jamf | PRO

Jamf Pro Release Notes

Version 10.2.0

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

Support for External Patch Sources

Jamf Pro version 10.2.0 provides a framework for integration with external patch sources. You can expand Jamf Pro patch management functionality by using a server application in your environment or by connecting to a source hosted by the community. Software titles hosted on an external source can be used for patch reporting, patch notifications, and patch policies. You can use the Jamf Pro internal source (which currently provides more than 50 curated software titles) and pair it with external sources to customize a solution for your specific environment.

To learn about the endpoints required by Jamf Pro to host an external patch source in your environment, see the Jamf Pro External Patch Source Endpoints Knowledge Base article.

To connect Jamf Pro to an external patch source, go to **Settings > Computer Management > Patch Management**.

VPP Accounts Email Notifications Enhancements

The following features have been added to VPP Accounts email notifications:

- Jamf Pro now allows the email notifications to be sent when the VPP-managed distribution content item has been removed from the App Store or the iBooks Store. To enable VPP account email notifications in Jamf Pro, navigate to **Settings** > **Global Management** > **VPP Accounts** > **Notifications**.
- You can now customize the recipients' list of VPP Accounts email notifications. This allows the notifications to be sent to users not registered in Jamf Pro. To manually configure the recipients, navigate to the **Scope** tab of the notification.

Note: It is recommended that you verify the VPP Accounts email notifications settings after upgrading to Jamf Pro 10.2.0 if your configuration includes the "No more app licenses available" trigger.

Computer Management Capabilities

Added Reporting Capabilities for Security Attribute Fields

- You can now view the status for **Password Type** and **Minimum Passcode Length** in the Local User Account category of a computer's inventory information.

The **Security** pane has been added to the Computer Inventory Display settings and the advanced computer search **Display** tab. The following attribute fields now appear in the **Security** pane:

- Gatekeeper
- System Integrity Protection

- XProtect Definitions Version

Added Approved Kernel Extensions Payload for Computer Configuration Profiles

You can now configure a list of unique team identifiers and kernel extensions that are allowed to load without user consent on computers with macOS 10.13.2 or later. When you configure the team identifier only, all kernel extensions signed by this team are allowed to load.

For detailed information on changes to kernel extensions in macOS 10.13.2, see the following article from Apple's support website: https://support.apple.com/HT208019

Note: Computers with macOS 10.13.3 or later require User Approved MDM Enrollment to install this payload. The User Approved MDM inventory information will be available in an upcoming release of Jamf Pro.

Mobile Device Management Capabilities

Added DNS Proxy Payload for Mobile Device Configuration Profiles

You can now configure DNS Proxy settings in Jamf Pro for supervised mobile devices with iOS 11 or later.

The DNS Proxy payload enables the Cisco Security Connector app for extended visibility, control, and privacy of iOS devices. The Cisco Security Connector app can be deployed via Jamf Pro.

Apple School Manager User Criteria Enhancements

You can now edit and match Email Address and SIS Username criteria from Apple School Manager to Jamf Pro.

Note: The new Email Address criteria allows you to optionally add a different email address than the Managed Apple ID.

What's Changed

Changes and Considerations for This Release

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

Memcached Recommended for Clustered Environments

Memcached is recommended for Jamf Pro 10.2.0, 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
10.1.0	Removed integration with the Apache ActiveMQ Artemis message broker	Starting with Jamf Pro 10.1.0, the integration with the Apache ActiveMQ Artemis message broker was removed. In conjunction with this, the **Enable Message Broker Debug Mode** option on the Jamf Pro Server Logs page was removed.
10.1.0	Change to the FileVault 2 encryption status for macOS 10.9 or later	Due to a change in the `fdsetup` command, "Decrypted" is no longer a status for FileVault 2 on computers with macOS 10.9 or later. As computers submit inventory, the “Decrypted” status will automatically be updated to “Not Encrypted.” If you have smart computer groups that use the “Decrypted” criteria, you will need to change that criteria to “Not Encrypted.” Computers with macOS 10.7 and 10.8 will continue to list “Decrypted” as a status and that criteria can still be used for smart computer groups.

Starting with version...	Change or Consideration	Description
10.0.0	Implemented 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
10.0.0	Removed functionality	The following functionality has been removed: ▪ Java 1.7 compatibility ▪ Localization for Jamf Pro in Simplified Chinese and Spanish ▪ Localization for Jamf Self Service for macOS in Simplified Chinese ▪ Self Service Plug-in Bundles ▪ Peripherals ▪ Managed Preferences ▪ Provisioning Profiles
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	Apple has deprecated the ability to use installers to image computers with macOS 10.13	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.
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

Starting with version...	Change or Consideration	Description
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.
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.

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 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://dev.mysql.com/downloads/mysql/
- 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
- Recommended operating systems:
    - Ubuntu 14.04 LTS Server (64-bit)
    - Ubuntu 16.04 LTS Server (64-bit)
    - Red Hat Enterprise Linux (RHEL) 6.9
    - Red Hat Enterprise Linux (RHEL) 7.4

In addition, you need the following:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available

- 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://dev.mysql.com/downloads/mysql/
- 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
- 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://dev.mysql.com/downloads/mysql/
- 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:

- **Casper Focus—**The Casper Focus app has been deprecated and will not be updated beyond the currently available version (9.96). Casper Focus will be removed from the App Store in August 2018, at which time it will no longer be available to new customers. Jamf will continue to offer technical support for existing Casper Focus customers until August 2018.
  Jamf recommends using Apple Classroom for the best iOS classroom management experience. Information on best practices for migrating from Casper Focus to the Classroom app will be available soon. In the meantime, if you are currently using Casper Focus and need assistance or have questions, contact your Jamf account representative.
  Note: Due to the known issues 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 more information, see Known Issues.
- **Jamf Distribution Server (JDS)—**JDS functionality will be removed in the second half of 2018. The JDS was 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.

The following functionality has been removed:

- **Support for Android devices**—Support for Android devices has been removed due to a low adoption and our desire to focus on helping organizations succeed with Apple. Note that this deprecation is specific to Android devices. Management of personally owned iOS devices remains intact.
- **Support for Apple's iPhone Configuration Utility (iPCU)**—The ability to install enrollment profiles on mobile devices using Apple's iPCU has been removed. It is recommended that you use Apple Configurator to install enrollment profiles.

Bug Fixes and Enhancements

Jamf Pro Server

- Improved the overall communication between Jamf Pro and Microsoft Intune.
- Improved the collection of Azure Active Directory information by Jamf Pro for a user and a computer.
- Fixed an issue that caused Jamf Pro to report passcode settings incorrectly to Microsoft Intune if both user-level and computer-level configuration profiles with Passcode payloads were configured.
- [AS-4689] Fixed an issue that caused the General pane of a saved VPP invitation to be editable even when not in edit mode.
- [BS-4321] Fixed an issue that prevented Jamf Pro from reporting files that failed to upload to JCDS using Jamf Admin.
- [PI-000364] Fixed an issue that causes advanced mobile device searches and advanced computer searches in large environments to experience performance issues.
- [PI-000879] Fixed an issue that prevented computers and mobile devices from enrolling with Jamf Pro if the PKI settings are configured with an external CA that uses the "Dynamic-Microsoft CA" challenge type.
- [PI-002133] Fixed an issue that prevented iOS configuration profiles from saving when “Only Allow Some Apps” or “Do Not Allow Some Apps” was selected in the **Restrict App Usage** pop-up menu, and an app was added to Page Layout when configuring Home Screen Layout.
- [PI-002260] Fixed an issue that caused initial VPP import to fail when the VPP token had no licenses assigned to it.
- [PI-002576] Fixed an issue that caused all devices to be added to a PreStage enrollment if they were all selected with the checkbox under Scope, even if the specific devices were then unselected.
- [PI-002641] Fixed an issue that prevented device-based VPP apps that have been removed from the App Store from distributing to devices and caused a log error. This issue was fixed in 10.1.0.
- [PI-002948] Fixed a display issue that occurred on the Restrictions payload of a mobile device configuration profile that prevented the Restrict App Usage (supervised only) setting from being saved.
- [PI-003321] Fixed an issue that causes duplicate entries in the Jamf Pro database.
- [PI-003356] Fixed an issue that prevented labels on the Settings page from displaying properly after an upgrade.
- [PI-003731] Jamf Pro no longer allows iOS configuration profiles with a SCEP payload that used the "Dynamic-Microsoft CA" challenge type to be saved if the required fields are blank.
- [PI-003771] Fixed an issue that prevented the jamf binary from installing due to a timeout when the Account Settings payload was configured for a computer PreStage enrollment.
- [PI-003837] Policies that contain scripts with line break elements (
) no longer incorrectly display the line break element in the policy logs.

- [PI-004023] Fixed an issue that prevented Site names from being edited after associated VPP Accounts were deleted.
- [PI-004320] Fixed an issue that caused MDM looping when app inventory ran before an app had finished installing.
- [PI-004380] Jamf Pro now limits the number of characters to 40 in the **Record Number** message field that displays on the Escrowed FileVault Recovery Key screen of a computer.
- [PI-004549] Fixed an issue that caused certificate inventory for computers to be truncated when data size limits were exceeded in MySQL with strict mode enabled.
- [PI-004584] Patch policies that are disabled and patch policies that are not in the scope for deployment are no longer incorrectly displayed in the management information for a computer.
- [PI-004670] Jamf Pro no longer incorrectly allows you to select an LDAP user group as a limitation for the scope of a patch policy.
- [PI-004686] Fixed an issue that prevented the **Add** button from displaying when attempting to add targets to the scope of an object.
- [PI-004689] Fixed an issue that caused computers with macOS 10.13 or later with recovery partitions to not display in smart computer groups.
- [PI-004701] Configuration profiles with the VPN payload configured no longer require specifying a user account to authenticate the VPN connection.
- [PI-004704] Fixed an issue that incorrectly allowed a new advanced computer search with the same name as an existing advanced computer search to be saved.
- [PI-004798] Fixed an issue that prevented users without the "Delete" privilege for the Buildings object in Jamf Pro from sometimes seeing a **New** button on the Building settings page.
- [PI-004809] Fixed an issue that created incorrect commands for tvOS devices.
- [PI-004825] Fixed an issue that incorrectly caused the **Complete** tab in user-initiated enrollment settings to be mislabeled as **Device Ownership**.
- [PI-004838] Fixed an issue that incorrectly marked the **Username** and **Password** fields as required in the Network payload of a computer configuration profile.
- [PI-004915] Fixed an issue that caused Apple Push Notifications to fail for Jamf Pro 10.0.0 or later if the server could not reach http://www.apple.com/DTDs/PropertyList-1.0.dtd. This issue might have occurred in environments with an outbound firewall that restricted Jamf Pro from accessing the Internet.
- [PI-005032] Fixed an issue that caused new licenses to be assigned to devices when a VPP-managed distribution content item was manually disabled in Jamf Pro.
- [PI-005037] Fixed a display issue that occurred on Purchasing category in the mobile device inventory information settings.
- [PI-005116] Fixed an issue that incorrectly caused all icons uploaded to a Jamf Pro object (e.g., a policy) to load automatically when navigating to the object, preventing the page from loading quickly.
- [PI-005146] Fixed an issue that prevented the pagination settings from displaying in the PreStage Enrollment settings and the **Devices** tab in the Device Enrollment Program settings.
- [SUS-4843] Fixed an issue that occasionally prevented users with a slow internet connection from logging in to Jamf Pro.

Jamf Self Service for macOS

- [PI-004602] Fixed an issue that caused a 400 error to incorrectly display in the `JAMFSoftwareServer.log` after Self Service for macOS was launched on a computer for the first time.
- [PI-004653] Item descriptions now display correctly in the **History** tab in Self Service for macOS.
- [PI-004685] Fixed an issue that prevented Self Service notifications for Mac App Store apps from being disabled when the distribution method was changed to “Install Automatically”.
- [PI-004722] You can now use the Jamf API to set the Self Service display name of an object made available in Self Service for macOS.
- [PI-004819] You can now use the Jamf API to customize the secondary action button for policies made available in Self Service for macOS.
- [PRI-727] Fixed an issue that prevented the "Update All" button from displaying on the **Updates** tab after an "App must be closed" warning appeared in Self Service for macOS.
- [PRI-757] Fixed an issue that caused Self Service for macOS to crash when the Escape key was used to clear search results.

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-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):

- 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 is 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.
- 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`.
- When an in-house app update is available in Self Service for mobile devices, it is deployed automatically instead of being executed by the end user.
- 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-000113] Jamf Pro incorrectly calculates scope if an existing item's scope is edited to include all users as the target and an LDAP user group as a limitation after an initial scope was saved.
- [PI-000219] Jamf Pro incorrectly reinstalls a managed app after removing it from a mobile device when a user who is assigned to the device is added as an exclusion to the scope of the app.
- [PI-002269] Upon login, policies will intermittently failed to be executed by the Loginhook trigger.

- [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-003043] Unselecting the Enable checkbox for a policy does not immediately disable it.
- [PI-003356] Jamf Pro may incorrectly display placeholder text in Settings.
  Workaround: Clear your web browser cache.
- [PI-003385] Jamf Pro Change Management logs do not reflect changes made to user inventory information.
- [PI-003432] Jamf Pro scope calculations incorrectly include policies that are disabled.
- [PI-003459] In large environments, flushing logs for Mobile Device Inventory and Computer Inventory records may cause performance issues.
- [PI-003515] When a policy doesn’t complete successfully, future occurrences of that policy will not be available for a period of up to 60 minutes.
  Workaround: Edit and save the existing policy.
- [PI-003681] When using an LDAP user as an exclusion for the scope of a restricted software record, the macOS Sierra Installer becomes unresponsive on computers in the scope when the application is opened.
- [PI-003717] Unsupervised Apple TV devices with tvOS 10.2 cannot enroll in Jamf Pro using an enrollment profile via Apple Configurator .
- [PI-003952] Attachments added to Apple TV devices during enrollment do not display in the devices’ inventory information.
- [PI-004052] When attempting to enroll a device in Jamf Pro as a personal device before it has been unassigned from a DEP PreStage enrollment, Jamf Pro will display pending commands resulting in MDM commands failing to process.
- [PI-004146] In some environments, user and location history is updated for every check-in, instead of only occurring during an inventory update.
  Workaround: Contact your Jamf account representative and reference PI-004146.
- [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-004344] The Jamf Pro Dashboard sometimes incorrectly displays failed commands when installing configuration profiles.
- [PI-004367] The Jamf API incorrectly allows a site administrator to delete a patch management software title that uses an extension attribute in Jamf Pro versions 9.101.0 and earlier.
- [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-004444] When the Restrictions payload is configured for the tvOS configuration profiles, Jamf Pro incorrectly saves the options selected in the interface.

- [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.
- [PI-004504] Packages may intermittently fail to upload to JCDS via Jamf Admin.
- [PI-004553] When a managed in-house eBook is edited in Jamf Pro, the eBook is incorrectly removed from devices that are in the scope and then reinstalled.
- [PI-004640] Jamf Pro incorrectly displays an endless page loading indicator after clicking the **Download Jamf Pro Metadata** button from the Single Sign-On settings.
  Workaround: Refresh the page.
- [PI-004646] Jamf Pro incorrectly allows blank pop-up menu choices to be saved when configuring a computer extension attribute with “Pop-up Menu” selected as the Input Type.
- [PI-004668] A patch report does not display correctly when viewing it on a mobile device.
- [PI-004673] Jamf Pro incorrectly allows users without the Log Flushing privilege to flush policy logs.
- [PI-004775] Policies with an Enrollment Complete trigger do not run upon completion of enrollment under certain circumstances.
- [PI-004864] Mobile device groups can be deleted even if they are referenced by other groups, resulting in "Null Pointer Error."
- [PI-004868] When a VPP invitation is accepted by an end user more than once for the same Apple ID, or licenses are transferred between MDM servers without performing full migration, Jamf Pro incorrectly allows multiple VPP-managed distribution eBook license assignments to the same user. This may cause Jamf Pro performance issues.
- [PI-004878] Collecting inventory information for LDAP users associated with many mobile devices may severely impact performance during an inventory update. It is recommended that you turn off the "Collect user and location information from LDAP" setting in Inventory Collection.
- [PI-004879] VPP Store apps do not display correctly when searching recently purchased mobile device apps in Jamf Pro if the associated VPP token is tied to a site.
- [PI-004892] Enabling User Level MDM on a previously MDM-approved computer reinstalls the MDM profile via a non-User Approved MDM method resulting in an unapproved MDM state.
- [PI-004897] If there are three or more packages in a policy and the FUT, FEU, or Update Autorun Data settings are changed for that package, the settings for the second package will also be changed.
- [PI-004921] When editing a smart device group or a smart computer group with multiple conditions, the OR operator cannot be changed to the AND operator.
- [PI-004935] When creating a smart computer group with two "Patch Reporting Software Title" criteria and an OR operator, saving the smart computer groups causes an “Error saving criteria” message.
- [PI-004957] Using a mass action to delete computers may intermittently cause performance issues.
- [PI-004967] Enrolling Apple TV devices with Jamf Pro via Apple Configurator 2 fails when Jamf Pro is enabled as SCEP Proxy.
- [PI-005030] When viewing the management information for a computer, Jamf Pro fails to display Mac App Store apps for a specific user when the username is entered in the **Username** field and the **Update** button is clicked.

- [PI-005036] When creating a policy with the Install Package and Update Autorun Data selected, the package is installed, but not added to Autorun Data for the Computer.
- [PI-005039] The Jamf Pro System Settings page does not display smoothly when viewed using Safari.
- [PI-005044] In Jamf Pro environments with a large number of devices (e.g., 1,000+), including at least one date/time field in the Inventory Display settings causes performance issues.
- [PI-005048] When the Automatically update app checkbox is selected for a large quantity of apps installed on a large quantity of devices, the quantity of InstallApplication commands may cause Jamf Pro performance issues.
- [PI-005050] In Jamf Pro environments with a large number of devices (e.g., 1,000+), selecting the **Devices** tab in the Prestage Enrollments configuration pane with at least one date/time field causes performance issues.
- [PI-005089] An icon uploaded via the API will fail to be associated to the ID specified in the endpoint.
  Workaround: Use Jamf Pro to upload a new icon.
- [PI-005091] When saving a policy that includes a script payload which contains more than 255 characters, the policy will fail to save due a schema error and the script payload will be removed from the policy.
- [PI-005113] Jamf Pro fails to allow packages, scripts, printers, or directory bindings to be added or removed from the Configurations settings.
  Workaround: Use Jamf Admin to manage these items until this issue is resolved.
- [PI-005161] Failure to install a large number of VPP-managed distribution applications on mobile devices may cause Jamf Pro performance issues.
- [PI-005198] The pagination settings sometimes fail to display when attempting to add a mobile device to the scope of a configuration profile or application if there are more than 100 mobile devices in Jamf Pro.
- [PI-005216] When a Push Certificate is renewed, notes added in the History pane are deleted.
- [PI-005217] Jamf Pro incorrectly loads all deployable objects twice when navigating to the Management tab of a mobile device, preventing the page from loading quickly.
- [PI-005239] When selecting criteria for the Jamf Pro Summary, the “Smart User Groups” checkbox cannot be selected.
- [PI-005254] When re-enrolling a mobile device using a PreStage enrolment, the Username value is cleared if other fields are empty in User and Location.
- [PI-005272] If mobile devices are enrolled in Jamf Pro 10.0.0 or earlier and Jamf Pro is then upgraded to 10.1.0 or 10.1.1, MDM functionality is lost.
- [PI-005274] The MDM command for installing macOS updates may fail.
- [PI-005311] Jamf Pro fails to append an identifier to certificates distributed to computers and mobile devices via a configuration profile with a SCEP payload if the Redistribute Profile option is configured.
  Workaround: Ensure $PROFILE_IDENTIFIER is entered in the Subject field of the SCEP payload in Jamf Pro when modifying the configuration profile.
- [PI-005315] Jamf Pro sometimes fails to display the page of configured patch management software titles in a large environment.

- [PI-005352] On computers with macOS 10.13.2 or later with an APFS-formatted drive, using the `jamf bless -setOF` command on a second partition causes computer to boot to the current partition instead of the second partition.
- [PI-005357] The “Configure SMTP Server” message fails to display on the Notifications tab of the Healthcare Listener settings.
  Workaround: Configure an SMTP server before attempting to configure email notifications for Healthcare Listener.
- [PI-005361] Jamf Pro incorrectly requires the "Team ID" value when configuring the Approved Kernel Extensions payload of a macOS configuration profile.
- [PI-005372] A display issue occurs when scrolling on the Buildings setting page.
- [PI-005374] Jamf Pro incorrectly still labels Android devices as “Managed” after support for Android devices was removed.
- [PI-005376] The “Android Personal Enrollment Enabled” field is incorrectly listed in the Jamf Pro Summary.
- [SUS-4885] Pressing the Enter key incorrectly causes the SMTP Server Test page to reload.

Jamf Self Service for macOS

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

- Maintenance Pages do not work in Self Service for macOS.
- [PI-004674] Self Service for macOS incorrectly allows a policy to run after the user has logged out.
- [PI-004728] 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 Self Service for macOS. Self Service does not support animated GIFs.
- [PI-004848] Self Service for macOS occasionally crashes if the **Account** pop-up menu is clicked a second time.
- [PI-004947] Self Service for macOS currently does not support the Kerberos network authentication protocol.
- [PI-004985] A policy incorrectly displays in Self Service for macOS if the policy and computer belong to the same site but the user account does not.
- [PI-005098] Users cannot log in to Self Service for macOS using Single Sign-on if the Limited Access setting in Jamf Pro is set to anything other than “Full Access”.

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".
  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.

Composer

The following issues are known in Composer:

- [PI-005066] Composer will only build packages that are formatted with APFS.
- [PI-005352] On computers with macOS 10.13.2 or later with an APFS-formatted drive, using the jamf bless -setOF command on a second partition causes computer to boot to the current partition instead of the second partition.
- [PI-005356] In some versions of macOS 10.12.6 or earlier, sources cannot be deleted in Composer.

Jamf Admin

The following Jamf Admin (formerly Casper Admin) change in functionality is no longer considered to be a known issue. It will be removed from this section in a subsequent release.

[PI-004377] 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-005184] When running a script in Jamf Imaging, the script will intermittently fail, resulting in error code 1999.
- [PI-005200] Jamf Imaging defaults to the master distribution point set in Jamf Pro, instead of the distribution point specified in the network segment.

- [SUS-5024] After PreStage or Autorun information is populated in Jamf Imaging, clicking **Image** fails to begin the imaging process.

Product Documentation

To view additional Jamf Pro documentation for this release, log in to Jamf Nation and go to:

https://www.jamf.com/jamf-nation/my/products