

jamf | PRO

# Jamf Pro Release Notes

Version 10.4.0



© copyright 2002-2018 Jamf. All rights reserved.

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

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of Jamf.

Apache Tomcat and Tomcat are trademarks of the Apache Software Foundation.

Apple, the Apple logo, macOS, and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

The CASPER SUITE, COMPOSER®, the COMPOSER Logo®, Jamf, the Jamf Logo, JAMF SOFTWARE®, the JAMF SOFTWARE Logo®, RECON®, and the RECON Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

Intel is a registered trademark of the Intel Corporation in the U.S. and other countries.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Ubuntu is a registered trademark of Canonical Ltd.

All other product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

# Contents

## **4 What's New**

- 4 User Approved MDM Profile Notification
- 4 Mobile Device Configuration Profiles
- 5 Mobile Device Remote Commands
- 5 Webhooks Enhancements
- 5 Entrust CA Integration
- 5 Microsoft Intune Integration Enhancements
- 6 Recon Timeout
- 6 Upcoming GDPR Support
- 6 Further Considerations

## **7 What's Changed**

- 7 Changes and Considerations for This Release
- 8 Change History

## **11 Installation**

- 11 Preparing to Upgrade
- 11 Upgrading Jamf Pro

## **16 Deprecations and Removals**

## **17 Bug Fixes and Enhancements**

- 17 Jamf Pro Server
- 18 Jamf Self Service for iOS
- 18 Composer
- 18 Jamf Admin
- 18 Jamf Imaging

## **19 Known Issues**

- 19 Third-party Software
- 21 Jamf Pro Server
- 27 Jamf Self Service for macOS
- 27 Casper Focus
- 28 Composer
- 28 Jamf Admin
- 28 Jamf Imaging

## **29 Product Documentation**

- 29 Documentation Deprecations

# What's New

## User Approved MDM Profile Notification

You can now notify users in Self Service and in Notification Center that they must approve your organization's MDM profile.

Users are notified via a pop-up dialog every time they launch Self Service and via a Notification Center notification that is automatically sent once per week or after Tomcat is restarted. In order to approve your organization's MDM profile, end users must be able to access the Profiles pane in System Preferences.

**Note:** This feature is enabled by default. However, the Notification Center notification will not be sent unless Self Service Notifications are enabled and a valid proxy server token is uploaded to Jamf Pro.

To access this feature in Jamf Pro, navigate to **Settings > Computer Management - Management Framework > Self Service > Configuration**.

## Mobile Device Configuration Profiles

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

Setting	OS Requirement	Description
<b>TV Remote</b>		
	iOS 11.3 or later tvOS 11.3 or later	You can now configure the TV Remote payload for mobile devices to restrict Apple TV Remote app connections, and define available Apple TV destinations.
<b>Home Screen Layout</b>		
Dock Layout /Page Layout	Supervised devices with iOS 11.3 or later	You can now add web clips to the Home Screen Layout payload when your configuration includes the Web Clips payload. <b>Important:</b> The following settings must match the respective fields in both payloads: <ul style="list-style-type: none"><li>▪ The <b>Display Name</b> field in the Home Screen Layout payload must match the <b>Label</b> field in the Web Clips payload.</li><li>▪ The <b>Unique ID</b> field in the Home Screen Layout payload must match the <b>URL</b> field in the Web Clips payload.</li></ul> <b>Note:</b> When you deploy configuration profiles with the Home Screen Layout payload with web clips to a device with iOS 11.2 or earlier, the Dock layout items may fail to display.

## Mobile Device Remote Commands

You can now prevent users from being prompted to configure their wiped device using Proximity. To prevent the use of Proximity during set up, select the **Suppress Proximity Setup** checkbox when wiping mobile devices with iOS 11.3 or later. This command can be sent as a remote command or a mass action.

## Webhooks Enhancements

The following features have been added to the Webhook settings:

- **Basic Authentication**—You can now use the username and password option for Basic Authentication when configuring a webhook. When specified, the credentials will be included in the Authorization header sent to your webhook receiver.  
**Note:** It is recommended to use HTTPS (TLS) connections whenever a webhook may contain authentication or other sensitive information.
- **Webhook events for specific smart device groups**—You can now choose which smart device group will trigger the "SmartGroupMobileDeviceMembershipChange" webhook event. The webhook message will include all devices that have been added or removed from a smart device group.  
**Note:** When a smart device group associated with a webhook is deleted, a warning displays in Jamf Pro.

More information can be found on the Jamf Developer Portal:

<https://developer.jamf.com/webhooks#smartgroupmobiledevicemembershipchange>

## Entrust CA Integration

You can now integrate with an Entrust Certificate Authority to enroll computers and mobile devices with Jamf Pro and to issue device certificates.

## Microsoft Intune Integration Enhancements

- **Change in logging output from jamfAAD for computers registered with Azure Active Directory**  
This version of jamfAAD adopts Apple's Unified Logging that uses a Mac system-wide database to store log data (available for macOS 10.12 or later). You may see the log information for a computer by using the Console.app program on a Mac, or from Terminal using the following command:  
`log show --predicate 'subsystem CONTAINS "jamfAAD"' --last 30m`  
**Note:** The "--last 30m" option can be changed to other time frames of interest.
- The Microsoft Intune Integration connection test setting now appears inside the Microsoft Intune Integration settings page and is available without going into edit mode.

## Recon Timeout

You can now set the communication timeout in Recon. The default timeout is two minutes. To access this feature in Recon, navigate to **Preferences > Jamf Pro Server**.

## Upcoming GDPR Support

Jamf is committed to complying with the EU General Data Protection Regulation (GDPR) when it becomes enforceable on May 25, 2018. Jamf is also committed to updating our products to help our customers comply with applicable GDPR requirements. Information describing GDPR compliance workflows will be available with an upcoming supplemental release of Jamf Pro.

## Further Considerations

- Feature requests implemented in this release can be viewed at:  
<https://www.jamf.com/jamf-nation/feature-requests/versions/191/jamf-pro-10-4-0>
- Privileges associated with new features in Jamf Pro are disabled by default.
- It is recommended that you clear your browser's cache after upgrading Jamf Pro to ensure that the Jamf Pro interface displays correctly.

# 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 Distribution Server (JDS) Removal

Starting with Jamf Pro 10.4.0, Jamf Distribution Server (JDS) settings are no longer directly accessible via the Jamf Pro user interface. JDS functionality will be completely removed in a future release of Jamf Pro.

**Important:** If you are still using the JDS, you should not upgrade to Jamf Pro 10.4.0. Jamf discontinued the JDS at the end of 2017. We do not recommend using the JDS in its current state, as we cannot guarantee it will continue to function as expected. For questions or assistance in migrating away from the JDS, contact your Jamf account representative.

### Jamf Self Service for iOS

"Self Service Mobile" has been renamed to "Jamf Self Service" in the App Store.

**Note:** Jamf Self Service for iOS 10.3.0 requires devices with iOS 8 or later.

Jamf Self Service 10.3.0 will be available from the App Store when it is approved by Apple.

### Jamf Self Service for macOS

Jamf Self Service for macOS is now available in Chinese.

### Tomcat 8.5

With the release of Jamf Pro 10.4.0, Apache Tomcat 8.5 is installed by the Jamf Pro Installers for macOS, Linux, and Windows. Jamf Pro 10.4.0 can be hosted on any server with Apache Tomcat 7 or 8.x.x (8.5.x is recommended).

**Note:** If you have created custom scripts, you may need to run them as the "jamftomcat" user or verify they function correctly running as another user after upgrading Tomcat.

### Mobile Device PreStage Enrollment

- The **Move from Android** skip step for mobile device PreStage enrollments now only displays when the **Apps & Data** checkbox is selected.
- The **Keyboard** skip step has been removed from Jamf Pro, as it is not supported by Apple.

## Computer PreStage Enrollment

The **Set Up as New or Restore** skip step has been renamed to **Transfer Information**.

## Computer Configuration Profiles

The following changes have been made to the Restrictions payload:

- The **Allow use of Game Center** checkbox and its relative options are now selected by default on the Applications tab.
- The options for services available in the share menu are now selected by default on the Sharing Services tab.

## Computer Inventory Information

The following changes have been made to the General category:

- The User Approved Enrollment attribute field has been renamed to User Approved MDM.  
**Note:** This change is reflected in the Jamf API. You may need to update API scripts or other custom logic created outside Jamf Pro. In addition, the `user_approved_enrollment` field has been deprecated in the Jamf API and will be removed in a future release.
- The User Approved MDM and Enrolled via DEP attribute fields are now displayed regardless of the computer's OS version.

## Mobile Device Configuration Profiles

The **Allow keyboard continuation** checkbox has been removed from the tvOS tab in the Restrictions payload, as it is not supported by Apple.

## Mac Apps Compatibility Alert

Due to the upcoming requirement for Mac apps to support 64-bit, a compatibility alert will display on macOS 10.13.4 or later when opening Jamf Admin, Jamf Imaging, or Jamf Remote. Functionality is not currently impacted, and Jamf will address the 64-bit requirement in an upcoming release.

## Memcached Recommended for Clustered Environments

Memcached is recommended for this version of Jamf Pro, 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
10.3.0	Incremental Upgrade Required for Jamf Pro 8.73 or Earlier	When upgrading from Jamf Pro 8.73 or earlier to Jamf Pro 10.3.0 or later, you must first perform an incremental upgrade to any version between Jamf Pro 9.0 and Jamf Pro 10.2.2. You cannot upgrade from Jamf Pro 8.73 or earlier directly to Jamf Pro 10.3.0 or later without first performing this incremental upgrade.
10.3.0	Redistribute SCEP-issued Certificates via Configuration Profiles	Jamf Pro appends an identifier to certificates distributed to computers and mobile devices via a configuration profile with a SCEP payload configured to automatically redistribute the profile before the SCEP-issued certificate expires.  <b>Important:</b> To ensure the profile is redistributed before the SCEP-issued certificate expires, you must manually redistribute the profile to all devices that had the profile installed between Jamf Pro 10.0.0–10.2.x. If the appended identifier is not included in the Subject field of the SCEP payload, the profile is not redistributed before the certificate expires. Redistributing the profile to affected devices after upgrading to Jamf Pro 10.3.0 mitigates this issue.
10.2.0	Removed functionality	The following functionality has been removed: <ul style="list-style-type: none"> <li>▪ Support for Android devices</li> <li>▪ Support for Apple's iPhone Configuration Utility (iPCU)</li> </ul>
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 <b>Enable Message Broker Debug Mode</b> 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 <code>fdsetup</code> 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	<p>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.</p> <p>For more information, see the following Knowledge Base article: <a href="#">Jamf Pro Compatibility Reference for macOS</a></p>
10.0.0	Removed functionality	<p>The following functionality has been removed:</p> <ul style="list-style-type: none"> <li>▪ Java 1.7 compatibility</li> <li>▪ Localization for Jamf Pro in Simplified Chinese and Spanish</li> <li>▪ Localization for Jamf Self Service for macOS in Simplified Chinese</li> <li>▪ Self Service Plug-in Bundles</li> <li>▪ Peripherals</li> <li>▪ Managed Preferences</li> <li>▪ Provisioning Profiles</li> </ul>

# 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.

**Note:** The *Manually Installing Jamf Pro* technical paper will be discontinued in an upcoming release of Jamf Pro. Instructions for manually installing Jamf Pro will be included in the *Jamf Pro Installation and Configuration Guide for Linux* and *Jamf Pro Installation and Configuration Guide for Windows*.

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
  - macOS 10.10
  - macOS 10.11
- Recommended operating systems:
  - 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/>  
**Note:** The latest versions of MySQL may not be compatible with older macOS operating systems. For information on MySQL supported platforms and versions, see the following webpage:  
<https://www.mysql.com/support/supportedplatforms/database.html>
- 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/>  
**Note:** The latest versions of MySQL may not be compatible with older Linux operating systems. For information on MySQL supported platforms and versions, see the following webpage:  
<https://www.mysql.com/support/supportedplatforms/database.html>
- 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/>

**Note:** The latest versions of MySQL may not be compatible with older Windows operating systems.

For information on MySQL supported platforms and versions, see the following webpage:

<https://www.mysql.com/support/supportedplatforms/database.html>

- 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. For considerations when moving from Casper Focus to Apple Classroom, see the [Moving from Casper Focus to the Apple Classroom App](#) Knowledge Base article.  
**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](#).
- With the removal of support for Recon.exe in Jamf Pro 9.100.0, the following functionality has been deprecated:
  - **Extension Attributes for Windows Computers**—The ability to create extension attributes for Windows computers will be removed in a future release of Jamf Pro.
  - **Collect Application Usage Information for Windows**—The ability to collect application usage information for Windows computers will be removed in a future release of Jamf Pro.

The following functionality has been removed:

**Jamf Distribution Server (JDS)**—Starting with Jamf Pro 10.4.0, Jamf Distribution Server (JDS) settings are no longer directly accessible via the Jamf Pro user interface. JDS functionality will be completely removed in a future release of Jamf Pro.

**Important:** If you are still using the JDS, you should not upgrade to Jamf Pro 10.4.0. Jamf discontinued the JDS at the end of 2017. We do not recommend using JDS in its current state, as we cannot guarantee it will continue to function as expected. For questions or assistance in migrating away from the JDS, contact your Jamf account representative.



# Bug Fixes and Enhancements

## Correction—Updated 3 May 2018

The following known issue in Jamf Pro 10.4.0 was incorrectly documented as fixed in the original publishing of these release notes:

[PI-004878] Collecting inventory information for LDAP users associated with many mobile devices may severely impact performance during an inventory update.

Workaround: Contact your Jamf account representative and reference PI-004878.

## Jamf Pro Server

- [AS-5937] Fixed an issue that prevented LDAP users from being assigned to a mobile device during enrollment, when assigned by a local administrator in Jamf Pro.
- [AUT-3655] The Jamf API can now be used to create Jamf Pro user accounts with passwords, and to update the passwords of existing accounts.
- [PI-003937] Fixed an issue that caused communication between Jamf Pro and an iPad to fail if the iPad was enabled as Shared iPad and the Managed Apple ID used to log in to the device was not imported from Apple School Manager.
- [PI-004247] Fixed an issue that caused successful logins to be incorrectly marked as "failed" in the `JAMFSoftwareServer.log`
- [PI-004513] Fixed an issue that prevented devices from being included in the results of an advanced mobile device search if an extension attribute was selected as a display item.
- [PI-004889] When using the POST operation to create a software title, the Jamf API now uses the same XML structure as the GET operation. (POST and GET now return `<patch_management_software_title>` as the outermost wrapper.)
- [PI-005039] Fixed an issue that prevented the Jamf Pro System Settings page from displaying smoothly when viewed using Safari.
- [PI-005274] Fixed an issue that caused the MDM command for installing macOS updates to fail.
- [PI-005369] Fixed an issue that caused errors in some environments that used sites and personal device profiles, when both an institutionally owned device and a personally owned device were enrolled in the same environment.
- [PI-005431] Fixed an issue that caused Jamf Pro to incorrectly display a "No VPP Accounts" message while loading VPP accounts.
- [PI-005594] Fixed an issue that prevented computers from enrolling via a PreStage enrollment when user-initiated enrollment was not configured.
- [PI-005607] Fixed an issue that caused the "matches regex" operator to not function for smart device groups or advanced mobile device searches when a mobile device extension attribute was created.

- [PI-005678] Fixed an issue that caused mobile devices to remain in a failed MDM loop when using the Jamf Pro "Update iOS Version" remote command to push iOS 11.3 updates to devices due to changes with the MDM Software Update workflow. Any devices in a failed loop state will have their MDM communication restored after upgrading to Jamf Pro 10.3.1 or later.
- [RAT-1845] Fixed an issue that prevented Self Service for macOS from automatically launching upon enrollment completion when enrolling computers with macOS 10.13.3 or later using the user-initiated enrollment with an MDM profile method.
- [SUS-5156] Improved the handling of leading and trailing spaces in names when importing users from Apple School Manager to Jamf Pro.

## Jamf Self Service for iOS

[PI-005609] Fixed an issue that prevented Jamf Self Service for iOS from connecting to the Jamf Pro server on devices with iOS 11.3.

## Composer

- [PI-005066] Fixed an issue that caused Composer to only build APFS-formatted DMGs.
- [PI-005356] Fixed an issue that occasionally prevented Composer from deleting package sources on computers with macOS 10.12.6 or earlier.

## Jamf Admin

[PI-004249] Fixed an issue that caused some files to not be replicated correctly and some files to report a size mismatch when uploading multiple files to a JCDS that was set as set as the master distribution point with an SMB share set as the child distribution point.

## Jamf Imaging

[PI-005660] Fixed an issue that caused an error to display when imaging computers using Jamf Pro administrator passwords containing special characters.

**Note:** When interacting with the Jamf API, the encoding for credentials must be UTF-8. Failure to use this encoding may cause authentication issues with the Jamf API when the username or password contain certain international characters.

# Known Issues

## Correction—Updated 3 May 2018

The following known issue in Jamf Pro 10.4.0 was incorrectly documented as fixed in the original publishing of these release notes:

[PI-004878] Collecting inventory information for LDAP users associated with many mobile devices may severely impact performance during an inventory update.

Workaround: Contact your Jamf account representative and reference PI-004878.

## 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 book 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 dsconfigd 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.
- [PI-004614] When a local user account (including the management account) is created via the jamf binary, FileVault is not enabled for that account.
- [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-005294] New users cannot be FileVault enabled via a policy when enrolled on computers with macOS 10.13.2 or later.
- [PI-005462] FileVault 2-authenticated restart from a policy fails on computers with macOS 10.13 or later.

## 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.
- 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.
- 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 submitting inventory, the `com.jamfsoftware.jamf` daemon causes multiple jamf processes to fail to complete successfully.
- When updating a mobile device via the Jamf API, a large number of queries are written to the `JAMFSoftwareServer.log`.
- 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.
- Mobile device configuration profiles with the TV Remote payload configured fail to correctly define settings on iPhones.
- [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-002228] For personal iOS devices, apps are incorrectly distributed before user-based VPP licenses can be assigned, which causes paid apps to fail to install, and free apps to direct users to the App Store.
- [PI-002269] Upon login, policies will intermittently fail to be executed by the Loginhook trigger.
- [PI-002379] MDM commands at the macOS user level may be queued even after a user logs out of their computer.
- [PI-002745] Mobile device configuration profiles that include the Web Clips payload fail to deploy on Shared iPads.
- [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] Deselecting the **Enable** checkbox for a policy does not immediately disable it.
- [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. Additionally, the default policy timeout has been decreased to 60 seconds.
- [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-003836] User-based policies may incorrectly be applied to the system setup user instead of the user that is created through DEP.
- [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-004144] A drop in network connectivity may cause policies with an Enrollment Complete trigger to fail.
- [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-004311] Apple School Manager users not logged in to iTunes do not have their Apple IDs automatically registered for VPP, which causes looping invitations from Jamf Pro. This may cause Jamf Pro performance issues.

- [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-004406] Assigning the same MDM capable user to multiple computers or mobile devices may cause performance issues.
- [PI-004428] 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.
- [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-004473] The **Skip Account Creation** checkbox may not be respected when selected for PreStage enrollment due to a backlog of pending commands.
- [PI-004491] The **Use as a Login Window configuration** checkbox fails to remain selected for computer configuration profiles with WPA2 Enterprise as security type.
- [PI-004504] Packages may intermittently fail to upload to JCDS via Jamf Admin.
- [PI-004553] When a managed in-house book is edited in Jamf Pro, the book 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-004777] If a PreStage enrollment is configured to display Location Services and FileVault during computer enrollment, the Setup Assistant fails to do so.
- [PI-004822] Content caching is incorrectly restricted in computer configuration profiles that include a configured Security & Privacy payload but do not include a configured Restrictions payload, causing users to be incorrectly restricted from settings.  
Workaround: Include a Restrictions payload in the same configuration profile that allows content caching.

- [PI-004841] 32-bit apps scoped to mobile devices with iOS 11 or later cause looping installation attempts, which may cause Jamf Pro performance issues.
- [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 book 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.  
Workaround: Contact your Jamf account representative and reference PI-004878.
- [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-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-004970] A configuration profile scoped to a user is incorrectly removed from the computer when any smart or static user group that the user is a member of is modified.
- [PI-005007] Patch policies do not save correctly when using different web browsers to access Jamf Pro.
- [PI-005020] Pressing the Enter key incorrectly causes the SMTP Server Test page to reload.
- [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-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-005058] Enable Lost Mode management command does not display in the management history log.
- [PI-005068] When installing a user-level Symantec certificate on a computer or mobile device that is busy or unreachable, the certificate for that device is still generated in Symantec PKI Manager with a related entry in Jamf Pro.



- [PI-005089] An icon uploaded via the Jamf 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-005102] When viewing the history for a computer, Jamf Pro incorrectly prevents log tables from being resized.
- [PI-005130] Under rare circumstances when using the MyISAM database engine, Jamf Pro may write duplicate records to the database, which could result in incorrect patch reporting and patch policy data. If you have questions or need more information, contact your Jamf account representative.
- [PI-005149] When a PreStage enrollment is scoped to all devices, and then all devices are deselected and the PreStage enrollment is scoped to individual devices only, the scope will not save correctly.
- [PI-005161] Failure to install a large number of VPP-managed distribution applications on mobile devices may cause Jamf Pro performance issues.
- [PI-005185] Management accounts created with DEP may contain differences in the account settings due to variables in the environment or workflow during account creation.
- [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 enrollment, the "Username" value is cleared if other fields are empty in the User and Location settings.
- [PI-005292] Jamf Pro incorrectly requires the **Proxy Server URL** field for automatic proxy setup when configuring the Wi-Fi payload of a mobile device configuration profile.
- [PI-005315] Jamf Pro sometimes fails to display the page of configured patch management software titles in a large environment.
- [PI-005347] Cloned computer configuration profiles fail to save when they include the Security & Privacy payload configured to automatically encrypt and decrypt recovery keys.
- [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-005361] Jamf Pro incorrectly requires the "Team ID" value when configuring the Approved Kernel Extensions payload of a macOS configuration profile.
- [PI-005369] In some environments that use sites and personal device profiles, enrolling both an institutional device and a personal device in the same environment results in errors where neither device is enrolled successfully in Jamf Pro.
- [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.
- [PI-005394] VPP-managed App Store apps may be incorrectly disabled in Jamf Pro.
- [PI-005486] Mobile device configuration profiles fail to install when the VPN payload is configured with the IPsec (Cisco) connection type and the Shared Secret/Group Name authentication type.
- [PI-005492] Navigating to computer inventory information from a software title in a patch report fails in environments with multiple Jamf Pro web apps hosted on the same Apache Tomcat instance.
- [PI-005494] In a clustered environment, non-master Jamf Pro web app instances fail to inherit certificate settings if the certificate was modified and Jamf Pro is enabled as SCEP Proxy for configuration profiles.
- [PI-005519] If user and location information is collected from LDAP and location information is flushed during re-enrollment, all MDM commands will remain pending for iOS devices, resulting in errors in the logs.
- [PI-005520] When logged in with a network account, inventory collection incorrectly displays an error, even though the process completes successfully.
- [PI-005531] For Jamf Pro 10.2.0 or later hosted on Windows Server, Tomcat may fail to restart after changes to Tomcat memory settings are made using the Jamf Pro database utility.  
Workaround: Contact your Jamf account representative and reference PI-005531.
- [PI-005569] Jamf Pro applications time out when enrolling many (e.g., 1800+) computers via a Jamf Pro server setup with at least one site implemented.
- [PI-005576] When a Mac App Store app configured to update automatically is edited in Jamf Pro, the app's description is incorrectly displayed as "null" both in Jamf Pro and Self Service for macOS.
- [PI-005610] For mobile devices scoped to a class, enabling Apple Education Support in Jamf Pro causes the EDU profile to install twice, and disabling Apple Education Support attempts a second removal after the EDU profile has been removed.
- [PI-005633] Duplicate installation commands may be sent when updating a mobile device app if the **Automatically update app** checkbox is selected, and multiple copies of the app exist in Jamf Pro and are added to the scope of iOS devices.
- [PI-005650] Jamf Pro fails to clear pending commands for computers during re-enrollment when the Re-enrollment settings are configured to do so.
- [PI-005673] When computer inventory incorrectly displays an "Unknown" for FileVault status, FileVault recovery keys are hidden in Jamf Pro.
- [PI-005751] When upgrading a mobile device with iOS 11.3 to a later operating system using the ScheduleOSUpdate command, the command is continuously sent until acknowledged by the device. This may cause Jamf Pro performance or stability issues for large environments.
- [PI-005765] Jamf Pro fails to fully display the Edit Database Connection settings.  
Workaround: Resize your browser window.
- [PI-005781] When configuring the "SmartGroupMobileDeviceMembershipChange" webhook event, static groups are incorrectly included in the **Target Smart Device Group** pop-up menu. Additionally, when multiple webhooks are configured with different target smart device groups for the "SmartGroupMobileDeviceMembershipChange" webhook event, only the webhook that was registered first will receive a notification. All other webhooks for this event type will not be sent.

- [RAT-1843] The first time the jamf mdm command is run on a computer that has been enrolled with the user-initiated enrollment with an MDM profile method, the MDM profile is re-installed, causing the computer to have a non-User Approved MDM status. Subsequent use of the jamf mdm command does not produce this result.  
Workaround: Approve the MDM profile in **System Preferences > Profiles**.
- [SUS-2896] AirPlay Permissions do not display in the Jamf Pro Summary.
- [SUS-5128], [SUS-5253] Jamf Pro fails to disassociate an email address used for VPP registration when the user is deleted from Jamf Pro.

## 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".
- [PI-005189] Self Service for macOS fails to notify users that an update for a Mac App Store app is available if an older version of the app is already installed on the computer.
- [PI-005563] Notifications that appear in Self Service or in Notification Center may cause CPU to spike suddenly on computers.
- [PI-005760] Self Service notifications may fail to display in Notification Center.

## 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 issue is known in Composer:

[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.

## Jamf Admin

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

- [PI-004101] Jamf Admin fails to upload and replicate large packages to the JCDS or AWS distribution points.
- [PI-004504] Packages may intermittently fail to upload to JCDS via Jamf Admin.

## 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>

## Documentation Deprecations

The following documentation changes will be implemented in an upcoming release of Jamf Pro:

- ***Jamf Pro Release Notes PDF deprecation***—The release notes will be available in web-based format only.
- ***Manually Installing Jamf Pro deprecation***—Instructions for manually installing Jamf Pro will be included in the *Jamf Pro Installation and Configuration Guide for Linux* and *Jamf Pro Installation and Configuration Guide for Windows*.

The following PDF documents will be removed from the Composer DMG in an upcoming release:

- ***Composer Release Notes***
- ***Composer User Guide***