Manage Background Tasks with Jamf Pro

Contents

Preface

To follow along with this guide you will need the following:

- A Mac running macOS 13.0 or later enrolled in your Jamf Pro server.
- Administrative access to your Jamf Pro Server version 10.42 or later
- A code signing certificate. If you don't have one, this guide will show you how to create one using your Jamf Pro server.
- iMazing Profile Editor: https://imazing.com/profile-editor
- Dropbox Installer: https://www.dropbox.com/downloading
- Zoom Installer: https://zoom.us/support/download?os=mac

What are login and background tasks and why would you want to manage them?

Launch daemons, launch agents, and startup items are helper executables that macOS starts on behalf of the user that extend the capabilities of apps or provide additional capabilities to users. For example, a LaunchDaemon can provide persistent background service for an app, a LaunchAgent can provide auxiliary UI capabilities like menu bar extras, and a Login Item can provide the ability to auto-mount remote directories or launch applications when the user logs in.

Prior to macOS 13, part of the application-design process of helper executables included scripts that installed one or more property lists into specific directories based on the type of service, such as the following locations of property lists:

- $HOME/Library/LaunchAgents
- /Library/LaunchAgents
- /Library/LaunchDaemons

In macOS 13 and later, a new structure in the app bundle simplifies the installation of these login items and associated property lists. This new structure allows you to keep helper app resources inside the app's bundle, which reduces the need for specialized installation scripts or permission to write files into system directories. The SMAppService object is used to control helper executables that live inside an app's main bundle. It can also be used to register and control LoginItems, LaunchAgents, and LaunchDaemons as helper executables for an app and it works with any type of app regardless of how it was installed. Managing these items with a mobile device management (MDM) server allows organizations to keep login and background items enabled so users cannot disable them.

Section 1: Prepare your Mac

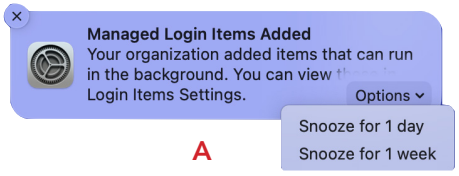
In this section we will prepare your Mac with the items needed to follow along with this guide. To follow along with this guide you will need the following:

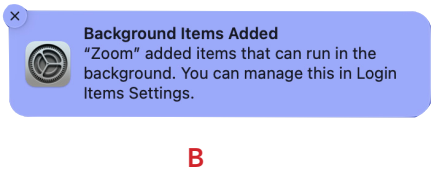
- A Mac running macOS 13.0 or later enrolled in your Jamf Pro server.
- Administrative access to your Jamf Pro Server version 10.42 or later
- A code signing certificate. If you don't have one, this guide will show you how to create one using your Jamf Pro server.
- iMazing Profile Editor: https://imazing.com/profile-editor
- Dropbox Installer: https://www.dropbox.com/downloading
- Zoom Installer: https://zoom.us/support/download?os=mac

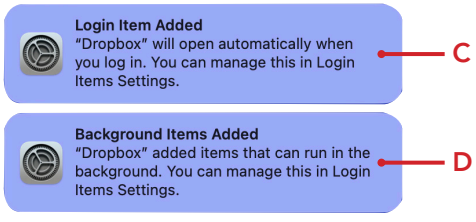
1. Install the following Applications and accept all the default prompts.
   - Dropbox
   - iMazing Profile Editor
   - Zoom

2. You will receive notifications when installing the applications.
   A. The Managed Login Items Added notification will appear when you enroll your Mac into your Jamf Pro Server
   B. The Background Items Added notification is presented once you install Zoom.
   C. The Login Item Added notification is presented when you install Dropbox.
   D. The Background Items Added notification is presented when you install Dropbox.

NOTE: If a notification has an Options dropdown menu, you can select to snooze the notifications for a duration of one day or one week. You can stop these notifications by creating a notifications profile and disabling Notifications and Critical Alerts for the bundle ID com.apple.btmnotificationagent. This will be covered this in section 5 of this guide.

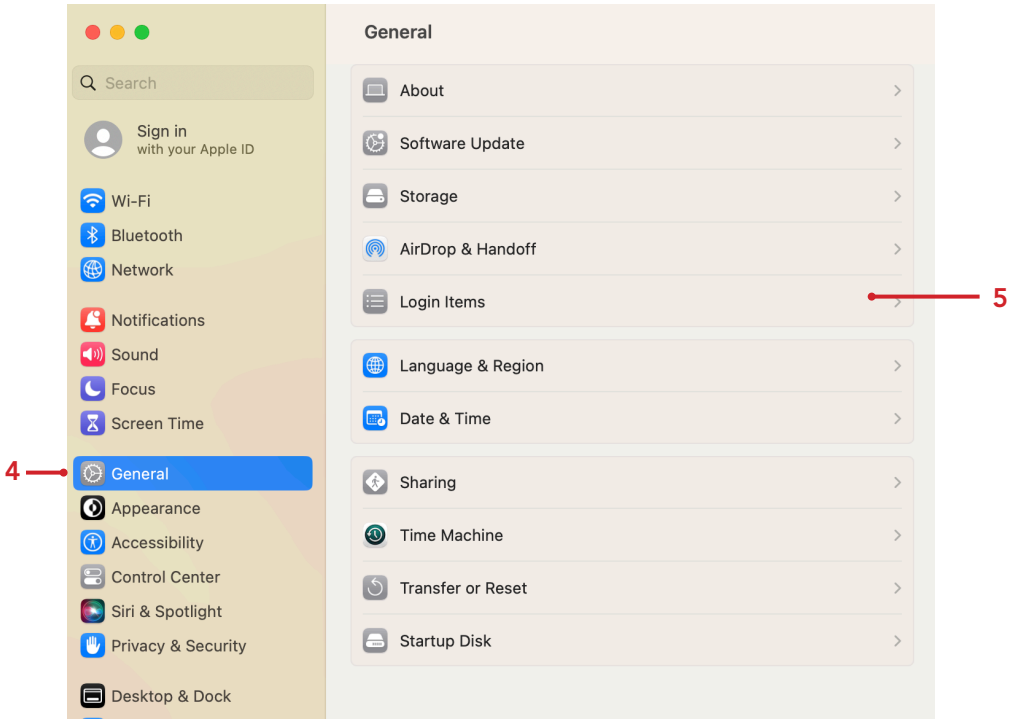






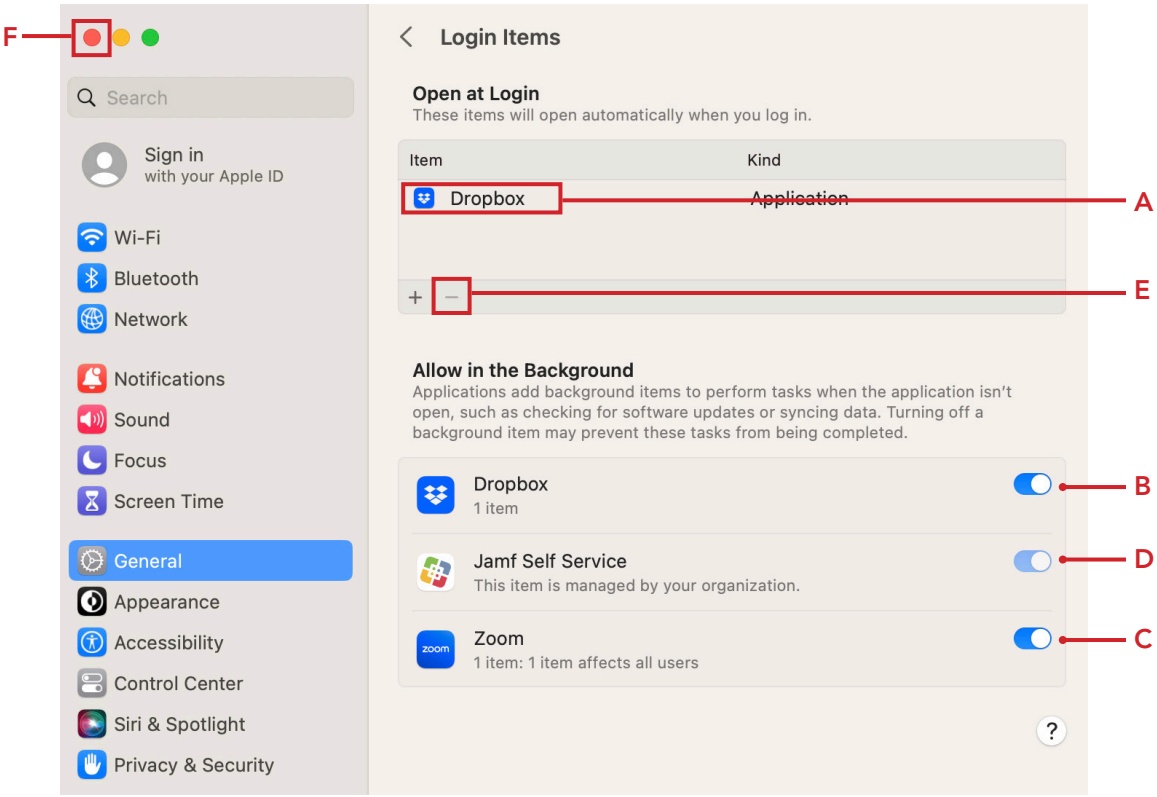
3. Open System Settings

4. Click General.
5. Click Login Items.



5. Confirm the following:
   A. Login Item for Dropbox was added during the installation.
   B. A background process was added for Dropbox.
   C. A background process was added for Zoom. The background processes for Dropbox and Zoom can be disabled by toggling the switch to off. This requires administrative credentials.
   D. A background process was added for Jamf Self Service. The background process for Jamf Self Service cannot be toggled off. This is being managed by the Jamf Pro server and was added automatically by Jamf during computer enrollment.
   E. The Dropbox Login item can be removed by clicking Remove (-).
   F. Close System Settings.

   NOTE: All of these items can be managed by Jamf Pro with a configuration profile. This will remove the ability to disable Login and Background items by an administrative user.



In the next section, we will create a signing certificate using your Jamf Pro server. If you already have a signing certificate you can skip the next section.

This completes this section.

Section 2: Creating a code signing certificate using Jamf Pro's CA

This section will cover creating a code signing certificate using your Jamf Pro server.

Requirements for following along with this section:

- A Mac running macOS 13.0 or later enrolled in your Jamf Pro server.
- Administrative access to your Jamf Pro server version 10.42.

Why do we need a code signing certificate?
Signing a configuration profile ensures all the information will stay in place when uploaded to the Jamf Pro server. There are times when older versions of Jamf Pro do not understand newer payloads introduced in later versions of Jamf Pro. In Jamf Pro 10.42.0 or later, you can create a configuration profile using the com.apple.servicemanagement payload for Managed Login Items to prevent end users from disabling certain background services of apps that are installed in your environment by uploading a configuration profile. Failure to sign the profile will result in missing data on earlier versions of Jamf Pro server prior to 10.42 as the Jamf Pro server will disregard information that is does not understand. In order to sign a configuration profile you need a signing certificate.

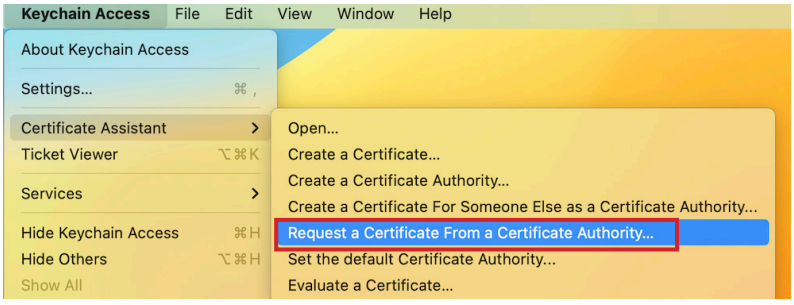
When creating a code signing certificate using your Jamf Pro server, make sure to follow the steps in this section on a Mac that is enrolled in Jamf Pro. Failure to do so will result in a code signing certificate that is not trusted.

NOTE: As of Jamf Pro version 10.42, signing your configuration profile to manage Login and Background items is NOT required. However, to avoid any unforeseen issues when uploading the profile to your Jamf Pro server, we recommend signing the configuration profile before uploading. Jamf currently does not have a way for you to edit the configuration profile in place as of version 10.42. That feature will be included in a later version of Jamf Pro. If you have your own signing certificate, feel free to use that and skip this section of the guide.

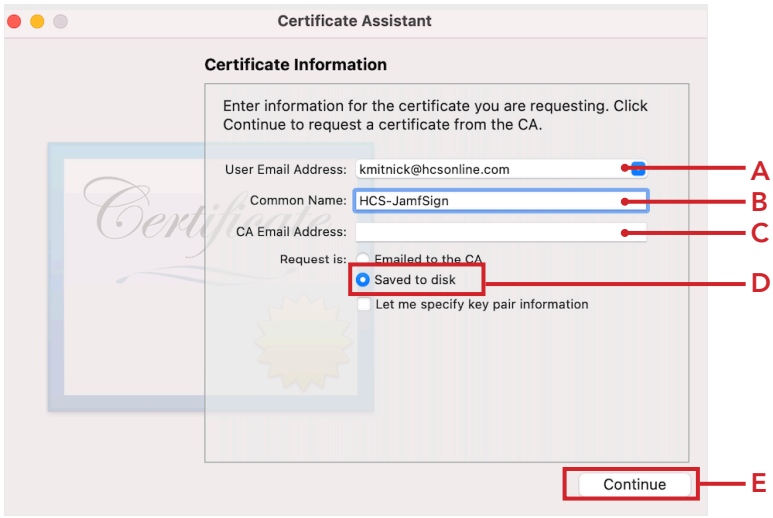
1. Open Keychain Access located in /Applications/Utilities.

Keychain Access

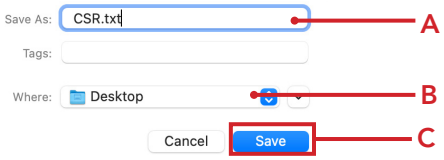
2. Select Keychain Access > Certificate Assistant > Request a Certificate From a Certificate Authority.



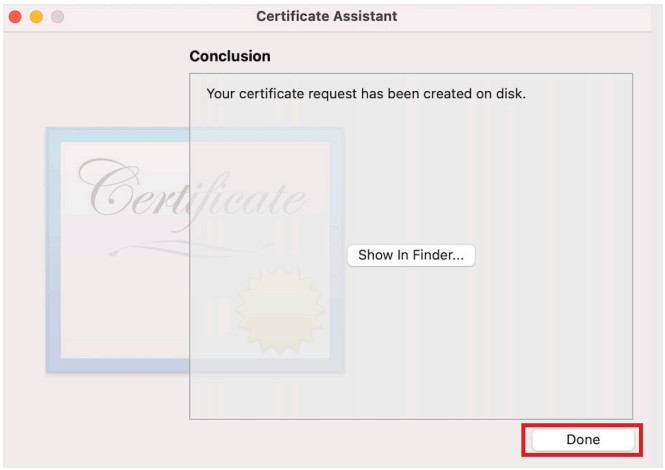
3. Configure the following:
   A. User Email Address: Enter your email address
   B. Common Name: Enter a name of your choosing. This guide will use HCS-JamfSign
   C. CA Email Address: Leave this blank.
   D. Request is: Select the radio button for Saved to Disk.
   E. Click Continue.



4. Configure the following:
   A. Save as: CSR.txt
   B. Where: Desktop
   C. Click Save



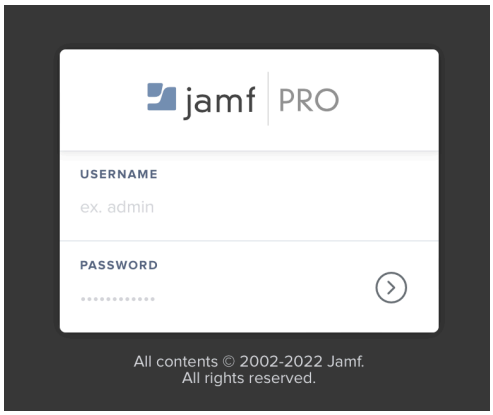
5. Click Done.



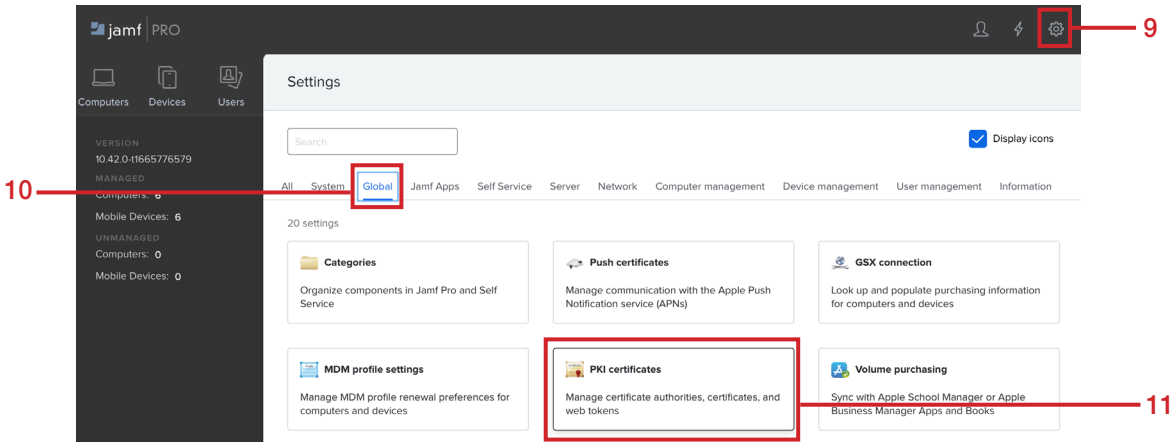
6. Open the CSR.txt file on your desktop with a text editor of your choice.

7. Copy the entire CSR text.

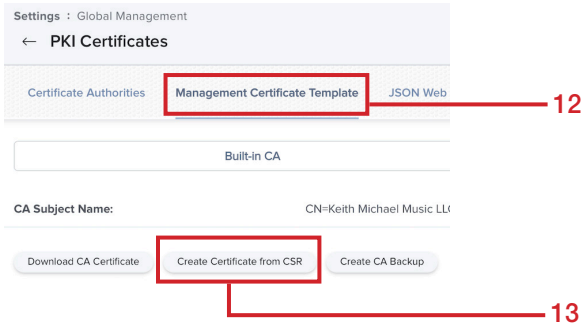
8. Log into your Jamf Pro Server.



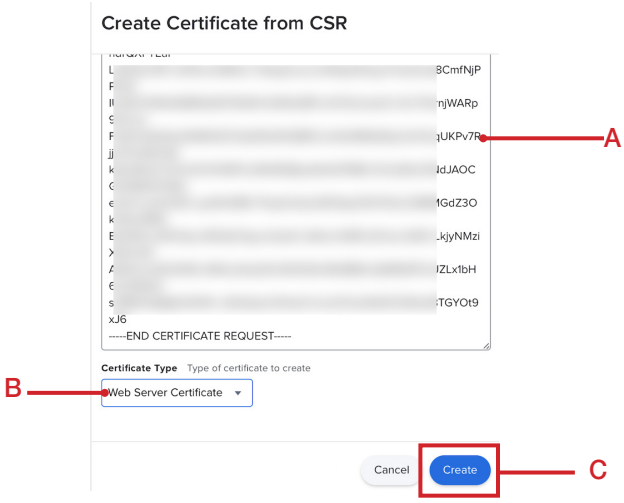
9. Click Settings (⚙) in the upper-right corner.
10. Click Global.
11. Click PKI Certificates.



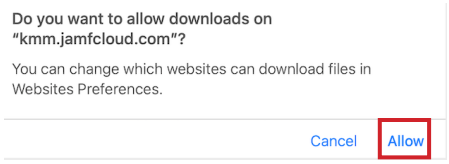
12. Click Management Certificate Template
13. Click Create Certificate from CSR.



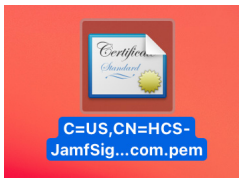
14. Configure the following:
    A. Paste in the CSR text that you copied in step 7.
    B. Certificate Type: Web Server Certificate
    C. Click Create.



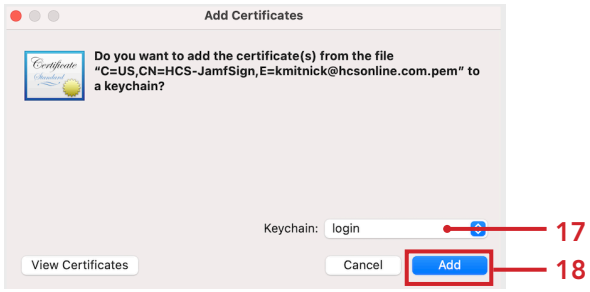
15. Click Allow.
    NOTE: After downloading the file your web browser may need to be refreshed to properly display things in Jamf Pro.



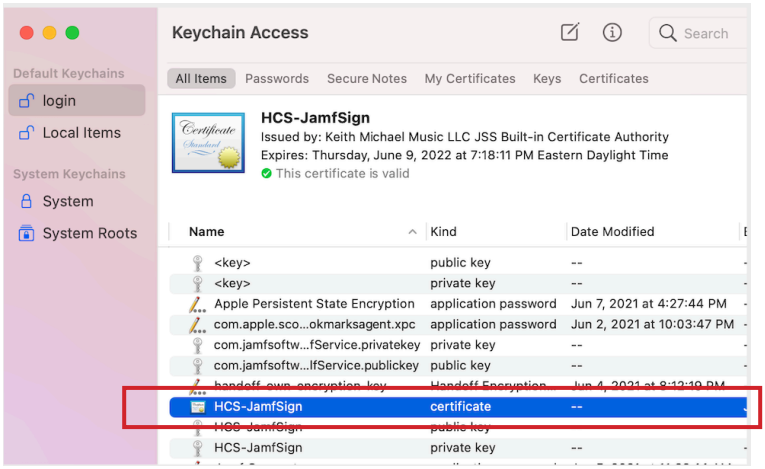
16. The certificate will download to your Downloads folder. Drag the certificate to your Desktop and double-click to open the file.



17. From the Keychain menu, select login.
18. Click Add.

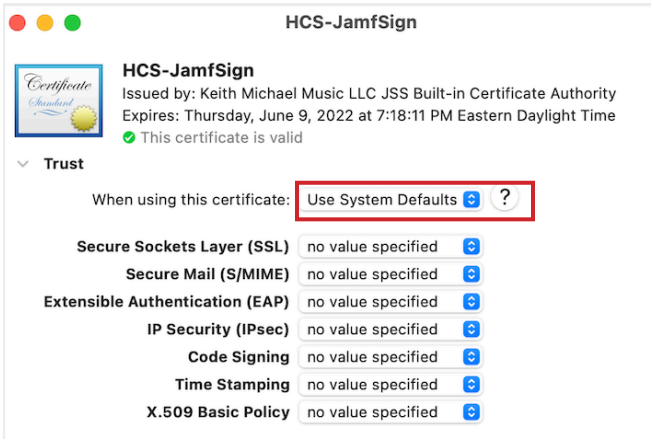


19. In Keychain Access Click your login keychain, you will see the certificate on the right side. Double click on your certificate to see more settings.

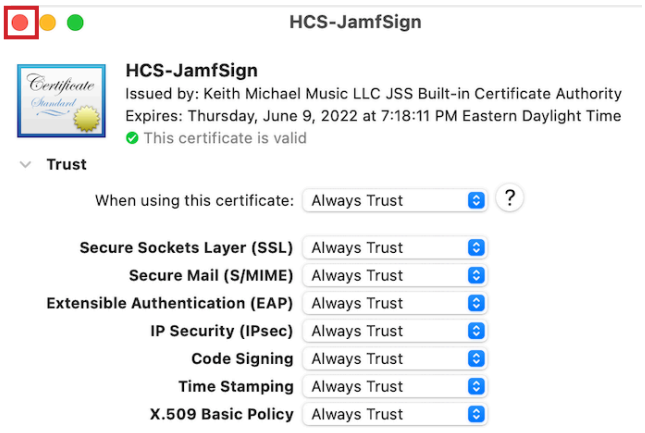


20. Expand (>) Trust to view the settings.

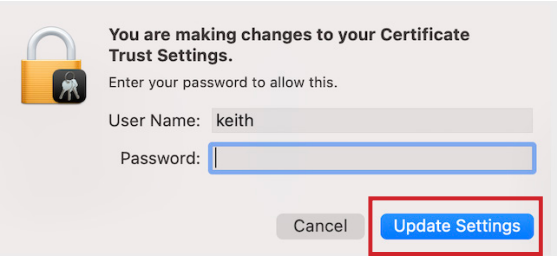
21. On the first item, When using this certificate section, click the menu and select Always Trust.



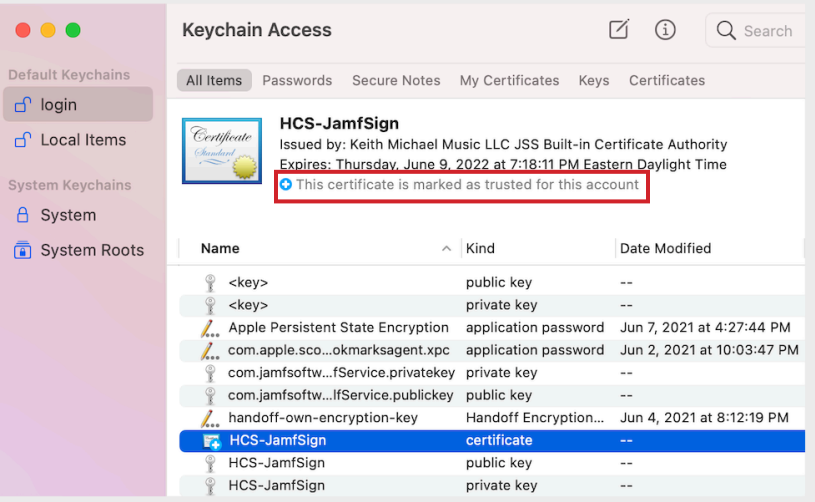
22. Close the window.



23. Enter your admin credentials and click Update Settings.



24. Confirm the certificate shows up as trusted. Quit Keychain Access.



In the next section, we will create a configuration profile to manage Login and Background items using the iMazing Profile Editor application.

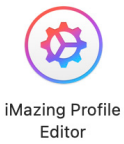
This completes this section.

Section 3: Create a Configuration Profile to Manage Login and Background Items

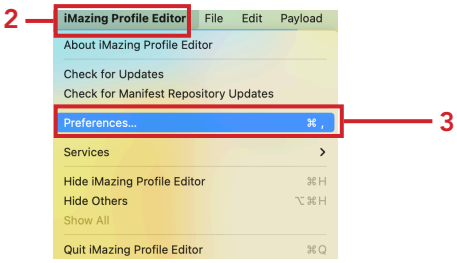
In this section we will create a configuration profile using iMazing Profile Editor. This configuration profile will allow you to manage Login and Background items. To follow along with this guide you will need the following:

- A Mac running macOS 13.0 or later enrolled in your Jamf Pro server version 10.42 or later.
- Administrative access to your Jamf Pro Server 10.42 or later.
- A code signing certificate. If you don't have one, refer to section 2 of this guide to create one.
- iMazing Profile Editor - Installed in section 1 of this guide.
- Dropbox and Zoom - Installed in section 1 of this guide.

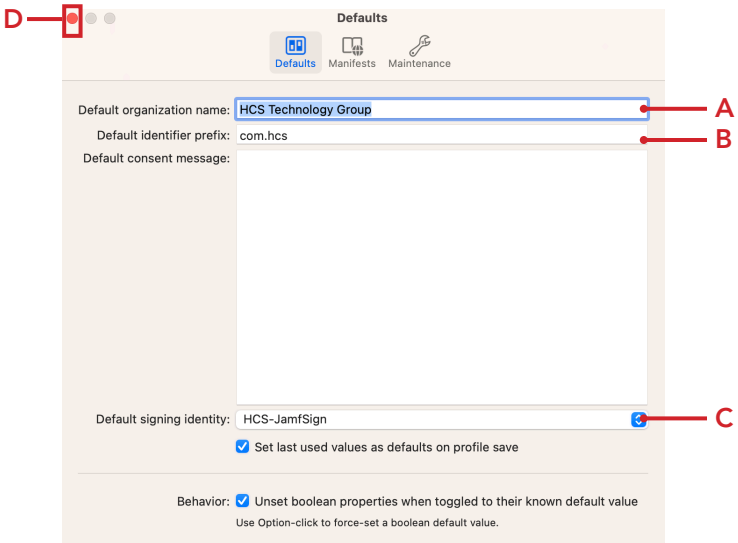
1. Go to your Applications folder and open iMazing Profile Editor.



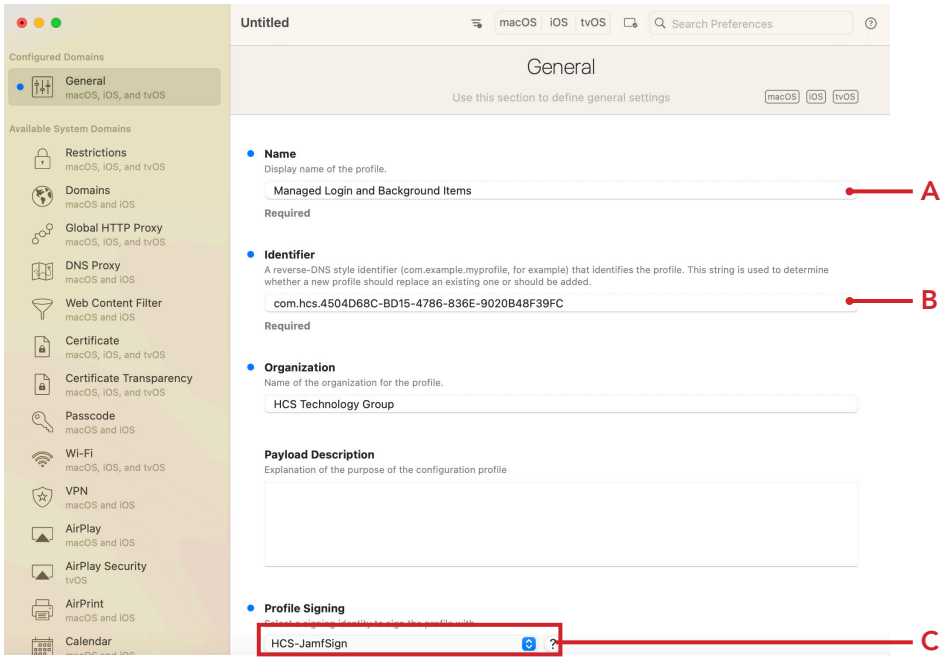
2. Click the iMazing Profile Editor menu
3. Select Preferences.



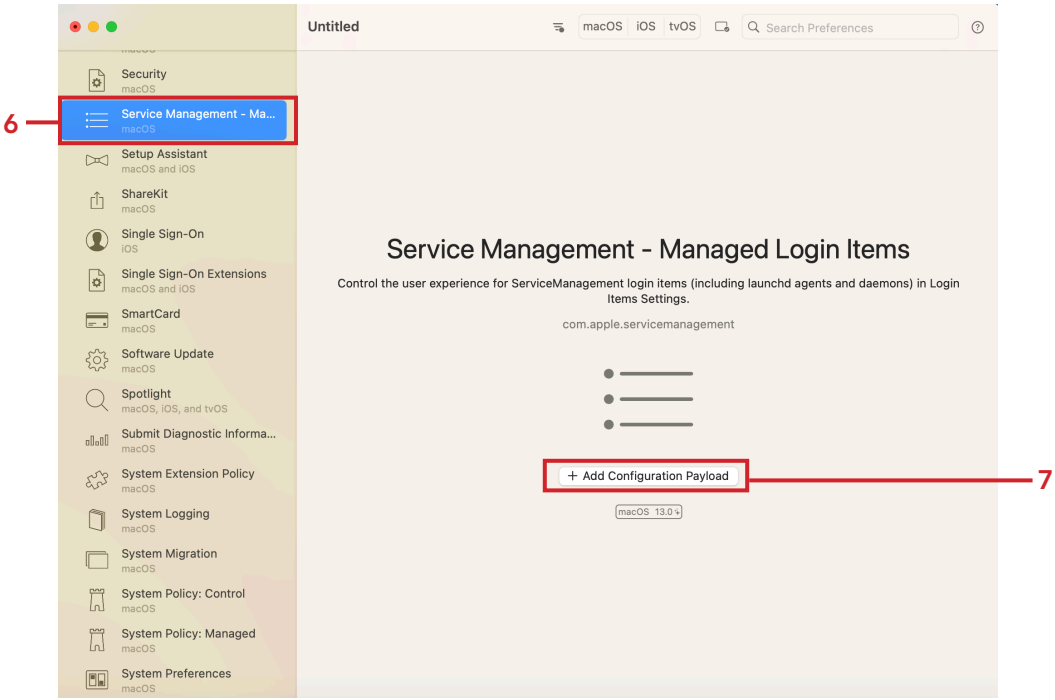
4. Enter the following:
   A. Default organization name: Enter your organization name. This guide will use HCS Technology Group
   B. Default identifier prefix: This will use a reverse DNS nomenclature. This guide will use com.hcs
   C. Default signing identity: Select your signing certificate. This guide will use HCS-JamfSign
   D. Close the window when done.
   E. Quit the iMazing Profile Editor application and re open it. This will allow us to use the new settings.



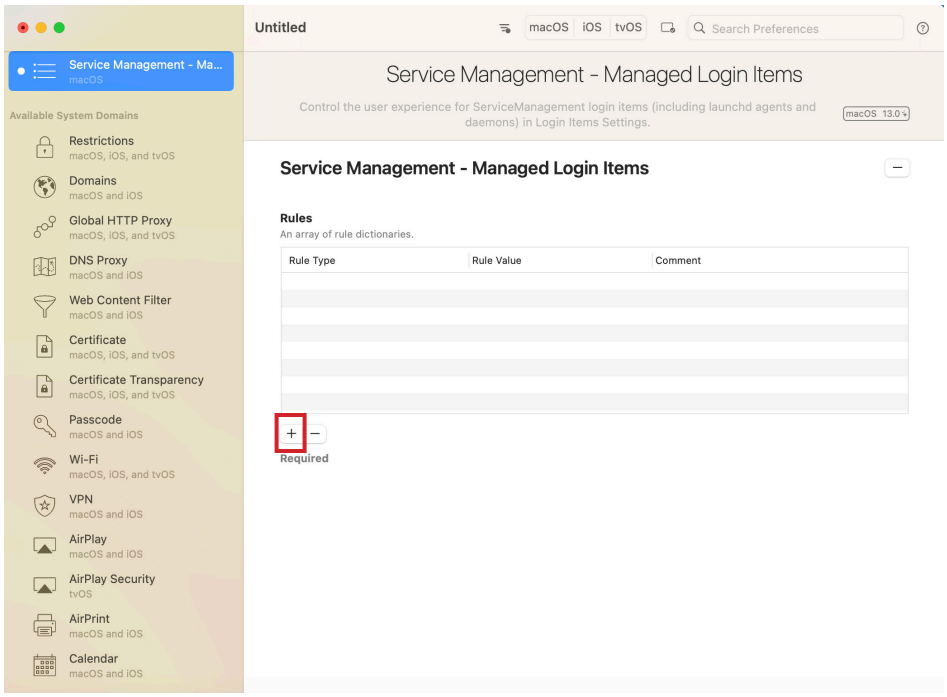
5. Select the General payload then enter the following:
   A. Name: Managed Login and Background Items
   B. Notice the Identifier and Organization are now configured with the settings we entered in step 4.
   C. Profile Signing: Select your signing certificate. This guide will use HCS-JamfSign



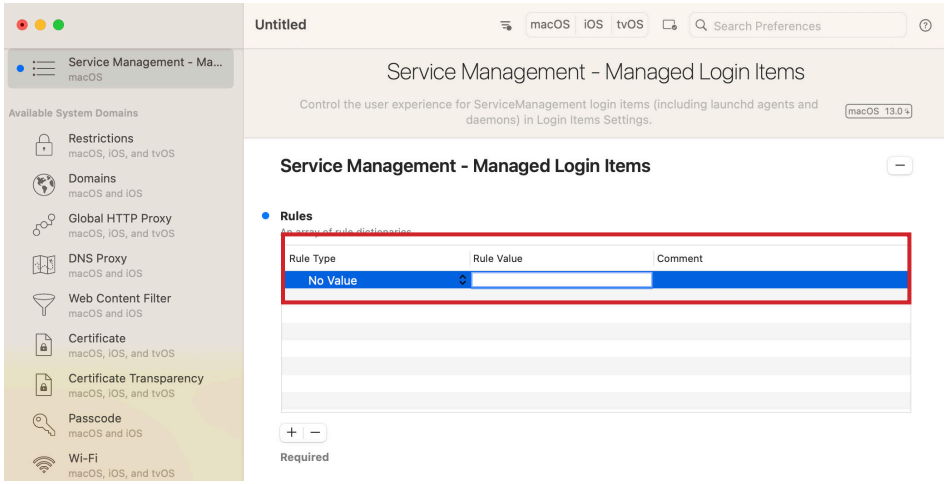
6. Click Service Management - Managed Login Items Payload
7. Click Add Configuration Payload.



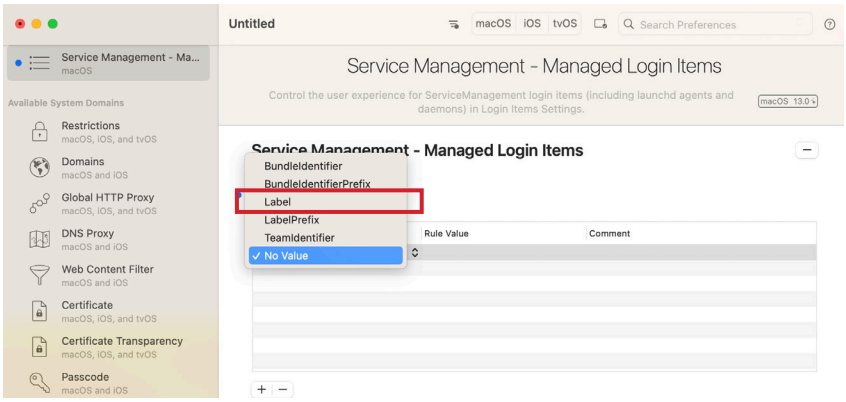
8. Click Add (+) to add a new Rule.



9. Confirm the following fields: Rule Type, Rule Value, Rule Comment



10. Select the Rule Type menu. There are five types of rules:
    A. BundleIdentifier: The bundle identifier of the app to match, which must be an exact match.
    B. BundleIdentifierPrefix: The prefix of the bundle identifier of the app to match.
    C. Label: The value of the launchd plist Label parameter to match, which must be an exact match.
    D. LabelPrefix: The prefix of the launchd plist Label parameter to match.
    E. TeamIdentifier: The team identifier from the code signing attributes, which must be an exact match.
11. Select Label from the menu.
    NOTE: Only use a LabelPrefix if it's absolutely necessary as it can cause malicious software to leverage an existing LabelPrefix. For example, if you use a LabelPrefix for com.apple, anything that uses that prefix will be trusted. I.E. com.apple.maliciousSoftware.

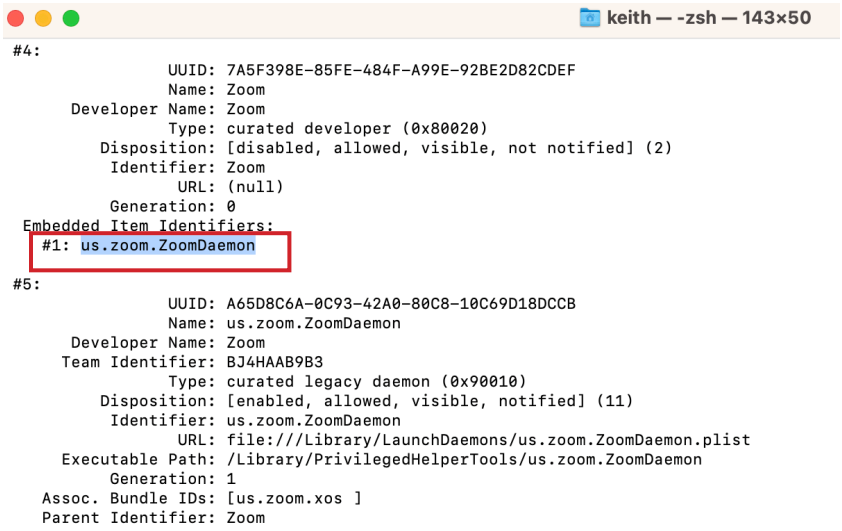


12. Open Terminal from /Applications/Utilities.

Terminal

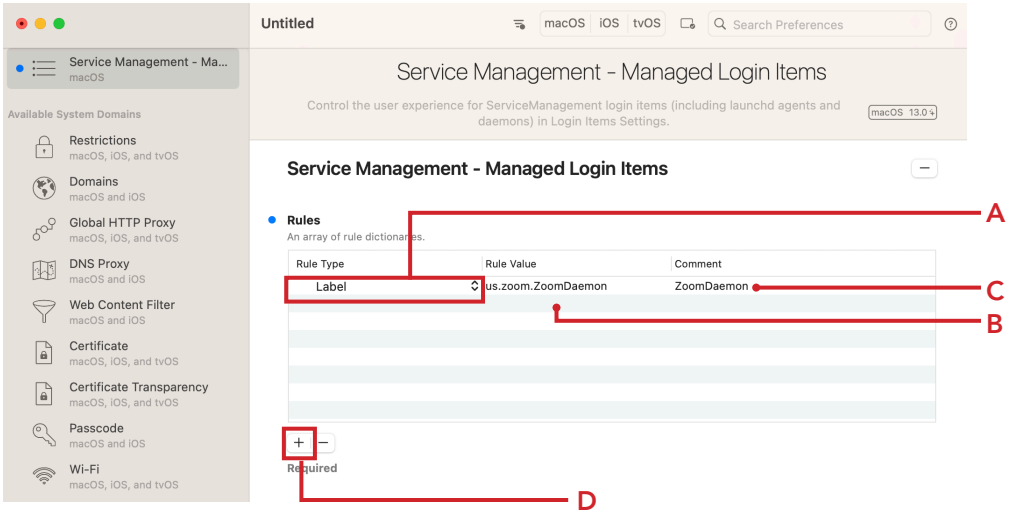
13. In order to find the information needed to set up the Rule Type and Rule Value, we can run the command below to print out a list of all currently added Login and Background items.
    A. Run this command: sudo sfltool dumpbtm
    B. Enter your administrative credentials.
    C. A list of all Login and Background items with their information is printed to the screen.

14. Scroll down the list until you find us.zoom.ZoomDaemon. Copy this info.



15. Switch back to the iMazing Profile Editor and enter the following:
    A. Rule Type: Label
    B. Rule Value: us.zoom.ZoomDaemon (this is case sensitive so enter as shown)
    C. Comment: Enter a description. This guide will use ZoomDaemon
    D. Click Add (+).

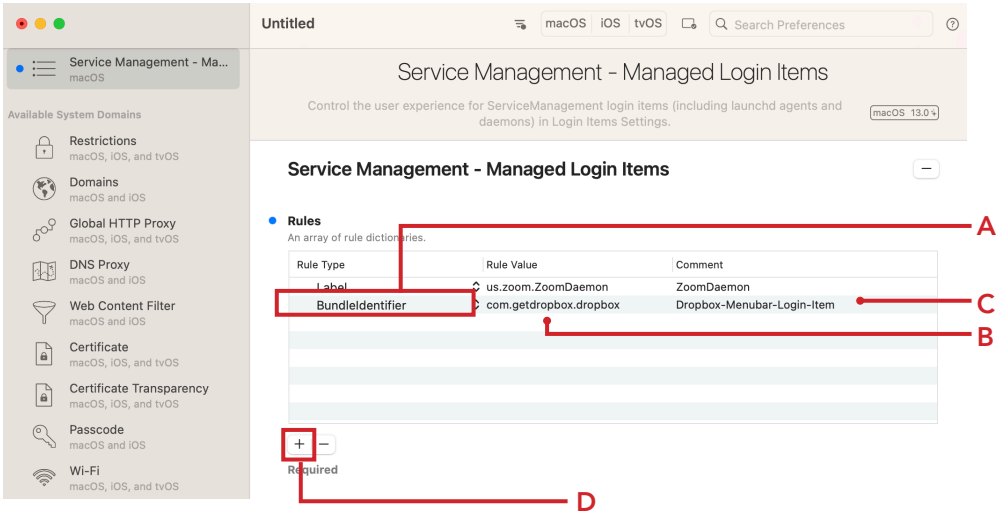
    NOTE: Zoom installs a daemon as a Background Item during the install. Using a Label Rule Type will allow you to manage it.



16. Scroll down the list until you find com.getdropbox.dropbox. Copy this info.

17. Switch back to the iMazing Profile Editor and enter the following:
    A. Rule Type: BundleIdentifier
    B. Rule Value: com.getdropbox.dropbox (this is case sensitive so enter as shown)
    C. Comment: Enter a description. This guide will use Dropbox-Menubar-Login-Item
    D. Click Add (+).

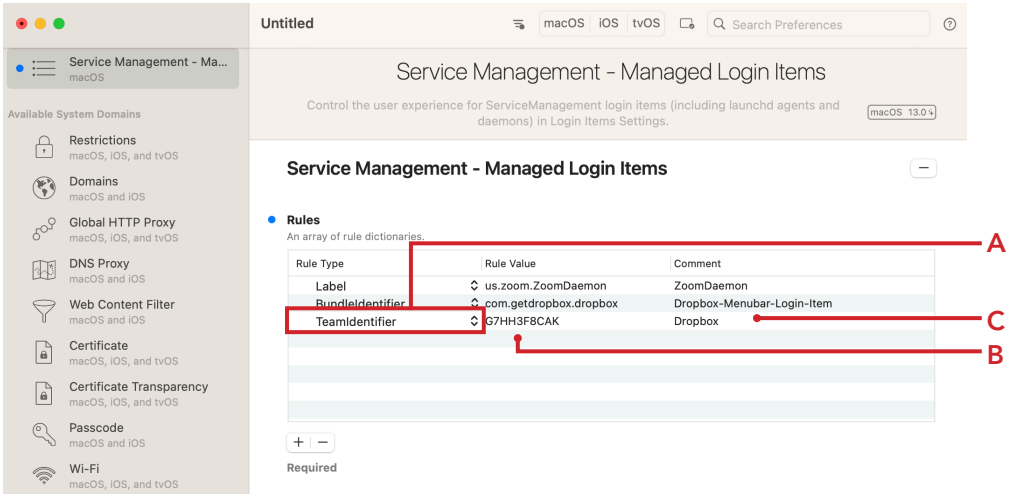
    NOTE: Dropbox installs a Login Item to launch it's Menu Bar item and also adds a Background Item during the install. Using a BundleIdentifier Rule Type will allow you to manage the login item.



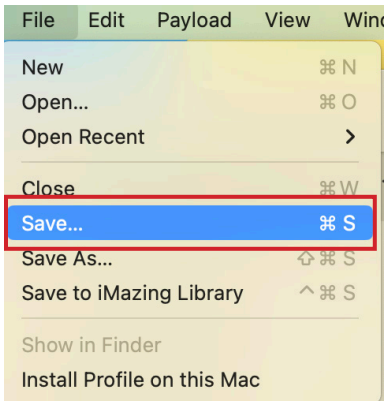
18. Scroll down the list until you find Team Identifier for zoom shown below. Copy this info.

19. Switch back to the iMazing Profile Editor and enter the following:
    A. Rule Type: TeamIdentifier
    B. Rule Value: G7HH3F8CAK (this is case sensitive so enter as shown)
    C. Comment: Enter a description. This guide will use Dropbox

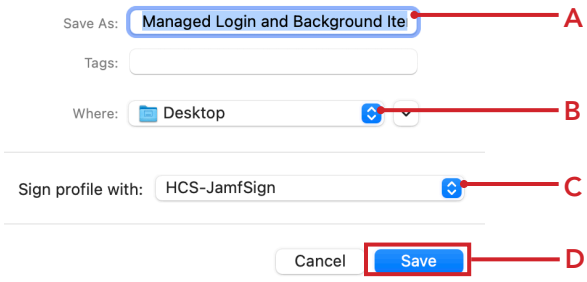
    NOTE: Dropbox installs a Background Item during the install. Using a TeamIdentifier Rule Type will allow you to manage it.



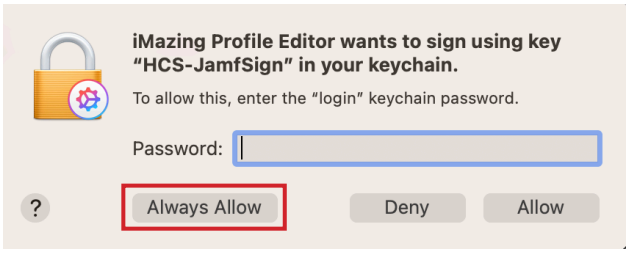
20. Save the Payload.



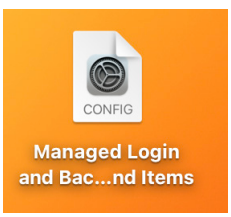
21. Enter the following:
    A. Save As: Managed Login and Background Items
    B. Where: Desktop
    C. Sign profile with: Select your signing certificate. This guide will use HCS-JamfSign
    D. Click Save



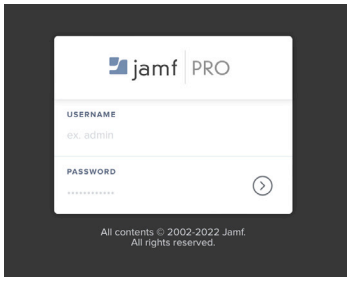
22. Enter your password at the message below and click Always Allow.



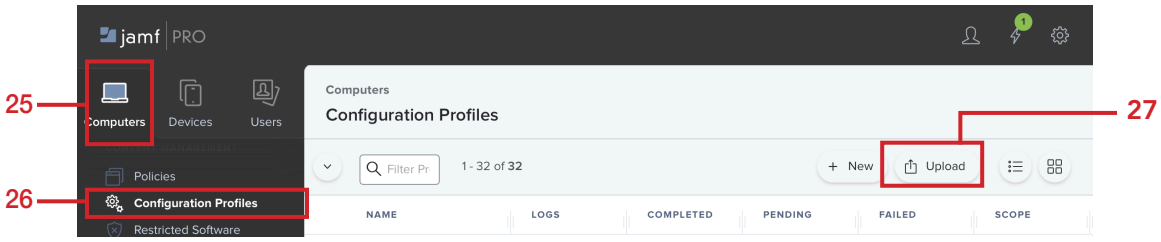
23. Confirm the file was saved to your Desktop.



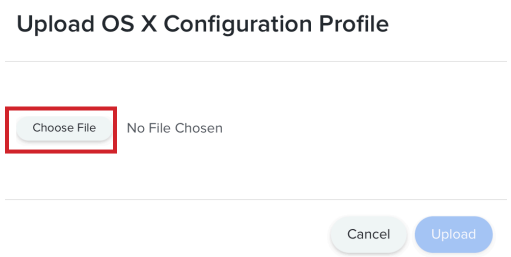
24. Log in to your Jamf Pro server with administrative credentials.



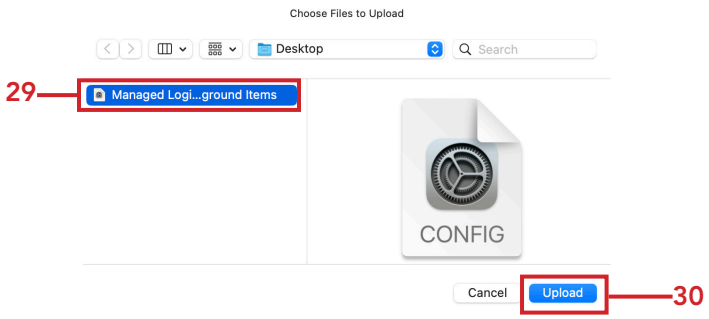
25. Click Computers
26. Click Configuration Profiles.
27. Click Uplaod.



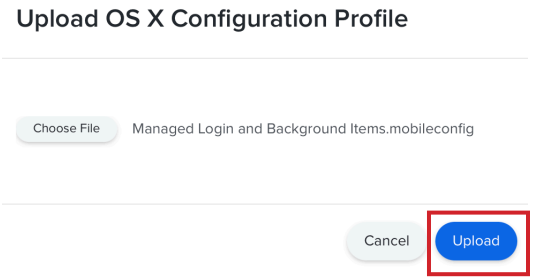
28. Click Choose File.



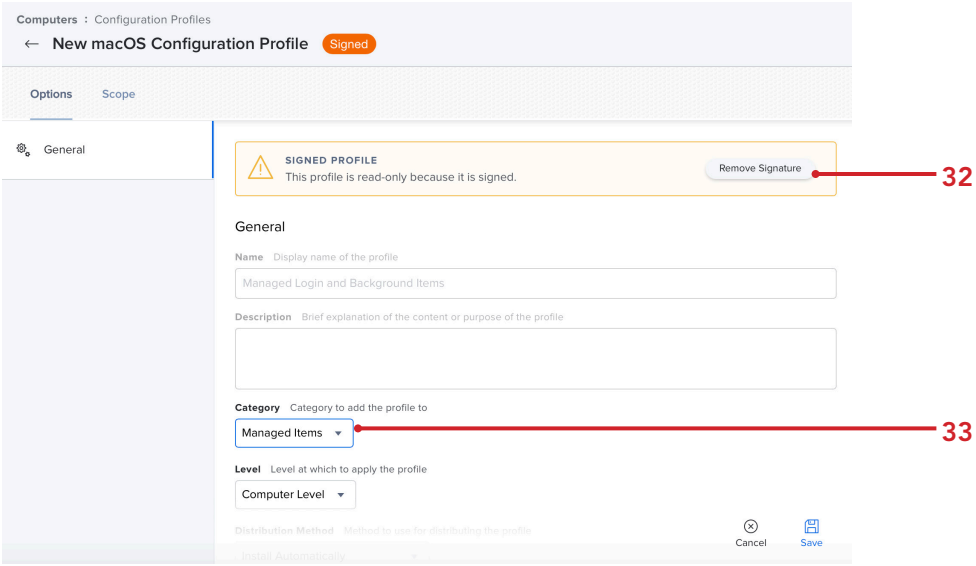
29. Navigate to the Desktop and select the Managed Login and Background Items configuration profile.
30. Click Upload.



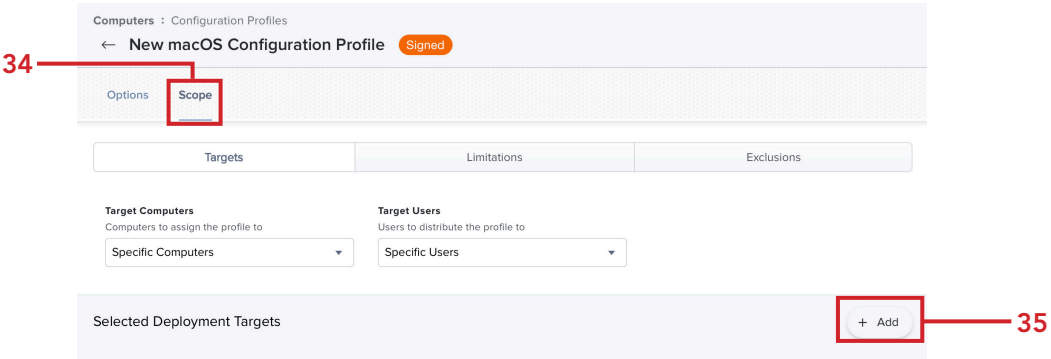
31. Click Upload.



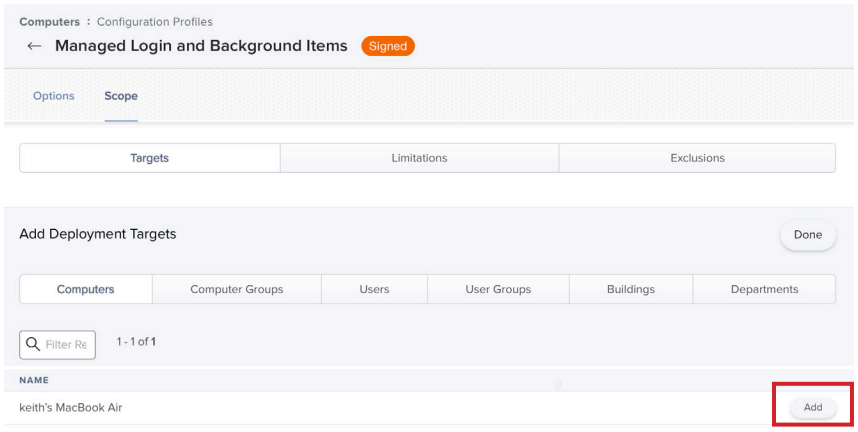
32. Notice the profile is signed.
33. Select a Category of your choosing. This guide will select Managed Items.



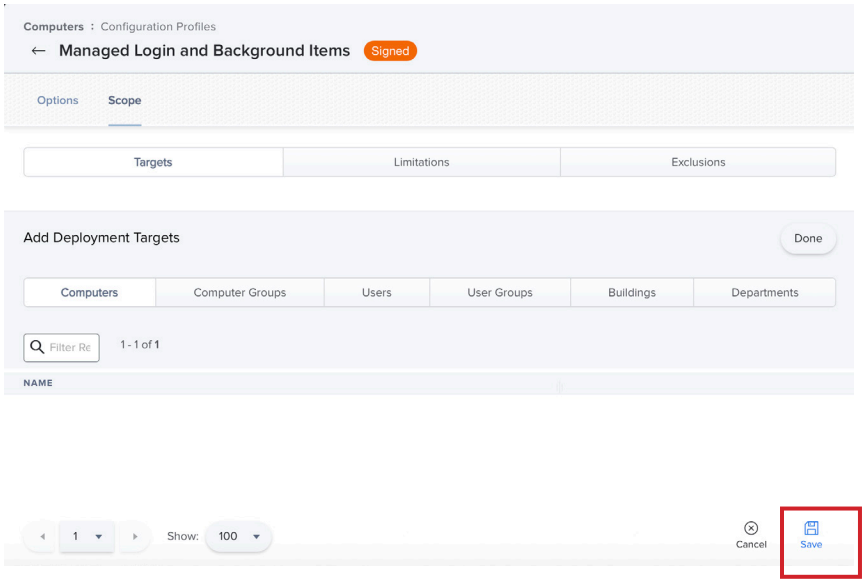
34. Click Scope.
35. Click Add.



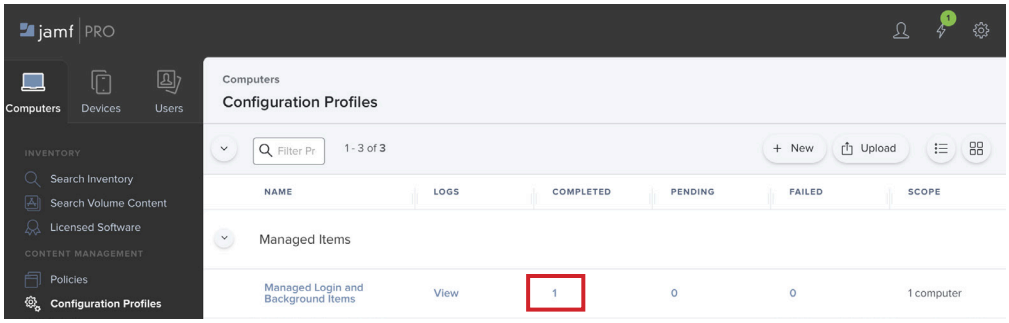
36. Add a Mac of your choosing by clicking Add.



37. Click Save.

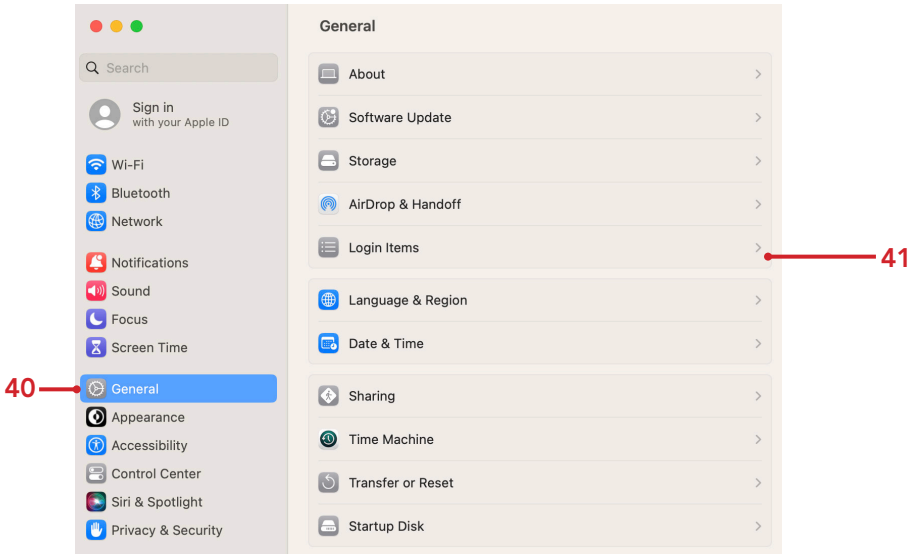


38. Confirm the configuration profile was deployed successfully.

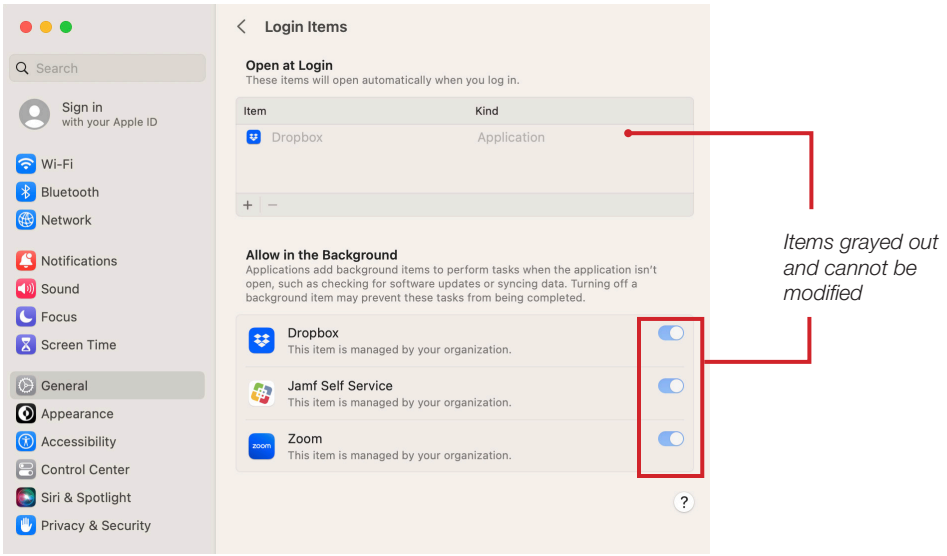


39. Open System Settings

40. Click General
41. Click Login Items.



42. Confirm the Login Item for Dropbox is now managed as well as all the Background Items. The toggle switch is greyed out and cannot be modified.



In the next section, we will go over some command line tools and other helpful files for viewing information related to Login and Background items.

This completes this section.

Section 4: Identifying Applications Using Login and Background Items

In this section we will discuss ways to identify applications that are using Login and Background items. To follow along with this section you will need the following:

- A Mac running macOS 13.0 or later enrolled in your Jamf Pro server version 10.42 or later.
- Administrative credentials on the Mac.

It's important to be aware of any items that use helper applications and executables that are deployed and registered with the SMAppService framework. There are command line tools that can assist with gathering pertinent information about Login and Background items.

Here are a list of helpful tools:

- Terminal
- Console
- attributions.plist

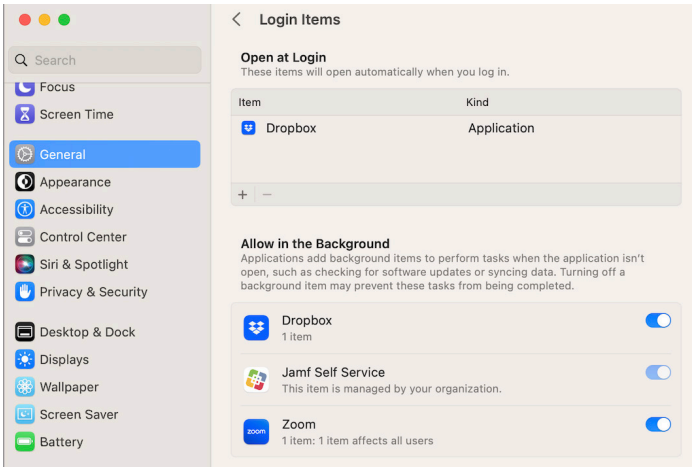
1. Open Terminal in /Applications/Utilities.

Terminal

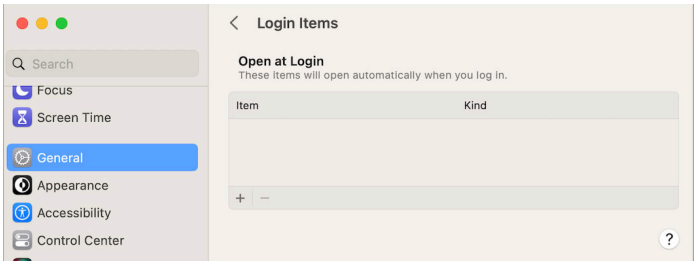
2. There are helpful Terminal commands to gather information on login and background items.
   A. **`sudo sfltool dumpbtm`** - Prints the current status of login and background items, including loaded servicemanagement payload UUIDs.

```
keith — -zsh — 145×52
Last login: Thu Oct 20 12:31:55 on ttys001
keith@keiths-Air ~ % sudo sfltool dumpbtm
Password:
=======================
 Records for UID -2 : FFFFEEEE-DDDD-CCCC-BBBB-AAAAFFFFFFFE
=======================

 ServiceManagement migrated: true
 SharedFileList migrated: false

 Items:

 #1:
                 UUID: CD5C170A-3981-4DEA-8961-7668CDECB9FD
                 Name: Jamf Self Service
       Developer Name: Jamf Self Service
                 Type: managed curated developer (0xa0020)
          Disposition: [disabled, allowed, visible, not notified] (2)
           Identifier: Jamf Self Service
                  URL: (null)
           Generation: 0
  Embedded Item Identifiers:
    #1: com.jamfsoftware.task.Every 15 Minutes

 #2:
                 UUID: 88EF0CE5-864A-4F58-ABDD-3B54231B1802
                 Name: Jamf.app
       Developer Name: Jamf Self Service
      Team Identifier: 483DWKW443
                 Type: managed curated legacy daemon (0xb0010)
          Disposition: [enabled, allowed, visible, notified] (11)
           Identifier: com.jamf.management.daemon
                  URL: file:///Library/LaunchDaemons/com.jamf.management.daemon.plist
     Executable Path: /Library/Application Support/JAMF/Jamf.app/Contents/MacOS/JamfDaemon.app/Contents/MacOS/JamfDaemon
           Generation: 2
    Assoc. Bundle IDs: [com.jamfsoftware.selfservice.mac ]
    Parent Identifier: Jamf Self Service

 #3:
                 UUID: D8870C32-0EEF-475E-8972-20C2DD1C9CAA
                 Name: jamf
       Developer Name: Jamf Self Service
      Team Identifier: 483DWKW443
                 Type: managed curated legacy daemon (0xb0010)
          Disposition: [enabled, allowed, visible, notified] (11)
           Identifier: com.jamfsoftware.task.Every 15 Minutes
                  URL: file:///Library/LaunchDaemons/com.jamfsoftware.task.1.plist
     Executable Path: /usr/local/jamf/bin/jamf
           Generation: 2
    Assoc. Bundle IDs: [com.jamfsoftware.selfservice.mac ]
    Parent Identifier: Jamf Self Service
```

B. **`sudo sfltool resetbtm`** - Resets login and background item data. This is useful when testing managed background items. A reboot is recommended when running this command. The pictures below show their Login and Background items before and after the sudo sfltool resetbtm command was ran.



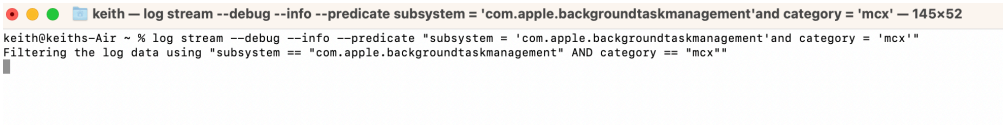
Before



After

You can also stream the logs and get real time log information using the following command:

```
log stream --debug --info --predicate "subsystem = 'com.apple.
backgroundtaskmanagement'and category = 'mcx'"
```

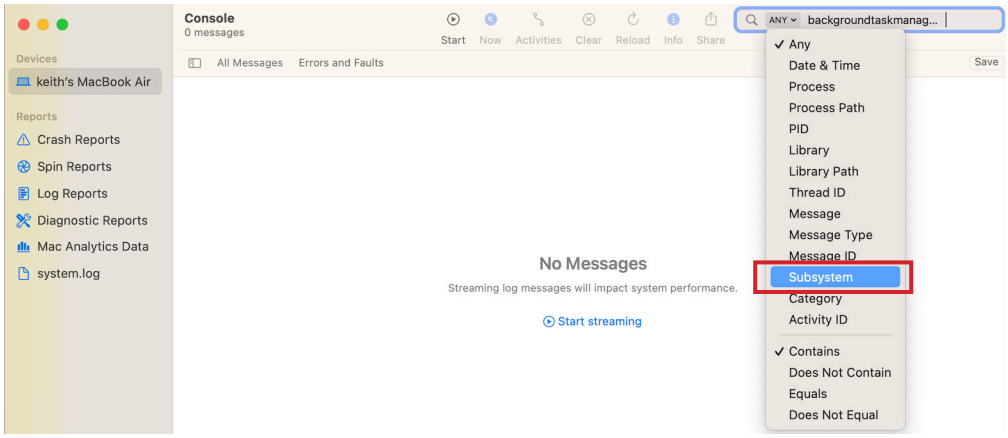


3. Open Console in /Applications/Utilities.

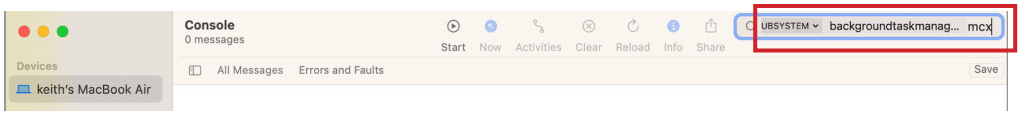
Console

4. You can monitor Login and background item management activity using the Console application by searching on the following:
   - subsystem:backgroundtaskmanagement
   - category:mcx

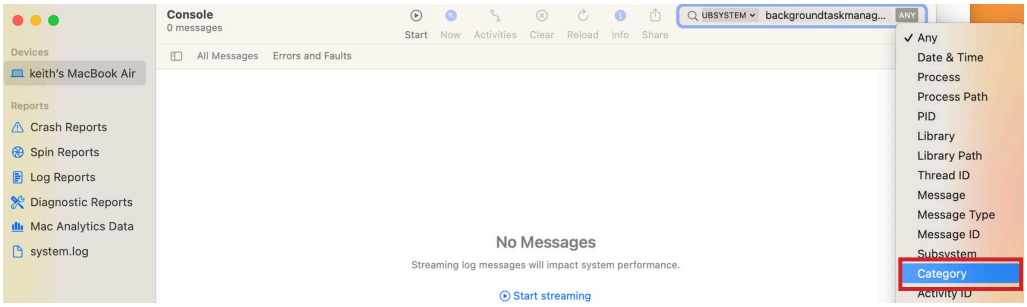
   In the search field enter backgroundtaskmanagement then press the return key. Click the filter menu and select Subsystem from the list.



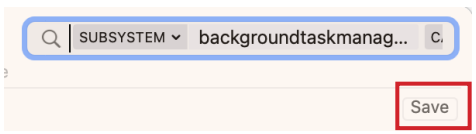
5. In the search field after the word backgroundtaskmanagement enter mcx then press the Return key.



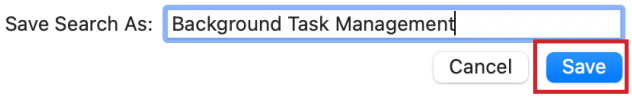
6. Click the filter menu and select Catergory from the list.



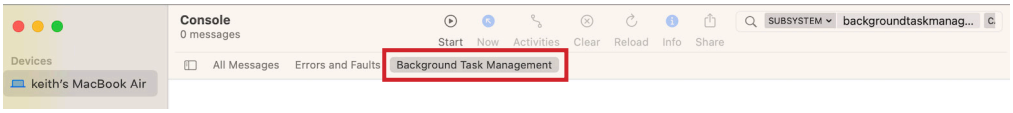
7. You can save this search for future use by clicking Save.



8. Save the search as Background Task Management.
9. Click Save.

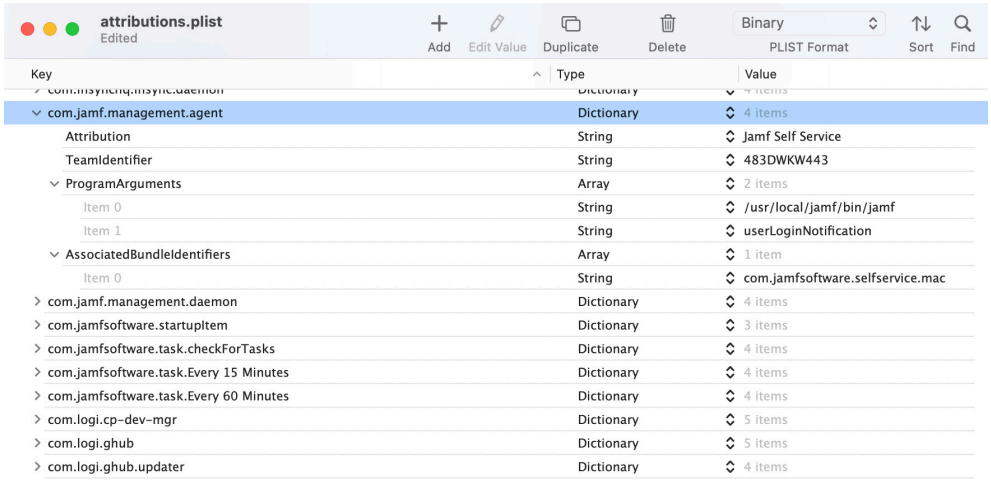


10. The item shows up in the Saved Search bar. The next time you need to perform this search, just click on it.



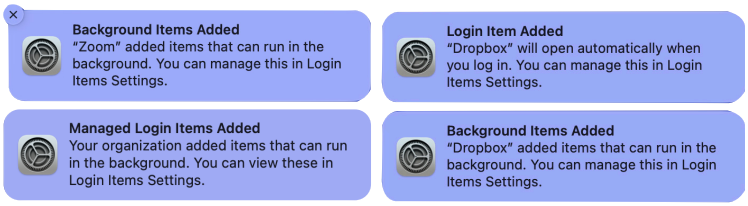
11. macOS 13.0 includes a file named attributions.plist which contains a listing of helper applications and executables used by a specific application. This will help you identify what applications and executable files show up in a users login items at startup. The file contains a myriad of information like TeamIdentifier, BundleIdentifiers, and Program Arguments. The file is located at the path below.

/System/Library/PrivateFrameworks/BackgroundTaskManagement.framework/Versions/A/Resources/attributions.plist



Section 5: Managing Login and Background Item Notifications

In this section we will create a configuration profile to manage Login and Background item Notifications as shown below.

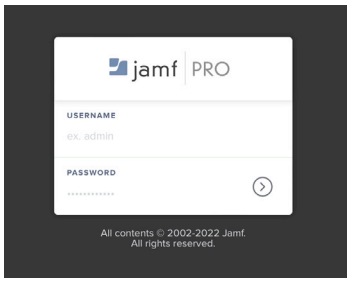


To follow along with this section you will need the following:

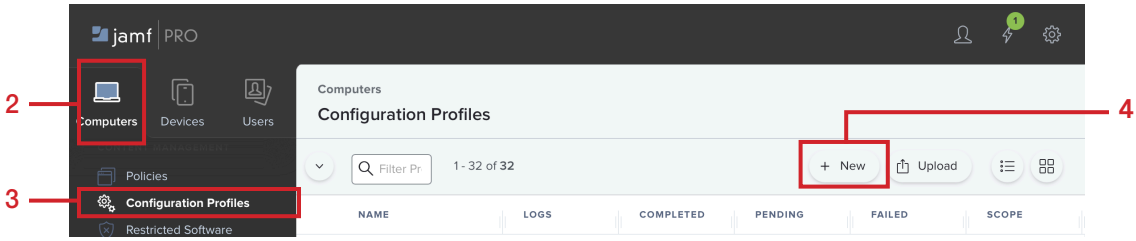
- A Mac running macOS 13.0 or later enrolled in your Jamf Pro server version 10.42 or later.
- Administrative credentials on your Jamf Pro Server.

NOTE: This section is optional. If you have a need for your users to see these notifications you can skip this section.

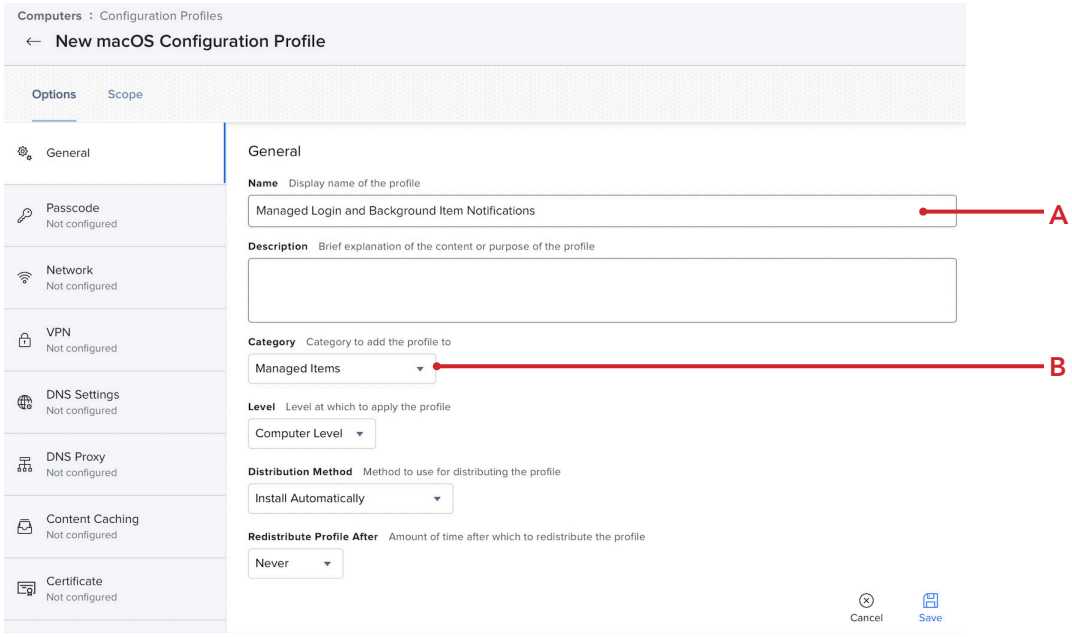
1. Log in to your Jamf Pro server with administrative credentials.



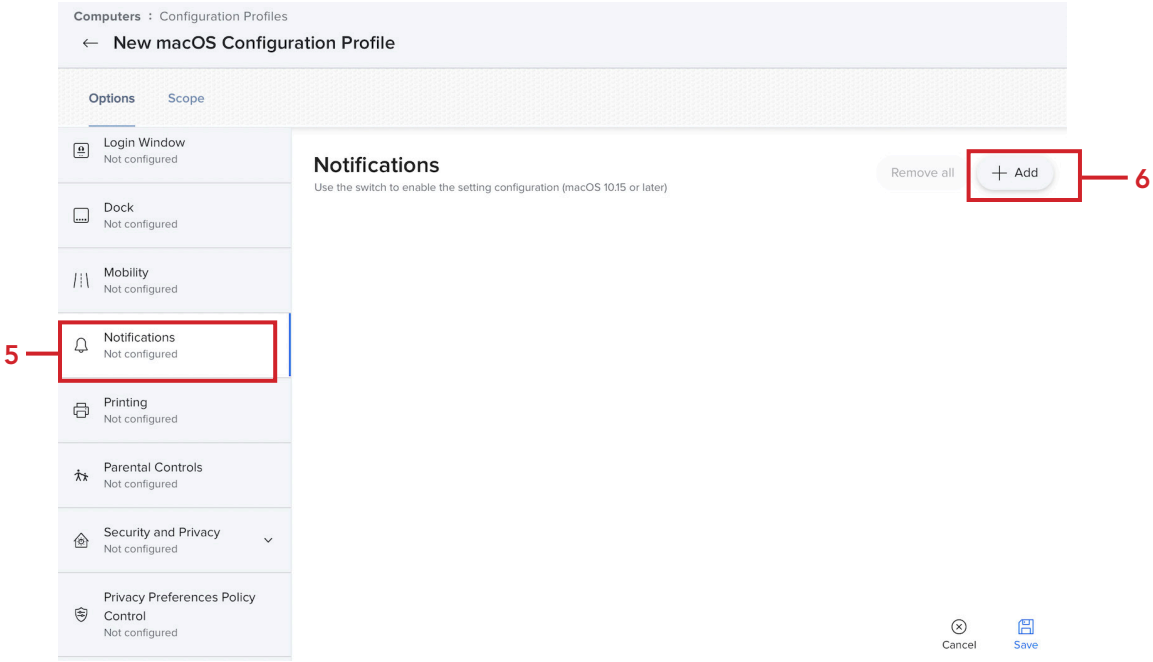
2. Click Computers
3. Click Configuration Profiles.
4. Click New.



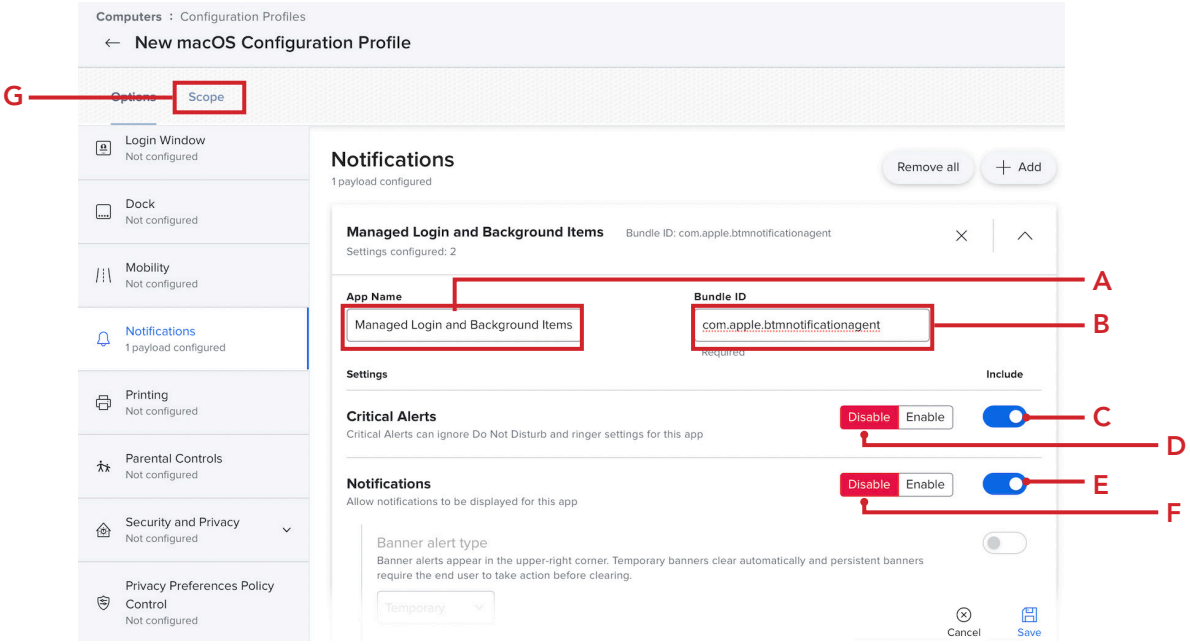
4. Enter the following:
   A. Name: Managed Login and Background Item Notifications
   B. Category: Select a category of your choosing. This guide will use Managed Items.



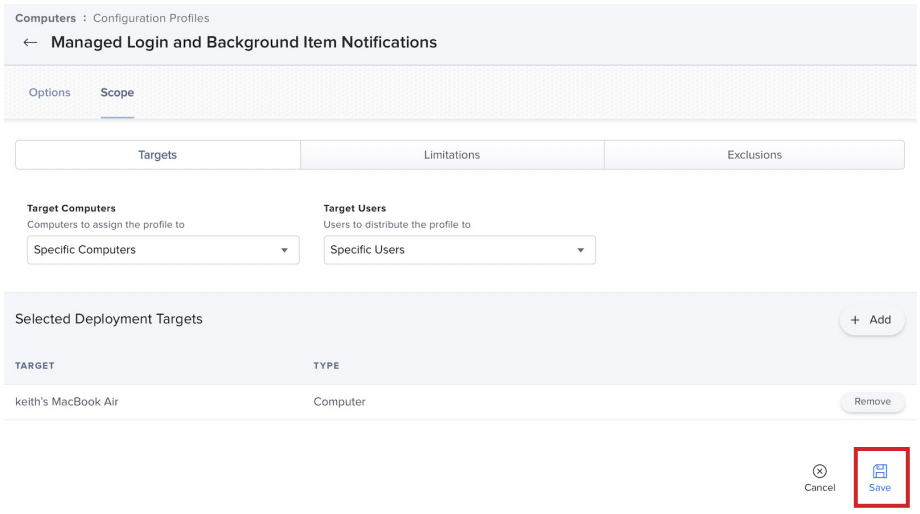
5. Click the Notifications Payload
6. Click Add.



7. Enter the following:
   A. App Name: Managed Login and Background Items
   B. Bundle ID: com.apple.btmnotificationagent
   C. Turn on Critical Alerts
   D. Click Disable
   E. Turn on Notiifications:
   F. Click Disable
   G. Click Scope



8. Scope to your needs.
9. Click Save.



10. To make scoping configuration profiles for Login and Background items easier, In Jamf Pro version 10.42 or later, create a Smart Computer Group with a Profile Identifier of com.jamf.servicemanagement.backgroundapps and scope both your Managed Login Items and Notifications payloads to that Smart Computer Group. This will allow you to deploy the configuration profiles only to Mac running macOS 13.0.

This completes this guide.