restrict downloads to mac app store jamf

Mac App Store Apps.

Jamf Pro allows you to distribute Mac App Store apps to computers and users. You can also use Jamf Pro to update Mac App Store apps that have been installed by Jamf Pro.

Jamf Pro provides two Mac App Store app distribution methods: make the app available in Self Service, or install the app automatically/prompt users to install the app. When you distribute a Mac App Store app, you add it to Jamf Pro and configure settings for the app, including the distribution method. Then, you specify the users and computers that should receive it (called "scope").

Note: Removing targets from the scope of the app revokes the app license (if applicable) but does not remove the app from the computer. To completely remove the app, the app must be manually dragged to the Trash on the target computer.

Mac App Store apps purchased in volume can be distributed to computers or users with managed distribution. For more information, see Managed Distribution for Computers and User-Based Volume Assignments.

As an alternative to managed distribution, Jamf Pro also supports distributing Mac App Store apps to computers using redeemable VPP codes. For more information, see VPP Code Distribution for Computers.

Mac App Store apps distributed with user-based assignments or with VPP codes are not managed by Jamf Pro. Users can update apps using the Mac App Store or uninstall the apps from their computers.

Requirements.

To allow users to install Mac App Store apps from Self Service via MDM, or to allow Mac App Store apps to be installed automatically you need:

A push certificate in Jamf Pro (For information, see Push Certificates.)

The Enable certificate-based authentication and Enable push notifications settings configured in Jamf Pro (For information, see Security Settings.)

Computers that are bound to a directory service or local user accounts that have been MDM-enabled (For information, see Binding to Directory Services and the Enabling MDM for Local User Accounts Knowledge Base article.)

Note: On computers with macOS 10.10 or later and Jamf Pro v9.64 or later, the local user account is automatically MDM-enabled the first time a Mac App Store app is installed automatically or via Self Service, or a user-level configuration profile is installed via Self Service. With PreStage enrollment, the first local user account that is created is made MDM-enabled.

On computers with macOS 10.9 or earlier and Jamf Pro v9.4–v9.64, the user is prompted with a "Local Administrator credentials required" message the first time a Mac App Store app is installed automatically or via Self Service, or a user-level configuration profile is installed via Self Service. The user can click OK or Cancel when prompted.

Apps assigned to computers or users via managed distribution.

For device-based assignments, you need:

Computers with macOS 10.11 or later.

For user-based assignments, you need:

Computers with macOS 10.9 or later.

Note: If a computer does not have macOS 10.9 or later and the "Install Automatically/Prompt Users to Install" distribution method is selected, the app will instead be made available in Self Service.

Users registered with volume purchasing and the apps assigned to them using volume assignments (For information, see Volume Purchasing User Registration and User-Based Volume Assignments.)

Users must be logged in to Mac App Store with the Apple ID used during volume purchasing registration.

Note: If the scope for a Mac App Store app is configured to include a computer and the user is not assigned to that computer in Jamf Pro, the app will instead be made available in Self Service.

To allow users to install apps from the Mac App Store (linked from Self Service), you need:

Computers with macOS 10.7 or later.

Computers that are bound to a directory service or local user accounts that have been MDM-enabled (For information, see Binding to Directory Services and the Enabling MDM for Local User Accounts Knowledge Base article.)

Users may be prompted to enter an Apple ID.

Distributing a Mac App Store App.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Mac App Store Apps .

Click New .

Do one of the following:

To add the app by browsing the App Store, enter the name of the app, choose an App Store country, and then click Next . Then click Add for the app you want to add.

To add the app by uploading a VPP code spreadsheet, click Choose File and upload the Excel spreadsheet (.xls) that contains VPP codes for the app.

To add the app by manually entering information about it, click Enter Manually .

Use the General pane to configure settings for the app, including the distribution method. For apps distributed using managed distribution, you can also enable automatic app updates.

Click the Scope tab and configure the scope of the app. For more information, see Scope.

(Optional) Click the Self Service tab and configure the way the app is displayed in Self Service. You can customize the text displayed in the description for the app in Self Service by using Markdown in the Description field. For information about Markdown, see the Using Markdown to Format Text Knowledge Base article.

Note: The Self Service tab is only displayed if "Make Available in Self Service" is chosen in the Distribution Method pop-up menu.

(Optional) If you want to distribute the app directly to computers via managed distribution, do the following:

Click the Managed Distribution tab, and then click the Device Assignments tab.

Select the Assign Volume Content checkbox.

Choose the location that has purchased the app to distribute to computers.

(Optional) If you want to associate VPP codes with the app and have not already uploaded a VPP code spreadsheet, do the following:

Click the Managed Distribution tab, and then click the VPP Codes tab.

Upload the Excel spreadsheet (.xls) that contains VPP codes for the app.

Click Save .

If users were added as targets to the scope, the app is distributed to the computers those users are assigned to the next time the computers check in with Jamf Pro.

Updating a Mac App Store App.

Jamf Pro allows you to update an individual Mac App Store app in the following ways:

Schedule automatic Mac App Store app updates —This automatically updates the app description, icon, and version in Jamf Pro and on computers. This update happens once a day depending on the time of day you specify.

Automatically force Mac App Store apps to update —You can automatically force a Mac App Store app to update on computers. This update happens automatically every time computers check in with Jamf Pro.

Manually force a Mac App Store app to update —You can manually force an app to update immediately on computers if there are updates available in Jamf Pro. This applies only to apps distributed using managed distribution for computers.

Distribute a Mac App Store app update —You can distribute an update for a Mac App Store app by manually updating the version number and URL for the app in Jamf Pro. The update is distributed to computers the next time they contact Jamf Pro.

Note: Jamf Pro also allows you to enable automatic updates for all Mac App Store apps, or force all Mac App Store apps to update immediately. For more information, see Mac App Store App Update Settings.

Scheduling Automatic App Updates.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Mac App Store Apps .

Click the app for which you want to enable automatic app updates.

Click Edit .

Select Schedule Jamf Pro to automatically check the App Store for app updates .

Choose a country or region to use when syncing apps with the App Store from the App Store Country or Region pop-up menu.

Set the time of day to sync apps with the App Store with the App Store Sync Time pop-up menus.

Click Save .

The app is updated in Jamf Pro and on computers in the scope based on the time you configure the app to sync with the Mac App Store.

Automatically Forcing an App Update.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Mac App Store Apps .

Click the app you want to update.

Click Edit .

Click Force Update .

Click Save .

The app is updated immediately on computers in the scope each time computers check in with Jamf Pro.

Manually Forcing an App Update.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Mac App Store Apps .

Click the app you want to update.

Click Edit .

Click Force Update .

Click Save .

The app is updated immediately on computers in the scope if there is an update available in Jamf Pro.

Distributing an App Update.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Mac App Store Apps .

Click the app you want to update.

Click Edit .

Enter the new version number and URL. Important: Do not change the bundle identifier. Jamf Pro uses the existing bundle identifier to distribute the update.

Click Save .

The update is distributed the next time computers in the scope contact Jamf Pro.

Further Considerations.

Apps are enabled by default when added to Jamf Pro. This means you can edit the app details and assign licenses, and the app will be installed on computers or displayed in Self Service based on the selected distribution method. You can disable an app by deselecting the Enable checkbox. This stops the app's subsequent installations and it is not displayed in Self Service. You cannot edit app details if it is disabled.

A Mac App Store app will be automatically disabled in Jamf Pro if it is a managed distribution item that has been removed from the Mac App Store. You will not be able to assign licenses, and the installation commands will not be sent. The app will not be displayed in Self Service. An automatically disabled managed distribution item will not be removed from computers that already have this item installed.

Related Information.

For related information, see the following sections in this guide:

Computer Inventory Information Find out how to view and edit inventory information for a computer.

Viewing Mac App Store Apps for a Computer Find out how to view the Mac App Store apps in the scope of a computer.

Viewing the History for a Computer Find out how to view and cancel pending Mac App Store app installations for a computer.

Items Available to Users in Jamf Self Service for macOS Learn about which items can be made available to users in Self Service for macOS.

Computer Configuration Profiles You can create a computer configuration profile with a Per-App VPN connection.

Packaging and Deploying the macOS Installer.

If you want to automate the upgrade process, you can package the macOS installer and install it automatically or allow users to install it via Self Service. This method is recommended for major macOS releases. You can erase the data on computers with macOS 10.13.4 or later by using the --eraseinstall flag. Additionally, you have the option of using a script to customize the end user experience.

Deploying a policy to upgrade computers to macOS 10.13 or later involves the following steps:

Add the .app file for macOS to Jamf Admin or Composer.

Create a smart computer group to identify eligible computers.

Cache the InstallESD.dmg file using a policy.

Create a smart computer group with the cached PKG file.

Create a policy for upgrading macOS automatically or via Self Service.

Note: The name of the InstallESD.dmg file in Jamf Admin and Composer will vary depending on the version of macOS that you plan to deploy.

Requirements.

Jamf Pro 9.21 or later Note: If you are using Jamf Pro 8.3-9.1, see the Deploying macOS 10.7 or Later with Jamf Pro Knowledge Base article for instructions on deploying a macOS upgrade.

Jamf Admin or Composer.

The .app file for the version of macOS that you plan to deploy (For example, Install macOS Mojave.app .) You can obtain the latest .app file for macOS from the Mac App Store.

Managed computers with:

(Optional) Self Service.

The system requirements for the version of macOS that you plan to deploy.

Step 1: Add the .app File for macOS to Jamf Admin or Composer.

Adding the .app File for macOS to Jamf Admin.

Jamf Admin extracts the InstallESD.dmg file from the .app file so you can cache and install it using policies.

Open Jamf Admin and authenticate to the Jamf Pro server.

Drag the .app file to the main repository in Jamf Admin. Jamf Admin extracts the InstallESD.dmg file, analyzes its contents, and adds it to the

master distribution point and Jamf Pro. The InstallESD.dmg file is displayed in blue text until you add it to a category.

Double-click the package in the main repository.

Click the General tab and choose a category for the package.

Click OK .

Adding the .app File for macOS to Composer.

Composer packages the .app file so you can cache and install it using policies.

Open Composer and authenticate locally.

Drag the .app file into a folder in Composer.

Select the .app file from the Sources list in the sidebar.

In the toolbar, click Build as PKG . Note: If the Build flat PKGs preference is enabled and the package source contains scripts that are not supported by flat PKGs, a dialog will appear. To disable this preference for this package only, click Build as non-flat PKG . To build a flat PKG that ignores unsupported scripts, click Build as flat PKG . For more information on which scripts are supported by flat PKGs, see Adding Scripts to Package Sources in the Jamf Pro Administrator's Guide .

Select the master distribution point in Jamf Pro, and then click Save .

Step 2: Create a Smart Computer Group to Identify Eligible Computers.

Create a smart computer group to identify computers that can be upgraded.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Smart Computer Groups .

Click New .

Use the Computer Group pane to configure basic settings for the group. To enable email notifications, select the Send email notification on membership change checkbox.

Click the Criteria tab and add criteria to the group: Note: These are the minimum recommendations, consider adding other criteria to your smart computer group.

Click Add .

Click Choose for the "Operating System Version". Note: Only your 30 most frequently used criteria are listed. To display additional criteria, click Show Advanced Criteria .

Choose an operator from the Operator pop-up menu.

Enter the macOS version you want to upgrade in the Value field, or browse for a macOS version by clicking Browse .

(Optional) Repeat steps a through d to create a range of macOS versions to upgrade.

Choose "and" from the And/Or pop-up menus to specify the relationships between criteria.

To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.

Click Save . Operations in the group take place in the order they are listed (top to bottom). Group memberships are updated each time computers check in with Jamf Pro and meet or fail to meet the specified criteria.

To view the eligible computers, click View .

Step 3: Cache the InstallESD.dmg File.

After adding the .app file to Jamf Admin or Composer, you can cache the file using a policy. Caching the file ahead of time speeds up the upgrade process.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Policies .

Click New .

In the General payload, enter a display name for the policy. For example, “Cache InstallESD.dmg”.

Select Recurring Check-in as the trigger.

Choose “Once per Computer” from the Execution Frequency pop-up menu.

Select the Packages payload and click Configure .

Click Add for the DMG or PKG file.

Choose “Cache” from the Action pop-up menu.

Specify a distribution point for computers to download the package from.

Select the Maintenance payload and click Configure .

Ensure that the Update Inventory checkbox is selected.

Click the Scope tab and configure the scope of the policy. You can add the previously created smart group of eligible computers as the scope. For more information, see Scope in the Jamf Pro Administrator's Guide .

Click Save .

The PKG file is cached on computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload.

Step 4: Create a Smart Computer Group with the Cached PKG File.

Create a smart group of computers with the PKG file cached. The smart group will be used as the scope of the policy for installing the macOS upgrade automatically or for allowing users to download the upgrade via Self Service.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Smart Computer Groups .

Click New .

On the Computer Group pane, enter a display name for the smart computer group. For example, “InstallESD.dmg Cached”.

Click the Criteria tab.

Click Add .

Click Choose for “Cached Packages”. Note: Only your 30 most frequently used criteria are listed. To display additional criteria, click Show Advanced Criteria .

Choose “has” from the Operator pop-up menu.

Click Browse .

Click Choose for the PKG file. Note: The PKG file is not available as a value until it has been cached on at least one computer.

Click Save .

Step 4: Create a Policy for Upgrading macOS.

After caching the InstallESD.dmg file, you can create a policy that allows users to upgrade macOS through Self Service, or that upgrades macOS on computers in the scope automatically.

Creating a Self Service Policy for Upgrading macOS.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Policies .

Click New .

In the General payload, enter a display name for the policy. For example, “Upgrade macOS”.

Choose “Once per Computer” from the Execution Frequency pop-up menu.

Select the Packages payload and click Configure .

Click Add for the InstallESD.dmg file.

Choose “Install Cached” from the Action pop-up menu.

(Optional) To use a script to install macOS, use the Scripts payload to add the script and configure the settings. For information, see Managing Scripts and Running Scripts in the Jamf Pro Administrator's Guide . Note: You can also use Jamf Helper to add additional end-user messaging.

Select the Files and Processes payload and click Configure .

In the Execute Command field, enter the file path to the installer with the --startosinstall command. For example, " /file/path/Install macOS High Sierra.app/Contents/Resources/startosinstall ".

(Optional) To erase data while installing macOS, add the --eraseinstall flag to the command.

(Optional) To suppress end-user messages during installation, add the --agreetolicense flag to the command.

Click the Scope tab.

Click Add .

Click the Computer Groups tab.

Click Add for the smart computer group with the cached PKG file you just created.

Click the Self Service tab.

Select Make the policy available in Self Service .

Configure how the policy is displayed in Self Service using the settings on the pane.

Click Save .

The policy is made available in Self Service on computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload. macOS is upgraded when users run the policy from Self Service.

Upgrading FileVault 2-enabled drives from macOS 10.7 or 10.8 prompts users to enter their password after reboot. Upgrading FileVault 2-enabled drives from macOS 10.9 or later automatically bypasses authentication after reboot.

Creating a Policy for Upgrading macOS Automatically.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Policies .

Click New .

In the General payload, enter a display name for the policy. For example, “Upgrade macOS”.

Choose “Once per Computer” from the Execution Frequency pop-up menu.

Select the Packages payload and click Configure .

Click Add for the InstallESD.dmg file.

Choose “Install Cached” from the Action pop-up menu.

(Optional) To use a script to install macOS, use the Scripts payload to add the script and configure the settings. For information, see Managing Scripts and Running Scripts in the Jamf Pro Administrator's Guide .

Select the Files and Processes payload and click Configure .

In the Execute Command field, enter the file path to the installer with the --startosinstall command. For example, " /file/path/Install macOS High

Sierra.app/Contents/Resources/startosinstall "

(Optional) To erase data while installing macOS, add the --eraseinstall flag to the command.

(Optional) To suppress user messages while installing macOS, add the --agreetolicense flag to the command.

Click the Scope tab.

Click Add .

Click the Computer Groups tab.

Click Add for the smart computer group with the cached PKG file you just created.

(Optional) Click the User Interaction tab and enter messages to display to users or allow users to defer the policy. For more information, see User Interaction in the Jamf Pro Administrator's Guide .

Click Save .

The upgrade installs on computers in the smart group depending on the trigger configured in the policy.

Packaging and Deploying the macOS Installer.

If you want to automate the upgrade process, you can package the macOS installer and install it automatically or allow users to install it via Self Service. This method is recommended for major macOS releases. You can erase the data on computers with macOS 10.13.4 or later by using the --eraseinstall flag. Additionally, you have the option of using a script to customize the end user experience.

Deploying a policy to upgrade computers to macOS 10.13 or later involves the following steps:

Add the .app file for macOS to Jamf Admin or Composer.

Create a smart computer group to identify eligible computers.

Cache the macOS installer package file using a policy.

Create a smart computer group with the cached macOS installer package.

Create a policy for upgrading macOS automatically or via Self Service.

Note: The name of the macOS installer package file in Jamf Admin and Composer will vary depending on the version of macOS that you plan to deploy.

Requirements.

Jamf Pro 9.98 or later.

Note: If you are using Jamf Pro 8.3-9.1, see the Deploying macOS 10.7 or Later with Jamf Pro Knowledge Base article for instructions on deploying a macOS upgrade.

Jamf Admin or Composer.

The .app file for the version of macOS that you plan to deploy (For example, Install macOS Mojave.app .) You can obtain the latest .app file for macOS from the Mac App Store.

Managed computers with:

(Optional) Self Service.

The system requirements for the version of macOS that you plan to deploy.

Step 1: Add the .app File for macOS to Jamf Admin or Composer.

Adding the .app File for macOS to Jamf Admin.

Jamf Admin zips the .app file so you can cache and install it using policies.

Open Jamf Admin and authenticate to the Jamf Pro server.

Drag the .app file to the main repository in Jamf Admin. The .app file is displayed in blue text in the Unknown category until you add it to a category.

Double-click the package in the main repository.

Click the General tab and choose a category for the package.

Click OK .

Adding the .app File for macOS to Composer.

Composer packages the .app file so you can cache and install it using policies.

Open Composer and authenticate locally.

Drag the .app file into the sources section of the sidebar in Composer.

Note: The file path reflected in Composer is where the package will install on target computers.

Select the .app file from the Sources list in the sidebar.

In the toolbar, click Build as PKG .

Note: If the Build flat PKGs preference is enabled and the package source contains scripts that are not supported by flat PKGs, a dialog will appear. To disable this preference for this package only, click Build as non-flat PKG . To build a flat PKG that ignores unsupported scripts, click Build as flat PKG . For more information on which scripts are supported by flat PKGs, see Adding Scripts to Package Sources in the Composer User Guide .

Select the principal distribution point in Jamf Pro, and then click Save .

Step 2: Create a Smart Computer Group to Identify Eligible Computers.

Create a smart computer group to identify computers that can be upgraded.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Smart Computer Groups .

Click New .

Use the Computer Group pane to configure basic settings for the group. To enable email notifications, select the Send email notification on membership change checkbox.

Click the Criteria tab and add criteria to the group:

Note: These are the minimum recommendations, consider adding other criteria to your smart computer group.

Click Add .

Click Choose for the "Operating System Version".

Note: Only your 30 most frequently used criteria are listed. To display additional criteria, click Show Advanced Criteria .

Choose an operator from the Operator pop-up menu.

Enter the macOS version you want to upgrade in the Value field, or browse for a macOS version by clicking Browse .

(Optional) Repeat steps a through d to create a range of macOS versions to upgrade.

Choose "and" from the And/Or pop-up menus to specify the relationships between criteria.

To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.

Click Save . Operations in the group take place in the order they are listed (top to bottom). Group memberships are updated each time computers check in with Jamf Pro and meet or fail to meet the specified criteria.

To view the eligible computers, click View .

Step 3: Cache the macOS Installer Package Using a Policy.

After adding the .app file to Jamf Admin or Composer, you can cache the file using a policy. Caching the file ahead of time speeds up the upgrade process.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Policies .

Click New .

In the General payload, enter a display name for the policy.

Select Recurring Check-in as the trigger.

Choose “Once per Computer” from the Execution Frequency pop-up menu.

Select the Packages payload and click Configure .

Click Add for the macOS installer package file.

Choose “Cache” from the Action pop-up menu.

Specify a distribution point for computers to download the package from.

Select the Maintenance payload and click Configure .

Ensure that the Update Inventory checkbox is selected.

Click the Scope tab and configure the scope of the policy. You can add the previously created smart group of eligible computers as the scope. For more information, see Scope in the Jamf Pro Administrator's Guide .

Click Save .

The macOS installer package file is cached on computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload.

Step 4: Create a Smart Computer Group with the Cached macOS Installer Package.

Create a smart group of computers with the macOS installer package file cached. The smart group will be used as the scope of the policy for installing the macOS upgrade automatically or for allowing users to download the upgrade via Self Service.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Smart Computer Groups .

Click New .

On the Computer Group pane, enter a display name for the smart computer group.

Click the Criteria tab.

Click Add .

Click Choose for “Cached Packages”.

Note: Only your 30 most frequently used criteria are listed. To display additional criteria, click Show Advanced Criteria .

Choose “has” from the Operator pop-up menu.

Click Browse .

Click Choose for the macOS installer package file.

Note: The macOS installer package file is not available as a value until it has been cached on at least one computer.

Click Save .

Step 5: Create a Policy for Upgrading macOS.

After caching the macOS installer package file, you can create a policy that allows users to upgrade macOS through Self Service, or that upgrades macOS on computers in the scope automatically.

Creating a Self Service Policy for Upgrading macOS.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Policies .

Click New .

In the General payload, enter a display name for the policy. For example, “Upgrade macOS”.

Choose “Once per Computer” from the Execution Frequency pop-up menu.

Select the Packages payload and click Configure .

Click Add for the macOS installer package file.

Choose “Install Cached” from the Action pop-up menu.

(Optional) To use a script to install macOS, use the Scripts payload to add the script and configure the settings. For information, see Managing Scripts and Running Scripts in the Jamf Pro Administrator's Guide .

Note: You can also use Jamf Helper to add additional end-user messaging.

Select the Files and Processes payload and click Configure .

In the Execute Command field, enter the file path to the installer with the --startosinstall command. For example, " /file/path/Install macOS High Sierra.app/Contents/Resources/startosinstall ".

(Optional) To erase data while installing macOS, add the --eraseinstall flag to the command.

(Optional) To suppress end-user messages during installation, add the --agreetolicense flag to the command.

Click the Scope tab.

Click Add .

Click the Computer Groups tab.

Click Add for the smart computer group with the cached macOS installer package file you just created.

Click the Self Service tab.

Select Make the policy available in Self Service .

Configure how the policy is displayed in Self Service using the settings on the pane.

Click Save .

The policy is made available in Self Service on computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload. macOS is upgraded when users run the policy from Self Service.

Upgrading FileVault 2-enabled drives from macOS 10.7 or 10.8 prompts users to enter their password after reboot. Upgrading FileVault 2-enabled drives from macOS 10.9 or later automatically bypasses authentication after reboot.

Creating a Policy for Upgrading macOS Automatically.

Log in to Jamf Pro.

Click Computers at the top of the page.

Click Policies .

Click New .

In the General payload, enter a display name for the policy. For example, “Upgrade macOS”.

Choose “Once per Computer” from the Execution Frequency pop-up menu.

Select the Packages payload and click Configure .

Click Add for the macOS installer package file.

Choose “Install Cached” from the Action pop-up menu.

(Optional) To use a script to install macOS, use the Scripts payload to add the script and configure the settings. For information, see Managing Scripts and Running Scripts in the Jamf Pro Administrator's Guide .

Select the Files and Processes payload and click Configure .

In the Execute Command field, enter the file path to the installer with the --startosinstall command. For example, " /file/path/Install macOS High Sierra.app/Contents/Resources/startosinstall "

(Optional) To erase data while installing macOS, add the --eraseinstall flag to the command.

(Optional) To suppress user messages while installing macOS, add the --agreetolicense flag to the command.

Click the Scope tab.

Click Add .

Click the Computer Groups tab.

Click Add for the smart computer group with the cached macOS installer package file you just created.

(Optional) Click the User Interaction tab and enter messages to display to users or allow users to defer the policy. For more information, see User Interaction with Policies in the Jamf Pro Administrator's Guide .

Click Save . The upgrade installs on computers in the smart group depending on the trigger configured in the policy.

Jamf Pro - Restricting upgrades to macOS.

There are two ways to restrict OS updates on Macs with Jamf Pro: via Configuration Profiles, and via Restricted Software entries. The configuration profile will allow you to hide updates from end users for up to 90 days after release, while the restricted software entry will automatically quit the installer app if a user tries to launch it. It is recommended to use the configuration profile, but if you need to restrict upgrades for more than 90 days you should also make a Restricted Software entry.

Configuration Profile setup.

Go the Configuration Profiles section of Jamf Pro and click New. In the Restrictions payload on the left, click Configure. Under the Functionality tab, scroll down and check the "Defer updates" box. Set the the menu options to "Software Updates" and "90 days" (or less if you prefer). Click on the Scope tab, and select the computers, groups, or users you want this restriction to apply to. Save.

The configuration profile should be installed and take effect as soon as the target computers are connected to the Internet.

Restricted Software.

Go to the Restricted Software section and click New. Depending on your OS you can enter the following: In the "Process Name" field, enter e.g. " Install macOS Big Sur.app " or " Install macOS Catalina.app " Check the "kill process" box. Add a message to display to the end user if they try to launch the macOS installer. Click on the Scope tab, and select the computers, groups, or users you want this restriction to apply to. Save.

Software restrictions should take effect on computers after their next check in, which normally happens about once every half hour.

When a user tries to run the macOS installer, it will quit instantly and the user will see the message you specified.

My friend installed something called Jamf on my MacBook.

I have a MacBook Air 7,2. My friend installed something called Jamf on it. Now I can't access most of my applications. My son said he couldn't force quit it so I'm thinking it must be some kind of virus.

The IT man managed to get it up on Activity Monitor, but when he tried to force quit it, it just reopened and when he tried to uninstall it with terminal it just blocked terminal.

Any help that could be offered would be appreciated because otherwise, I may need to just throw out the MacBook and buy a new one.

4 Answers 4.

Jamf is a device management/mobile device management solution. It enables remote control and management of the configured device.

Due to the nature of the software, it can restrict users of the machine (even the admin users) from performing certain administrative operations (depending on the applied configuration). It is thus obvious that the end-users cannot uninstall and/or quit the Jamf app.

Jamf is one of the well-known among many remote/mobile device management solutions, generally used in enterprise/school environment to centrally manage a large number of mobile devices (laptops/tablets/phones). Jamf is absolutely not a virus , nor is it a ransomware.

You can learn more about Jamf product offerings here:

There is absolutely no reason to throw away your MacBook. I'd advise you to get in touch with your friend and ask him for the reason why it was installed in first place. You can also ask to remove it, if it was installed in accident, or just out of curiosity.

A mobile device management solution is generally not required for personal devices.