mobile device with iOS 11, a VPP license will be used, but the app will not install.
- 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] Jamf Pro fails to install configuration profiles with a Web Clip payload on computers with macOS v10.9.
- [D-006026] Jamf Pro 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 Jamf Pro will revert to the default Jamf Pro 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 Jamf Pro, 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 Jamf Pro.
- [D-007969] Compiled configurations created with Jamf 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] Jamf Pro 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 Jamf Pro disk images are mounted, the Jamf Pro Installer installs the version of Jamf Pro 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 Jamf Pro 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 Jamf Pro.
- [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 Pro Server

The following issues are known in the Jamf Pro server (formerly the Jamf Software Server):

- Some areas in the Jamf Pro interface do not display correctly.
- Some areas in the Jamf Pro interface incorrectly reference old product names.
- Some objects in Jamf Pro do not display correct gender rules when viewed in French.
- Pages in Jamf Pro may fail to load if the browser “Back” button is used.
- AirPlay Permissions do not display in the Jamf Pro Summary.
- A blank choice in generated for smart group criteria when viewing Apple Configurator enrollment URLs for mobile device enrollment invitations.
- 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 Jamf Pro.
- Deploying several in-house apps simultaneously to a large environment may cause significant delays in app deployment time. If you have questions or need more information, contact your Jamf account representative.
- Entering incorrect credentials on the Jamf Pro 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 Jamf Pro 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.
- Patch policies that are disabled and patch policies that are not in the scope for deployment are incorrectly displayed in the management information for a computer.
- When using multiple web browser tabs simultaneously, duplicates of a patch management software title may incorrectly be created.
- When creating a patch policy, an error is written to the `JAMFSoftwareServer.log` file.
- When using the PUT and POST operations to add a software title to a site, the Jamf API may incorrectly create duplicate titles.
- When using the GET operation with the /name endpoint, the Jamf API fails when the software title belongs to a site.
- When a user with custom privileges for only "Patch Management Software Titles" and "Patch Policies" who does not have the "Computers" privilege attempts to create a new patch policy, Jamf Pro fails to display the page.
- When included in a breadcrumb, the display name of a patch management software title supports only alphanumeric characters.

- A patch report does not display correctly when viewing it on a mobile device.
- The Limited Access settings are incorrectly displayed for non-master Jamf Pro instances when switching from "Full Access" and then saving.
- Jamf Distribution Server (JDS) instances do not display the correct uploaded packages in Jamf Pro.
- When a Jamf Pro user account is created via the jamf binary, FileVault 2 fails to be enabled for that account.
- When submitting inventory, the `com.jamfsoftware.jamf` daemon causes multiple jamf processes to fail to complete successfully.
- When updating a mobile device via the API, a large number of queries are written to the `jamfsoftwareserver.log`.
- The FileVault 2 Partition Encryption State reports as "Not Encrypted" instead of "Decrypted," causing SmartGroups based of that criteria to be populated incorrectly.
- Issuing a new recovery key for FileVault 2 via a policy fails on APFS volumes, unless the management account is already enabled for FileVault 2.
- [PI-002791] Mac App Store apps do not update automatically when the distribution method is set to “Install Automatically/Prompt Users to Install” and the Automatically update app checkbox is selected.
- [PI-003356] Jamf Pro may incorrectly display placeholder text in Settings.
  Workaround: Clear your web browser cache.
- [PI-003717] Unsupervised Apple TV devices with tvOS 10.2 cannot enroll in Jamf Pro using an enrollment profile.
- [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 Jamf Pro 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-004025] When creating a user and updating the user extension attribute with the API, the API fails to modify the user extension attribute values.
- [PI-004196] When Single Sign-On authentication is enabled in Jamf Pro, administrators are occasionally 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.
- [PI-004429] Devices with no available disk space receive an InstallApplication command with each check-in.
- [PI-004439] Upgrading from Jamf Pro 9.100 or later causes all configuration profiles that include the Home Screen Layout payload to deploy incorrectly. The Home Screen Layout payload is cleared and the content is not displayed on a device. Workaround: After the upgrade, configure the Home Screen Payload again and redeploy the configuration.

- [PI-004470] The **Show password hint when needed and available** option in the Login Window payload for computer configuration profiles functions opposite to selection. Workaround: To show the password hint, leave the checkbox unselected. To disable the password hint, select the checkbox.

Jamf Self Service for macOS

The following issues are known in Jamf Self Service for macOS:

- Upgrading to Jamf Pro 10.0.0 incorrectly causes the Self Service authentication type to switch from Single Sign-On to LDAP account or Jamf Pro user account. To resolve this issue, navigate to the **Configuration** tab in the Self Service settings, select **Single Sign-On** under Authentication Type, and then click **Save**.
- Users cannot log in to Self Service for macOS using their single sign-on credentials if Jamf Pro is not installed as the “ROOT” web application.
- Jamf Pro incorrectly displays GIFs as animated when uploaded to the Self Service Branding settings or as the icon of an item made available in Jamf Self Service for macOS. Self Service does not support animated GIFs.
- Maintenance Pages do not work in Jamf Self Service for macOS.
- A 400 error incorrectly displays in the `JAMFSoftwareServer.log` after Self Service for macOS is launched on a computer for the first time.
- The Self Service Bookmarks category cannot be set as the Library main page.

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 Jamf Pro 9.96 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.

Jamf Admin

The following issue is known in Jamf Admin (formerly Casper Admin):

Due to changes in the way Jamf Admin manages macOS installers for macOS 10.12.4 or later, the `InstallESD.dmg` file is no longer automatically extracted from the macOS `Installer.app` file.

Workaround: For macOS 10.12.4, 10.12.5, and 10.12.6, manually extract the `InstallESD.dmg` from the `Installer.app` update file and upload it to Jamf Admin. On the **General** tab, select the **Item is a DMG with a macOS Installer, or Adobe Updater/Installer for CS3 or CS4** checkbox, and click **OK**. The use of macOS installers for imaging is deprecated in macOS 10.13.

Jamf Imaging

The following issues are known in Jamf Imaging (formerly Casper Imaging):

- [PI-004430] Jamf Imaging does not populate information saved in a PreStage imaging configuration if using the List of Names method for naming computers.
- Computers with macOS 10.12 or earlier cannot be reimaged with macOS 10.13.

Recon

The following issue is known in Recon:

The ability to use the Tab key to switch between fields in Recon fails to function.