jamf | PRO

Jamf Pro Release Notes

Version 10.1.0

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

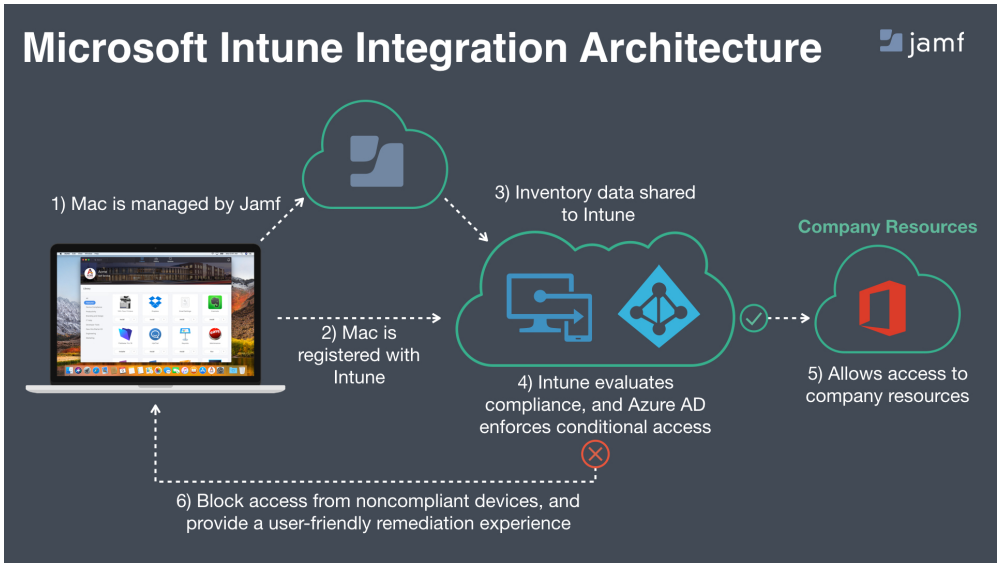
Contents

What's New

Microsoft Intune Integration for macOS

You can now integrate with Microsoft Intune to ensure that only trusted users, from compliant computers, using approved applications, are accessing organizational resources. Jamf Pro delivers information about the management state and health of Mac computers to Microsoft Intune's device compliance engine, which integrates with Azure Active Directory (Azure AD) Conditional Access. This allows you to identify unmanaged and non-compliant Mac devices, and remediate them.

To access the Microsoft Intune Integration settings in Jamf Pro, go to **Settings > Global Management > Microsoft Intune Integration**. For information on configuring the settings, see Microsoft Intune Integration in the *Jamf Pro Administrator's Guide*.



Integrating with Microsoft Intune allows you to do the following:

- **Share computer inventory with Microsoft Intune**
  Jamf Pro sends inventory information to Microsoft Intune for each computer that has registered with Azure AD. A centralized view of macOS computers managed by Jamf Pro is available in Microsoft Intune.
- **Restrict access to applications set up with Azure AD**
  You can enforce compliance on computers managed by Jamf Pro and restrict access to applications set up with Azure AD authentication (i.e., Office 365).
- **Feature compliance policies in Jamf Self Service for macOS**
  A new "Device Compliance" category has been added to Self Service. You can feature compliance policies in this category to ensure computers and applications are compliant with organizational security requirements.

- **Require users to register their devices with Azure AD via a policy payload**
  You can now deploy a policy to users initiating the registration process with Azure AD. Registering the computer with Azure AD is an end user workflow. To configure this policy for managed computers, navigate to the new Microsoft Intune Integration payload when creating a policy in Jamf Pro.
- **View Azure Active Directory ID information in Jamf Pro**
  When a computer is registered with Azure Active Directory, you can view Azure Active Directory information for a user and a computer in Jamf Pro. To view Azure Active Directory ID information, navigate to the General tab in inventory information of a computer.

For step-by-step instructions on how to integrate with Microsoft Intune, including information on the capabilities listed above, see the following technical paper:
Integrating with Microsoft Intune to Enforce Compliance on Macs Managed by Jamf Pro

iOS Configuration Profile Enhancement

Cisco AnyConnect is now available as a connection type in the VPN payload. The **Provider Type** menu has also been updated and now includes Packet-tunnel and App-proxy options.

Note: When upgrading to Jamf Pro 10.1.0, any existing iOS configuration profiles with Cisco AnyConnect selected in the **Connection Type** pop-up menu will be migrated to Cisco Legacy and the provider type will automatically be set to App-proxy.

VPP Accounts Enhancements

- Jamf Pro now displays VPP service token Location details for the configured VPP accounts if your environment integrates with Apple School Manager. For detailed information on migrating to Apps and Books in Apple School Manager, see the following article from Apple's support website:
  https://support.apple.com/HT208257
  Note: Information is only synced from Apple School Manager to Jamf Pro, not from Jamf Pro to Apple School Manager. Location is only displayed if it is available from Apple School Manager.
- Jamf Pro now allows a VPP Accounts email notification to be sent daily when there are no remaining licenses left for a particular VPP-managed distribution content item in a given VPP token. To enable VPP account email notifications in Jamf Pro, navigate to **Settings** > **Global Management** > **VPP Accounts** > **Notifications**.
  Note: At least one VPP account must exist in Jamf Pro and you must be logged in with a Jamf Pro user account that has full access to properly configure a notification.

Disabling Apps and eBooks

- Mac App Store apps, mobile device apps, and eBooks can now be manually disabled. This stops the item's subsequent installations and it is not displayed in Self Service. You cannot edit the app or eBook details if it is disabled. To manually disable the item, navigate to the **General** tab of the app or eBook details.
  Note: Disabling the content item will not remove the app or eBook already installed on computers and mobile devices.
- Mac App Store apps, mobile device apps, and eBooks will now be automatically disabled if they are VPP-managed distribution content items that have been removed from the App Store. You will not be able to assign licenses, and the installation commands will not be sent. The disabled items will not be displayed in Self Service. You cannot edit the automatically disabled items or enable them again. To view the item's "Enabled" status, navigate to the **General** tab of the app or eBook details.
  Note : Disabling the VPP-managed distribution content item will not remove the app or eBook already installed on computers and mobile devices.

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

In-house apps downloaded from the Jamf Pro database will now be automatically secured with JWT.

Note: If the token expires, the next push of the app installation will retrieve a new token with a new expiration time. Default expiration time is five minutes.

Jamf Self Service for macOS Branding Settings Enhancement

You can now choose to display a semi-transparent overlay over the branding header image in the Self Service.

What's Changed

Changes and Considerations for This Release

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

New Location for VPP Invitations Made Available In Jamf Self Service for macOS

VPP invitations that are made available in Self Service for macOS now appear in the Notifications list in Self Service. For more information, see the VPP User Registration section in the *Jamf Pro Administrator's Guide*.

FileVault 2 Partition Encryption State Change

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 or advanced computer searches that use 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 and advanced computer searches.

Memcached Recommended for Clustered Environments

Memcached is recommended for Jamf Pro 10.1.0, 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
10.0.0	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 ***This information was updated 15 December 2017.***
9.101.0	Change to FileVault personal recovery key settings for macOS 10.13 or later	On computers with macOS 10.13 or later, you must use the FileVault options in the Security & Privacy payload to enable and manage the FileVault personal recovery key. The FileVault Recovery Key Redirection payload is no longer supported on macOS 10.13 or later. However, you must continue to use the FileVault Recovery Key Redirection payload to manage the FileVault personal recovery key for computers with macOS 10.12 or earlier.
9.101.0	Additional privileges required for PreStage imaging and Autorun imaging workflows	A Jamf Pro user account with the "Jamf Imaging - PreStage Imaging and Autorun Imaging" privilege is now required for PreStage imaging and Autorun imaging workflows. For more information on the permissions required for imaging computers, see the following Knowledge Base article: Imaging Computer Permission Requirements

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.
9.99.0	Connection to Apple GSX requires TLS 1.2	Jamf Pro 9.99.0 and later use TLS 1.2 for GSX by default, regardless of Java version. For the Jamf Pro 9.98 or earlier, you must upgrade to Java 1.8 to maintain GSX connection.

Starting with version...	Change or Consideration	Description
9.99.0	Removed support for Home Screen Layout web clips for mobile device configuration profiles	Web clips can no longer be set for the Dock or page layouts in the Home Screen Layout payload for mobile device configuration profiles. After upgrading to version 9.99.0 or later, previously set web clips will no longer display when viewing mobile device configuration profiles in Jamf Pro.

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

The following functionality has been removed:

Apache ActiveMQ Artemis—The integration with the Apache ActiveMQ Artemis message broker has been removed. In conjunction with this, the **Enable Message Broker Debug Mode** option on the Jamf Pro Server Logs page has been removed.

Bug Fixes and Enhancements

Jamf Pro Server

- [PI-002088] Fixed an issue that resulted in some devices not showing up in a Mobile Device Smart Group search.
- [PI-002730] Fixed an issue that caused a "Confirm Form Resubmission" message to incorrectly display after the **Cancel All** button was clicked for all failed management commands on a mobile device.
- [PI-002997] Fixed an issue that resulted in performance issues in large environments when creating a smart group with the "Apps Not in App Catalog Installed" criteria.
- [PI-003224] Fixed a display issue that occurred when attempting to add a site to a user's inventory information.
- [PI-003324] Fixed an issue that caused in managed mobile devices to be displayed in a smart mobile device group even if it contained invalid criteria.
- [PI-003355] Fixed an issue that caused the “Expires” criteria to fail to function correctly when creating a smart mobile device group.
- [PI-003451] Fixed a server issue that caused a stack trace error to appear.
- [PI-003751] Fixed an issue that caused Jamf Pro to incorrectly display placeholder text in some areas.
- [PI-003995] Fixed an issue that caused incorrect mobile devices to be displayed in smart mobile device group searches that contained the “Cellular Technology” criteria or the “is/is not” operator.
- [PI-004009] Fixed an issue that caused incorrect mobile devices to be displayed in smart mobile device group searches that contained the “Certificates Expiring” criteria or the “in more than x days” operator.
- [PI-004020] Fixed an issue that caused incorrect mobile devices to be displayed in smart mobile device group searches that contained the “Certificates Expiring” criteria or the “in less than x days” operator.
- [PI-004025] Fixed an issue that that resulted in the API failing to modify the user extension attribute values when a user was created.
- [PI-004033] Fixed an issue that caused incorrect mobile devices to be displayed in smart mobile device group searches that contained the “App Identifier” criteria or the "is not" and "not like" operators.
- [PI-004036] Fixed an issue that caused incorrect mobile devices to be displayed in smart mobile device group searches that contained the “App Version” criteria or the "is not" and "not like" operators.
- [PI-004037] Fixed an issue that caused incorrect mobile devices to be displayed in a smart mobile device group search that contained the “Certificate Name” and "Identify" criteria and the "is not" operator.
- [PI-004140] Fixed an issue that caused Apple TV devices to be displayed incorrectly in a smart mobile device group search that contained the “Enrollment Method: PreStage enrollment” criteria.

- [PI-004225] During user-initiated enrollment of mobile devices with iOS 10 or later, pages now auto-advance promptly. This prevents the user from accidentally installing the CA certificate multiple times.
- [PI-004243] Fixed an issue that allowed in-house apps to download without authentication.
- [PI-004339] Fixed an issue that caused duplicate users to be created in Jamf Pro when importing users from Apple School Manager. This could prevent devices from enrolling and checking in with Jamf Pro.
- [PI-004383] Fixed an issued that caused the Adobe Temporary Install Account to not login automatically during the post-imaging process.
- [PI-004388] Fixed an issue that resulted in performance issues in large environments if a smart mobile device group search contained a large number of criteria using Extension Attribute data.
- [PI-004439] Fixed an issue that caused all configuration profiles that included the Home Screen Layout payload to deploy incorrectly when upgrading from Jamf Pro 9.100.0 or later.
- [PI-004550] Fixed an issue that caused packages to be deleted from the JCDS without user interaction. This caused Jamf Pro to incorrectly display the package as successfully uploaded.
- [PI-004587] You can now use the keyboard to navigate through assistants in Jamf Pro.
- [PI-004634] When using the PUT and POST operations to add a software title to a site, the Jamf API no longer incorrectly creates duplicate titles.
- [PI-004703] Fixed an issue that prevented licensed software record attachments from being downloaded.
- [PI-004706] Fixed an issue that caused the Computer PreStage Enrollments setting to incorrectly display as disabled when a Device Enrollment Program (DEP) instance was already configured.
- [PI-004724] You can now navigate to disabled policies via the Jamf Pro dashboard.
- [PI-004737] Fixed broken breadcrumbs.
- [PRI-229] Jamf Pro now correctly prevents users from modifying a patch management software title extension attribute.
- [PRI-486] The Jamf API no longer fails when using the GET operation with the /name endpoint when the software title belongs to a site.
- [PRI-689] The patch policies table in Jamf Pro now displays correctly.
- [PRI-708] Fixed an issue that resulted in an incorrect Jamf icon being displayed in the `/Library/Application Support/JAMF` directory.
- [PRI-707] Fixed an issue where the `jamf version` command displayed an error message in Terminal in some versions of macOS.
- [PRI-733] Fixed an issue where some database values were not removed when a computer record was deleted from Jamf Pro.
- [PRI-777] Fixed an issue that resulted in some pages displaying incorrectly if a Smart Mobile Device Group contained open and closed parentheses in the search criteria.

Jamf Self Service for macOS

- [PI-004660] Fixed an issue that caused Self Service for macOS to intermittently crash.
- [PI-004695] The Self Service Bookmarks category can now be set as the Library main page.

- [PI-004729] When making an existing policy available in Self Service, the Self Service **Display Name** text field is now automatically populated with the policy name.
- [PI-004730] Fixed an issue that caused the branding header image to display incorrectly in the **Preview** field in the Self Service Branding settings.
- [PRI-236] Display names of items made available in Self Service for macOS now wrap to a second line if needed in the Self Service for macOS application.
- [SUS-4714] Fixed issue where users cannot log in to Self Service for macOS using their single sign-on credentials if Jamf Pro is not installed as the "ROOT" web application.
- [THS-2978] Fixed an issue that caused Self Service for macOS to become unresponsive when viewed on a small screen.
- [THS-3308] Fixed an issue that incorrectly caused the Self Service authentication type to switch from single sign-on to LDAP account or Jamf Pro user account after upgrading to Jamf Pro 10.0.0.

Composer

[PI-004384] Fixed an issue that prevented Composer from building an APFS-formatted OS package correctly.

Recon

[PI-004718] Fixed an issue in Recon that caused the Tab key to fail to switch between fields.

Jamf Imaging

- [PRI-735] Fixed an issue that resulted in Jamf Imaging not unmounting AFP shares during multiple Target Mode Imaging attempts.
- [PI-004430] Fixed an issued that caused Jamf Imaging to fail to populate information saved in a PreStage imaging configuration if using the List of Names method for naming computers.

Known Issues

Third-party Software

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

- iOS 11 does not support 32-bit apps. If you deploy a 32-bit app and a VPP license to a mobile device with iOS 11, a VPP license will be used, but the app will not install.
- The "Allow all" or "Prevent all" cellular data usage and data roaming usage settings cannot be edited after they have been set on a mobile device with iOS 9.
- [D-004382] Tapping the URL in an email enrollment invitation on an iOS 6 device draws a blank page. Users should copy-and-paste the URL into the Safari app instead.
- [D-005532] macOS configuration profiles with a Login Window payload that is configured to deny users and groups the ability to log in fail to do so.
- [D-005882] The **Computer administrators may refresh or disable management** option in a Login Window payload of a macOS configuration profile is not applied at login.
- [D-005900] Jamf Pro fails to install configuration profiles with a Web Clip payload on computers with macOS v10.9.
- [D-006026] Jamf Pro fails to restrict Game Center when the **Allow use of Game Center** checkbox is deselected in the Restrictions payload in macOS configuration profiles.
- [D-006250] A customized Self Service web clip icon uploaded using Jamf Pro will revert to the default Jamf Pro icon on iOS 7 devices.
- [D-006393] The Start screen saver after: option in a Login Window payload of a macOS configuration profile is not applied on computers with macOS v10.8.4 or v10.8.5.
- [D-006662] Installed macOS configuration profiles that include a VPN payload with the Use Hybrid Authentication checkbox selected append "[hybrid]" to the group name in the VPN authentication settings on the computer, which causes group authentication to fail.
- [D-006758] iOS configuration profiles with a Single App Mode payload fail to require a passcode on supervised iOS 7 devices when the devices have a passcode and are locked.
- [D-006979] When enrolling a computer using a QuickAdd package, the QuickAdd installer incorrectly prompts users for local administrator credentials twice if the **Restrict re-enrollment to authorized users only** checkbox is selected.
- [D-007004] iOS configuration profiles with a cookies restriction fail to set the specified restriction and hide other cookies restrictions on the device. The restrictions that are hidden depend on the restriction specified in the profile.
- [D-007245] The configuration page fails to display correctly when enrolling a mobile device via PreStage enrollment.
- [D-007486] SMB shares sometimes fail to mount on a computer with macOS v10.9.
- [D-007511] If the option to skip the Restore page is selected for a PreStage enrollment in Jamf Pro, the Restore page is not skipped during enrollment if the enrollment process is restarted during the Setup Assistant.

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

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

Jamf Pro Server

Updated 15 December 2017 with the following additions:

- When the Microsoft Intune Integration is enabled, if both user-level and computer-level passcode profiles are in place, the less secure passcode setting is sometimes reported by Jamf Pro to Microsoft Intune. Due to this issue, it is recommended that you scope a complex passcode configuration profile to all users of the computer and also at the computer level.
- [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.

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

- Some areas in the Jamf Pro interface do not display correctly.
- Some areas in the Jamf Pro interface incorrectly reference old product names.
- Some objects in Jamf Pro do not display correct gender rules when viewed in French.
- Pages in Jamf Pro may fail to load if the browser “Back” button is used.
- AirPlay Permissions do not display in the Jamf Pro Summary.
- A blank choice 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.
- Patch policies that are disabled and patch policies that are not in the scope for deployment are incorrectly displayed in the management information for a computer.
- When using multiple web browser tabs simultaneously, duplicates of a patch management software title may incorrectly be created.

- When creating a patch policy, an error is written to the `JAMFSoftwareServer.log` file.
- When using the PUT and POST operations to add a software title to a site, the Jamf API may incorrectly create duplicate titles.
- When using the GET operation with the /name endpoint, the Jamf API fails when the software title belongs to a site.
- When a user with custom privileges for only "Patch Management Software Titles" and "Patch Policies" who does not have the "Computers" privilege attempts to create a new patch policy, Jamf Pro fails to display the page.
- When included in a breadcrumb, the display name of a patch management software title supports only alphanumeric characters.
- A patch report does not display correctly when viewing it on a mobile device.
- The Limited Access settings are incorrectly displayed for non-master Jamf Pro instances when switching from "Full Access" and then saving.
- Jamf Distribution Server (JDS) instances do not display the correct uploaded packages in Jamf Pro.
- When a Jamf Pro user account is created via the jamf binary, FileVault 2 fails to be enabled for that account.
- When submitting inventory, the `com.jamfsoftware.jamf` daemon causes multiple jamf processes to fail to complete successfully.
- When updating a mobile device via the API, a large number of queries are written to the `jamfsoftwareserver.log`.
- 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-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-002791] Mac App Store apps do not update automatically when the distribution method is set to “Install Automatically/Prompt Users to Install” and the Automatically update app checkbox is selected.
- [PI-003356] Jamf Pro may incorrectly display placeholder text in Settings.
  Workaround: Clear your web browser cache.
- [PI-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-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-003771] When the Account Settings payload is configured for a computer PreStage enrollment, the MDM profile is installed on the computer, but the jamf binary may not install due to a timeout.
- [PI-003803] When using the POST operation to create a Webhook in XML format, the Jamf API sometimes fails to create the Webhook.

- [PI-003940] Beginning with Jamf Pro 9.98, Android devices do not update after first enroll. The following commands are also unable to complete: Install Personal Device Profile, Wipe Institutional Device, and Lock Device.
- [PI-003952] Attachments added to Apple TV devices during enrollment do not display in the devices' inventory information.
- [PI-004025] When creating a user and updating the user extension attribute with the API, the API fails to modify the user extension attribute values.
- [PI-004196] When Single Sign-On authentication is enabled in Jamf Pro, administrators are occasionally not able to reliably configure which sites are visible to a user during user-initiated enrollment.
- [PI-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-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-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-004670] Jamf Pro incorrectly allows you to select an LDAP user group as a limitation for the scope of a patch policy. (The LDAP user group limitation is not supported.)
- [PI-004915] Apple Push Notifications will fail for Jamf Pro 10.0.0 or later if the server cannot reach http://www.apple.com/DTDs/PropertyList-1.0.dtd . This might occur in environments with an outbound firewall that restricts Jamf Pro from accessing the Internet. A "JAXBPlistParser timeout" error will appear in the `JAMFSoftwareServer.log` file, and all MDM requests will result in a 400 error.
  Workaround: Whitelist Jamf Pro to allow www.apple.com on port 80. If you have questions or concerns, contact your Jamf account representative and reference PI-004915.
- [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-005032] When a VPP-managed distribution content item is manually disabled, new licenses continue to be assigned to devices.
- [PI-005039] The Jamf Pro System Settings page does not display smoothly when viewed using Safari.
- [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 Jamf Self Service for macOS.
- [PI-004602] A 400 error incorrectly displays in the `JAMFSoftwareServer.log` after Self Service for macOS is launched on a computer for the first time.
- [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 Jamf Self Service for macOS. Self Service does not support animated GIFs.

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.

Jamf Admin

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

Due to changes in the way Jamf Admin manages macOS installers for macOS 10.12.4 or later, the `InstallESD.dmg` file is no longer automatically extracted from the macOS `Installer.app` file. Workaround: For macOS 10.12.4, 10.12.5, and 10.12.6, manually extract the `InstallESD.dmg` from the `Installer.app` update file and upload it to Jamf Admin. On the **General** tab, select the **Item is a DMG with a macOS Installer, or Adobe Updater/Installer for CS3 or CS4** checkbox, and click **OK**. The use of macOS installers for imaging is deprecated in macOS 10.13.

Jamf Imaging

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

Computers with macOS 10.12 or earlier cannot be reimaged with macOS 10.13.

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