Configure Software Update Settings for macOS in Jamf Pro

Rev20241025

Contents

Preface

Ensuring timely software updates is essential for maintaining the security and integrity of Apple devices. Regular updates not only keep your environment secure but also enable users to access the latest features and security enhancements. Therefore, it's crucial for your organization to continuously assess key components that work together within your environment throughout the year, so you're prepared to deploy each release as soon as it becomes publicly available.

Declarative Device Management now offers enhanced options for managing updates across iOS, iPadOS, and macOS. It allows for more flexibility in determining when and how updates or upgrades should be enforced. Users receive detailed information in the Settings app on iPhone and iPad, and System Settings on Mac, about the status of updates when requested or enforced.

Declarative status reports provide MDM solutions with greater visibility into the update process, such as tracking whether an update is pending, downloading, or installing.

This guide will cover how to manage macOS updates using Jamf Pro as the MDM server. We'll create a custom configuration profile that includes an Application & Custom Settings payload. While Jamf Pro offers a built-in Restrictions payload for managing macOS updates, it also includes additional settings that you may not want to apply to your Mac computers. By creating a custom configuration profile, we can focus specifically on managing macOS updates without affecting other system settings.

Apple classifies macOS updates into two categories: Major and Minor. A Major update is marked by a change in the first number of the macOS version (e.g., from macOS 14 to macOS 15). In contrast, a Minor update is indicated by a change in the number following the first dot (e.g., from macOS 14.6 to macOS 14.7). Apple allows software updates to be deferred for up to 90 days. After this period, users will start receiving notifications about available macOS updates.

Rapid Security Response (RSR) is a feature introduced by Apple that delivers important security updates to macOS, iOS, and iPadOS more quickly, without requiring a full operating system update. This feature allows Apple to push critical security fixes to devices between standard software updates to address vulnerabilities or security threats as they emerge.

This guide will cover the following macOS software update scenarios:

- Deferring Major macOS updates for 90 days and allowing Minor updates
- Deferring Major macOS updates for 90 days and deferring a minor point updates
- Deferring Major macOS updates and Minor macOS updates for 90 days
- Restricting the removal of Rapid Security Response
- Restricting access to the macOS Beta Program
- Restricting access to the automatic updates section in System Settings

Learn more about managed macOS software updates at the links below:
https://it-training.apple.com/tutorials/deployment/dm215/

Go to the link below and search for "SoftwareUpdate". You will see four keys that can be managed.
https://developer.apple.com/documentation/devicemanagement/restrictions

SoftwareUpdate payload keys:
https://developer.apple.com/documentation/devicemanagement/softwareupdate

New for macOS 15:
https://developer.apple.com/documentation/devicemanagement/softwareupdatesettings

Apple Platform Guide
https://support.apple.com/guide/deployment/

Section 1: Configuring Managed Software Updates in Jamf Pro

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this guide.

Hardware and Software:

- A Non-production Mac computer running a minimum of macOS 14.5 enrolled in Jamf Pro and supervised. This guide will use macOS 14.5 as it supports all of the key value pairs used in this section.You may download macOS 14.5 from here:

  https://mrmacintosh.com/macos-sonoma-full-installer-database-download-directly-from-apple/

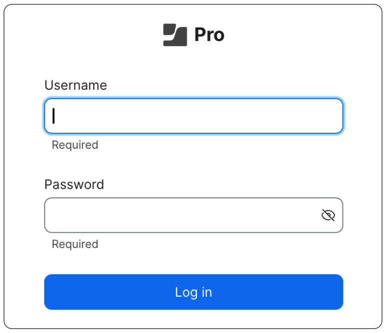
- A user with administrative credentials on a Non-production Mac computer. (Used to run terminal commands with elevated privileges)
- A Jamf Pro server with administrative user credentials

In this section we will configure the Jamf Pro server with a managed software update configuration profile using the update scenarios listed below.

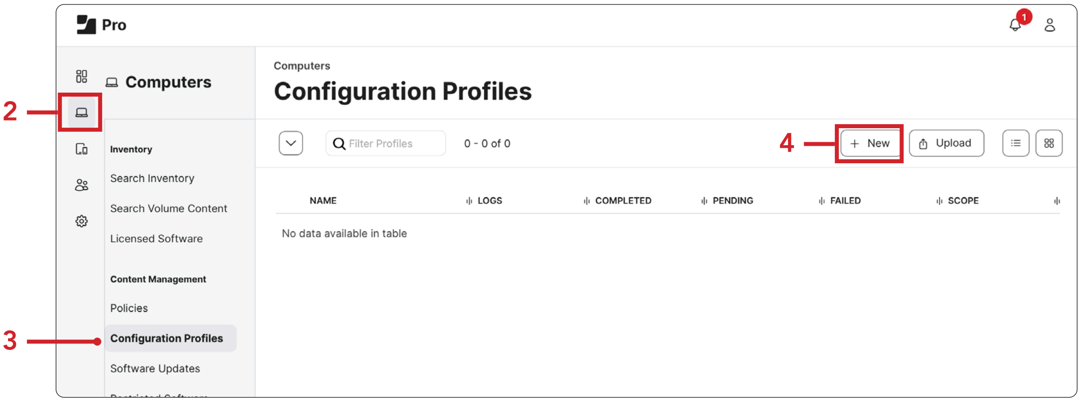
macOS software update scenarios:

- Deferring Major macOS updates for 90 days and allowing Minor updates
- Deferring Major macOS updates for 90 days and deferring a minor point updates
- Deferring Major macOS updates and Minor macOS updates for 90 days
- Restrict the removal of Rapid Security Response updates
- Restrict access to the macOS Beta Program (See note below)

1. Log into your Jamf Pro server with administrative credentials.



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



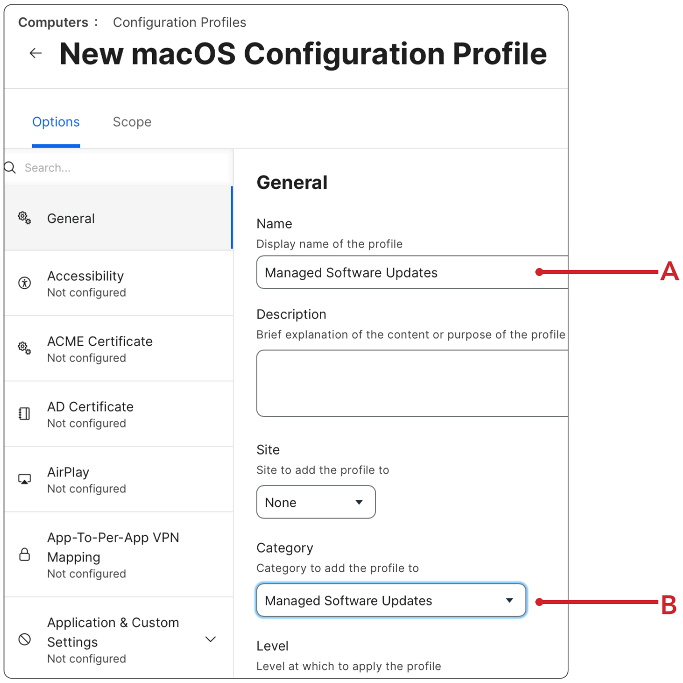
Computers

Configuration Profiles

0 - 0 of 0

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
No data available in table					

5. Configure the following:
   A. Name: **Managed Software Updates**
   B. Category: Select a category of your choosing. This guide will use Managed Software Updates.



Computers : Configuration Profiles

New macOS Configuration Profile

General

Name
Display name of the profile
Managed Software Updates

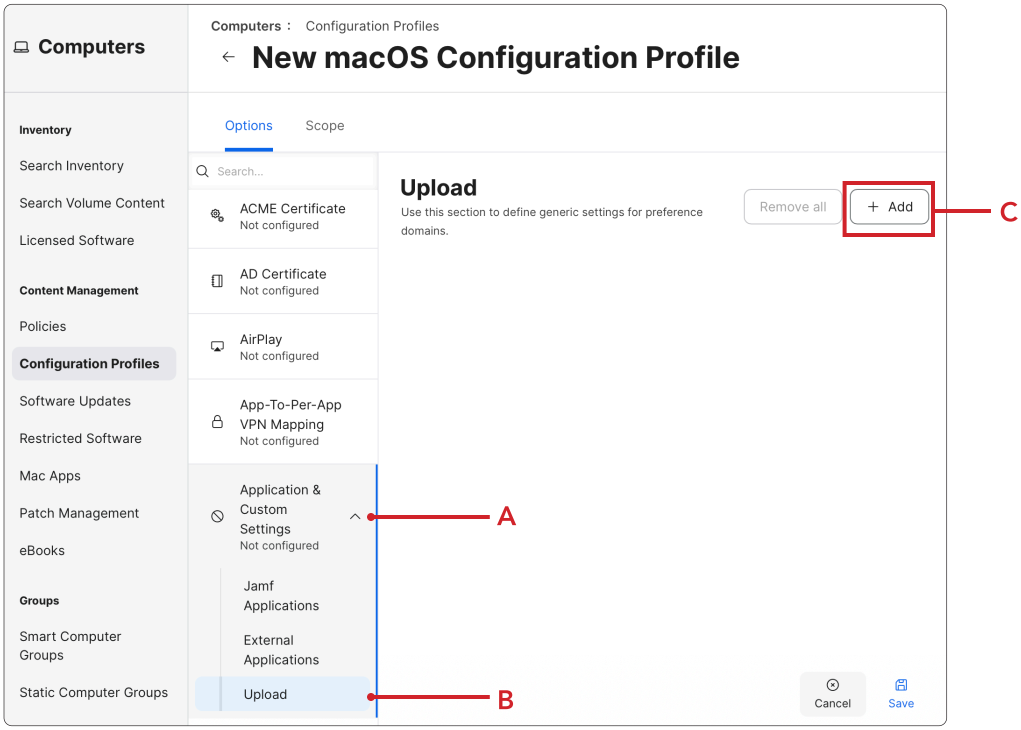
Description
Brief explanation of the content or purpose of the profile

Site
Site to add the profile to
None

Category
Category to add the profile to
Managed Software Updates

Level
Level at which to apply the profile

6. Configure the following:
    A. Select the Application & Custom Settings Payload. Expand to show the options.
    B. Select Upload
    C. Click Add.

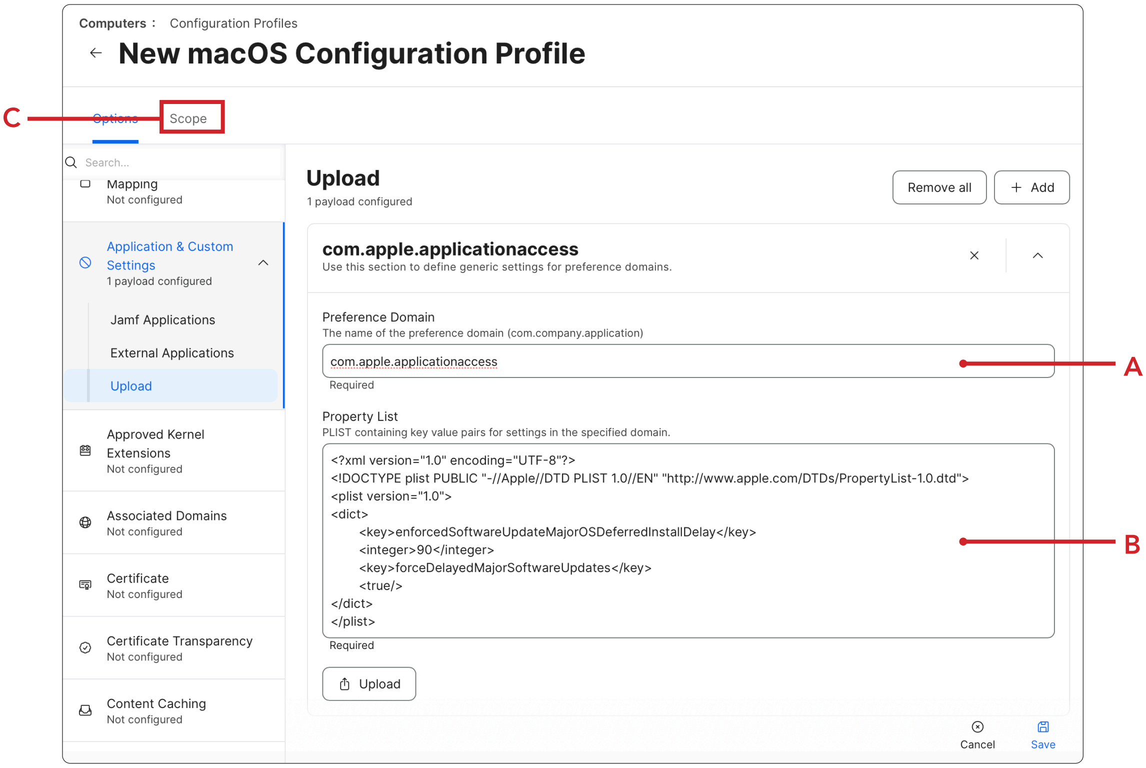


Use this section to define generic settings for preference domains.

7. Configure the following:
    A. Preference Domain: **com.apple.applicationaccess**
    B. Property List: Copy the XML below and paste it into the Property List field.
    C. Click Scope

This property list will block Major OS updates for 90 days which is the maximum amount of days allowed by Apple. I.E. macOS 14 to macOS 15. Minor updates will still be enabled. I.E. macOS 14.0 to macOS 14.7

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/DTDs/PropertyList-1.0.dtd”>
<plist version=”1.0”>
<dict>
   <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
   <integer>90</integer>
   <key>forceDelayedMajorSoftwareUpdates</key>
   <true/>
</dict>
</plist>
```



com.apple.applicationaccess
Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)
com.apple.applicationaccess
Required

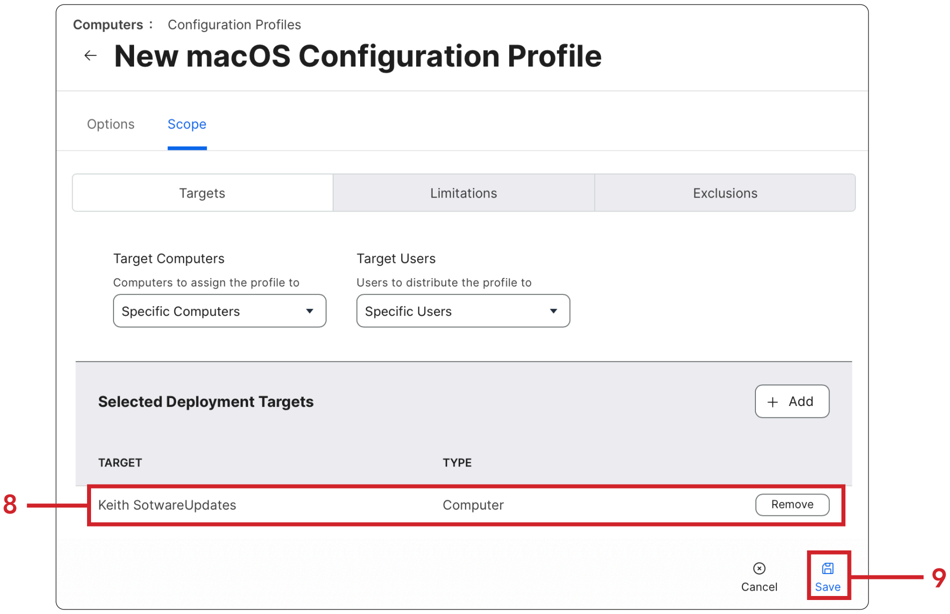
Property List
PLIST containing key value pairs for settings in the specified domain.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
</dict>
</plist>
```

Required

8. Scope to your non-production test Mac computer.

9. Click Save.



Computers : Configuration Profiles

New macOS Configuration Profile

Options | Scope

Targets | Limitations | Exclusions

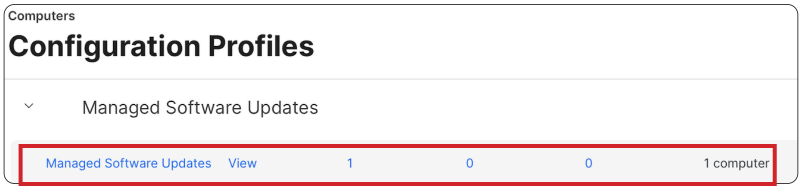
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE	
Keith SotwareUpdates	Computer	Remove

10. Confirm the Managed Software Updates configuration profile was created and scoped to your non-production Mac computer.



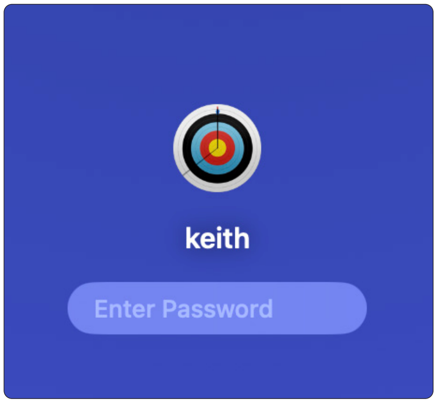
Computers

Configuration Profiles

Managed Software Updates

Managed Software Updates	View	1	0	0	1 computer

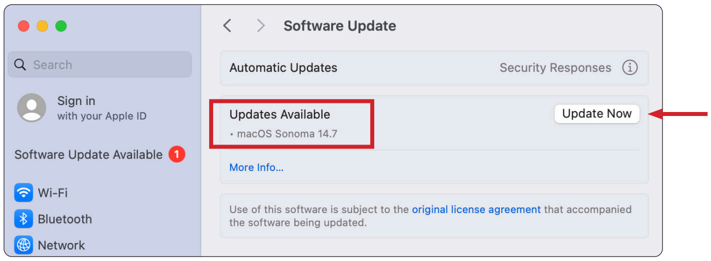
11. Log into your non-production test Mac computer with administrative credentials.



12. Open System Settings located under the Apple menu.

13. Select General > Software Update (DO NOT CLICK UPDATE NOW).

macOS 15 is not showing in the Software Update window because it's deferred for 90 days. The only update you will see is the macOS 14.7 update which is the latest version at the time of this writing.

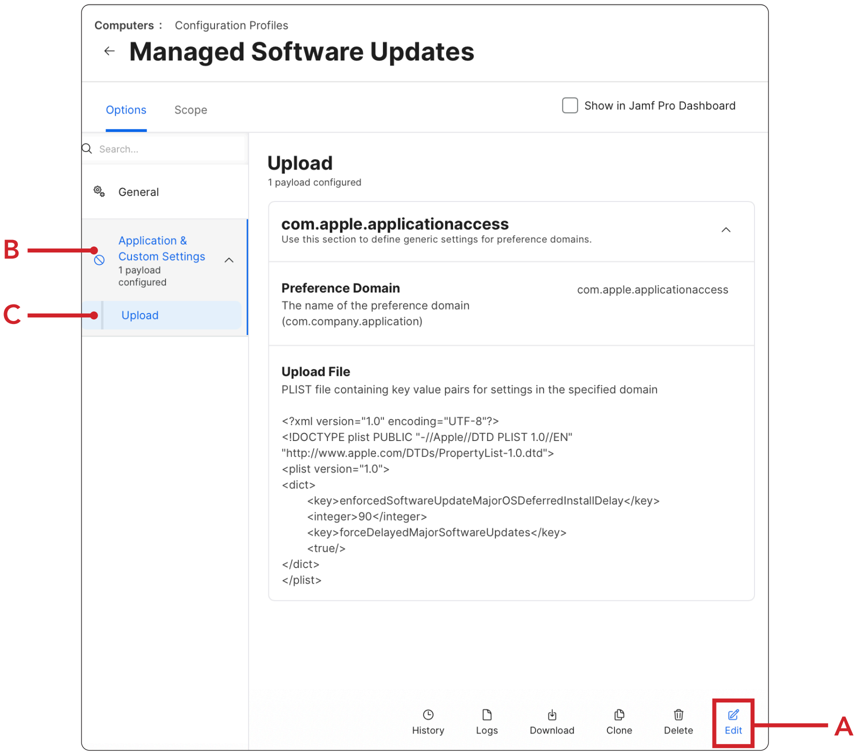


Updates Available
• macOS Sonoma 14.7

Use of this software is subject to the original license agreement that accompanied the software being updated.

Do not click Update Now

14. Switch back to your Jamf Pro server. Go to Computers > Configuration Profiles > Managed Software Updates. Select the following:
    A. Click Edit
    B. Select Application & Custom Settings
    C. Select Upload



Upload
1 payload configured

com.apple.applicationaccess
Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)
com.apple.applicationaccess

Upload File
PLIST file containing key value pairs for settings in the specified domain

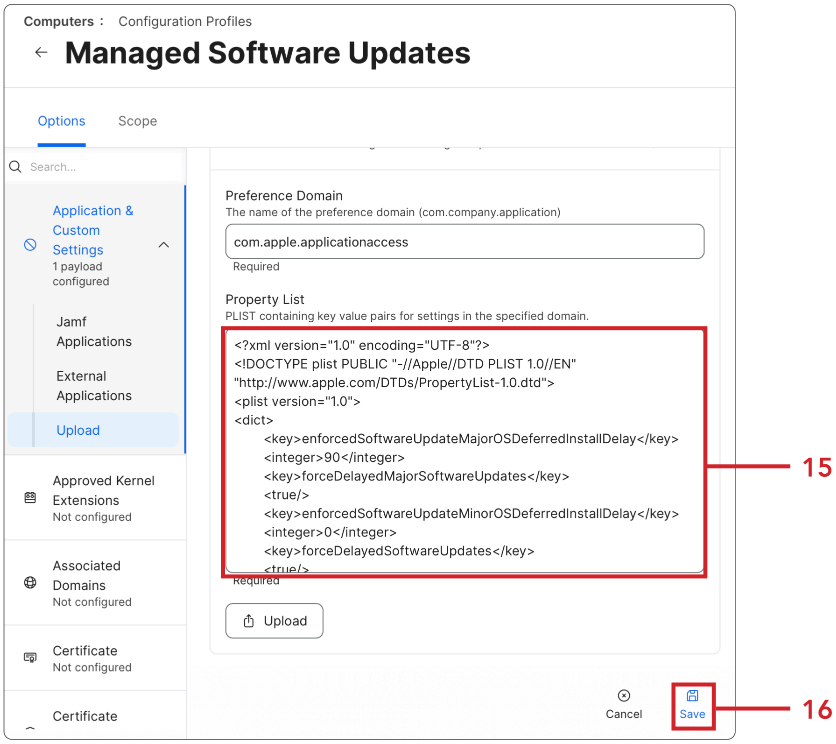
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
</dict>
</plist>
```

15. Delete the items in the plist field and replace it with the XML below.

    Minor updates will still be enabled I.E. macOS 14.0 to macOS 14.6.1 but not 14.7. We are using an undefined value of 0 in the key value pair named enforcedSoftwareUpdateMinorOSDeferredInstallDelay. The 0 value will tell macOS to use the default delay value of 30 days. By using this undefined value, it will tell the system to allow a minor update I.E. 14.6.1 but not a point update I.E. 14.7. There are some use cases where you may not want a point update I.E. 14.7 to be available to users until it is tested. Use this with caution as it is not supported by Apple however, it did work in our testing.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/DTDs/PropertyList-1.0.dtd”>
<plist version=”1.0”>
<dict>
   <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
   <integer>90</integer>
   <key>forceDelayedMajorSoftwareUpdates</key>
   <true/>
   <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
   <integer>0</integer>
   <key>forceDelayedSoftwareUpdates</key>
   <true/>
</dict>
</plist>
```

16. Click Save.



Computers : Configuration Profiles

Managed Software Updates

Preference Domain

The name of the preference domain (com.company.application)

com.apple.applicationaccess

Required

Property List

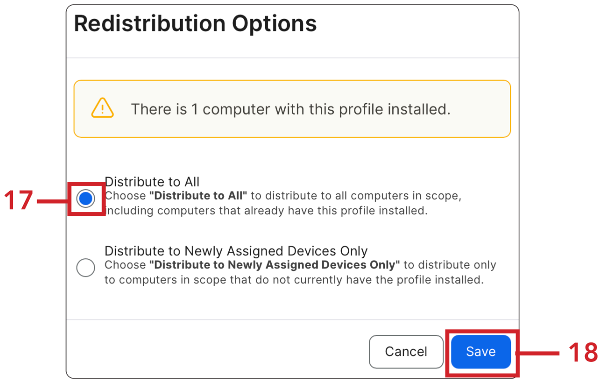
PLIST containing key value pairs for settings in the specified domain.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
      <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
      <integer>0</integer>
      <key>forceDelayedSoftwareUpdates</key>
      <true/>
```

Required

17. Select the redistribution option for your needs. This guide will click Distribute to all.

18. Click Save.



Redistribution Options

⚠ There is 1 computer with this profile installed.

● Distribute to All
Choose **"Distribute to All"** to distribute to all computers in scope, including computers that already have this profile installed.

○ Distribute to Newly Assigned Devices Only
Choose **"Distribute to Newly Assigned Devices Only"** to distribute only to computers in scope that do not currently have the profile installed.

Cancel | Save

19. Log into your non-production test Mac with administrative credentials. Open Terminal.app located in the Utilities folder.

Terminal

Run the command below to update the information shown in Software Update. The command requires administrative credentials.

```
sudo softwareupdate --list
```

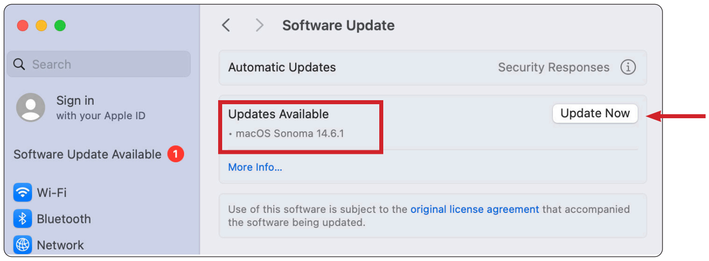
NOTE: To learn more about the softwareupdate command, read the man page by running this command in the Terminal.app

```
man softwareupdate
```

20. Open System Settings located under the Apple menu.

21. Select General > Software Update (**DO NOT CLICK UPDATE NOW**).

macOS 15 is NOT showing in the Software Update window because it's deferred for 90 days. The only update shown is macOS 14.6.1 which is NOT the latest version of macOS 14 at the time of this writing. macOS 14.7 is the latest version as was shown in step 13 of this guide.

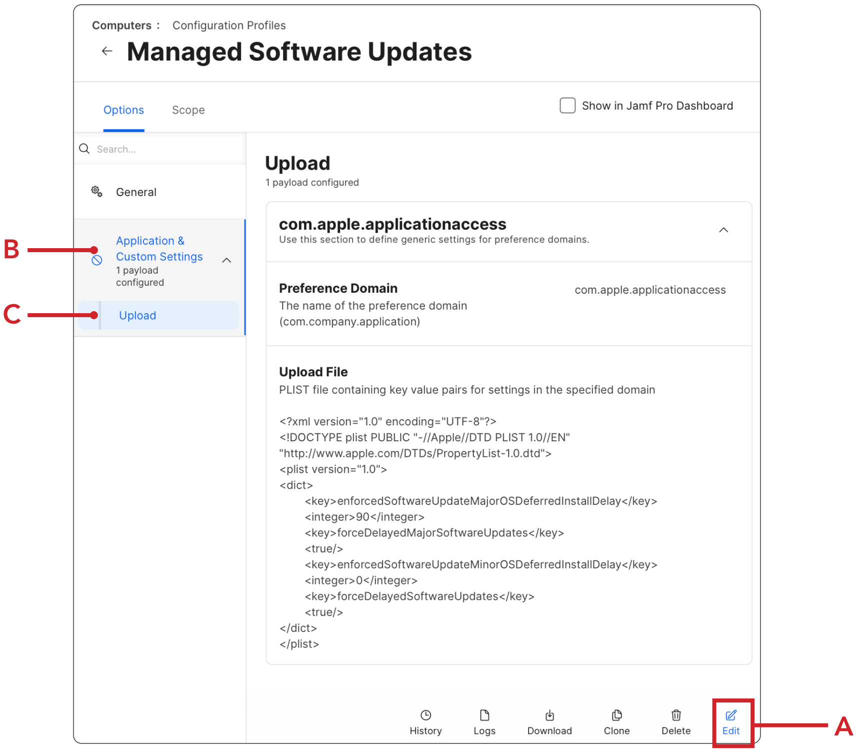


Updates Available
• macOS Sonoma 14.6.1

Use of this software is subject to the original license agreement that accompanied the software being updated.

Do not click Update Now

22. Switch back to your Jamf Pro server. Go to Computers > Configuration Profiles > Managed Software Updates. Select the following:
   A. Click Edit
   B. Select Application & Custom Settings
   C. Select Upload



Upload

1 payload configured

com.apple.applicationaccess

Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)

com.apple.applicationaccess

Upload File
PLIST file containing key value pairs for settings in the specified domain

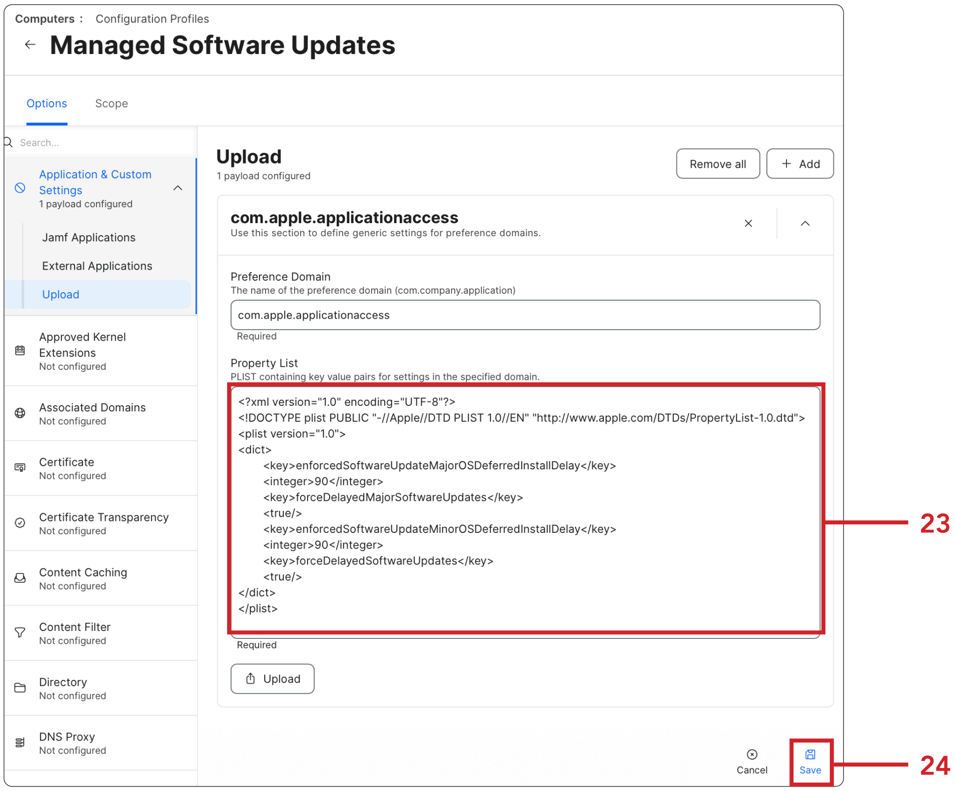
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
      <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
      <integer>0</integer>
      <key>forceDelayedSoftwareUpdates</key>
      <true/>
</dict>
</plist>
```

23. Delete the items in the plist field and replace it with the XML below.

24. Click Save.

This will block all Major and Minor macOS updates for 90 days which is the maximum amount of days allowed by Apple.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/DTDs/PropertyList-1.0.dtd”>
<plist version=”1.0”>
<dict>
   <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
   <integer>90</integer>
   <key>forceDelayedMajorSoftwareUpdates</key>
   <true/>
   <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
   <integer>90</integer>
   <key>forceDelayedSoftwareUpdates</key>
   <true/>
</dict>
</plist>
```



com.apple.applicationaccess
Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)

com.apple.applicationaccess

Required

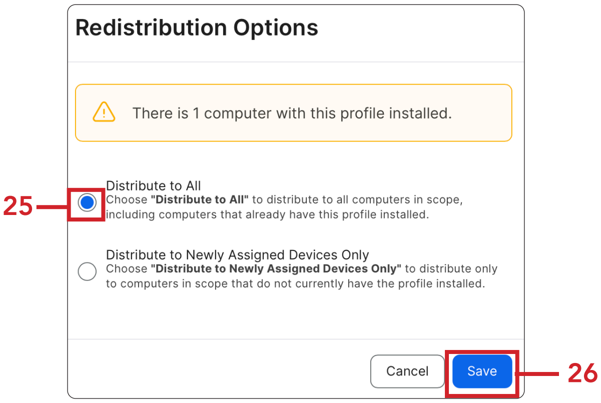
Property List
PLIST containing key value pairs for settings in the specified domain.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
      <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedSoftwareUpdates</key>
      <true/>
</dict>
</plist>
```

Required

25. Select the redistribution option for your needs. This guide will click Distribute to all.

26. Click Save.



Redistribution Options

⚠ There is 1 computer with this profile installed.

● Distribute to All
Choose **"Distribute to All"** to distribute to all computers in scope, including computers that already have this profile installed.

○ Distribute to Newly Assigned Devices Only
Choose **"Distribute to Newly Assigned Devices Only"** to distribute only to computers in scope that do not currently have the profile installed.

27. If necessary, Log into your non-production test Mac with administrative credentials. Open Terminal.app located in the Utilities folder.

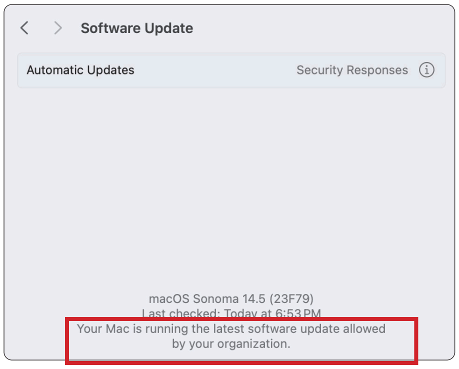
Terminal

Run the command below to update the information shown in Software Update. The command requires administrative credentials.

```
sudo softwareupdate --list
```

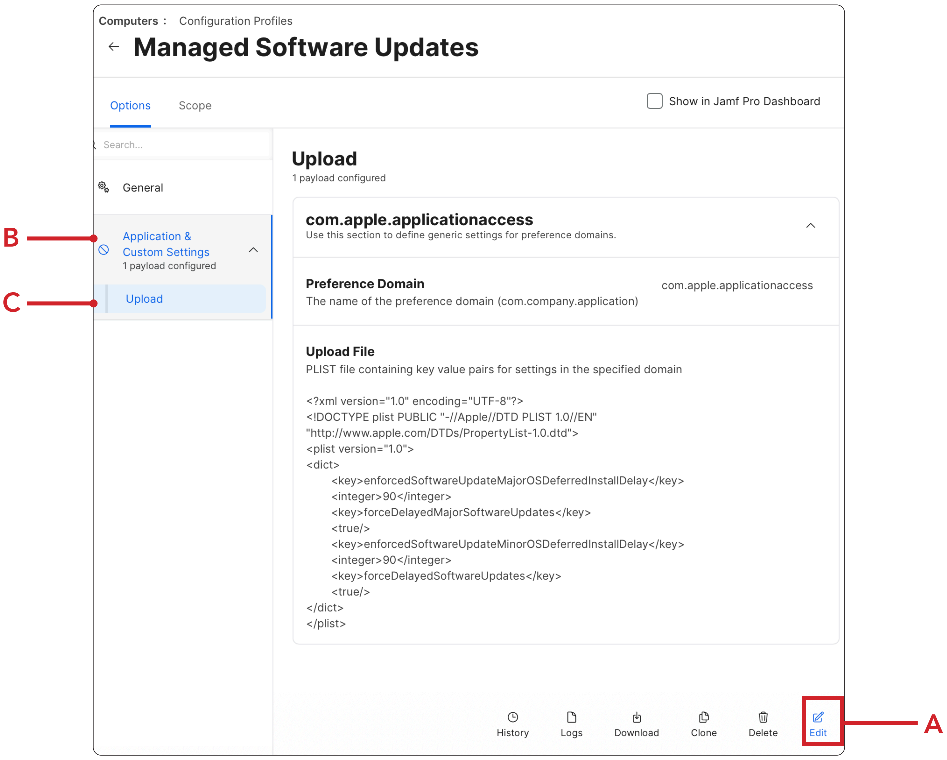
28. Open System Settings. Select General > Software Update.

macOS 15 and macOS 14.7 are NOT showing in the Software Update window because they are both deferred for 90 days. Notice the message says "Your Mac is running the latest software updated allowed by your organization."



macOS Sonoma 14.5 (23F79)
Last checked: Today at 6:53 PM
Your Mac is running the latest software update allowed by your organization.

29. Switch back to your Jamf Pro server. Go to Computers > Configuration Profiles > Managed Software Updates. Select the following:
    A. Click Edit
    B. Select Application & Custom Settings
    C. Select Upload



Managed Software Updates

Upload

1 payload configured

com.apple.applicationaccess
Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)
com.apple.applicationaccess

Upload File
PLIST file containing key value pairs for settings in the specified domain

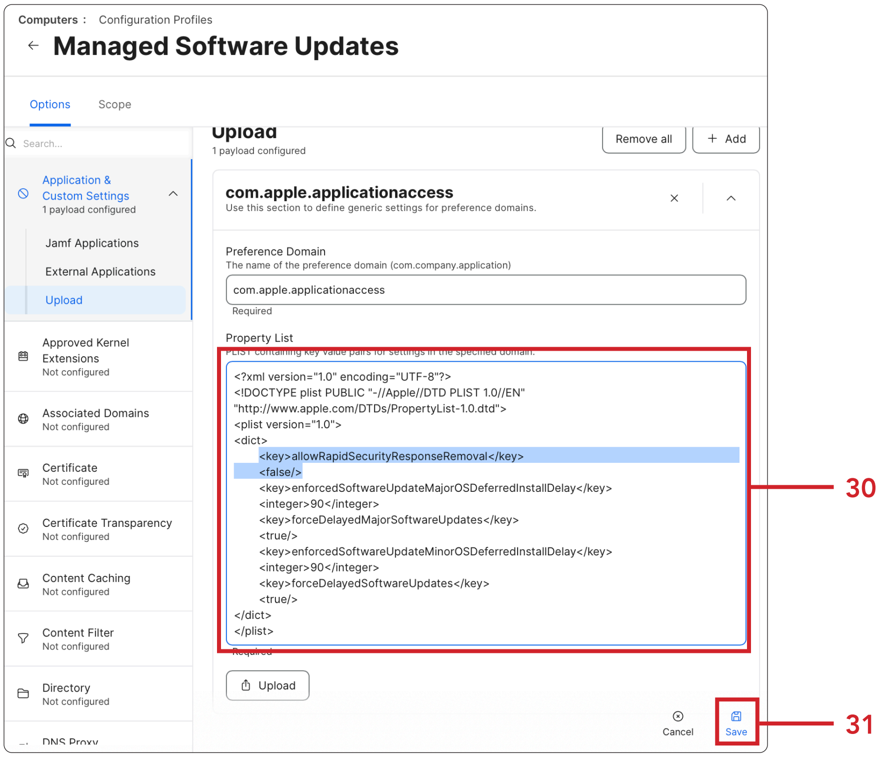
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
      <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedSoftwareUpdates</key>
      <true/>
</dict>
</plist>
```

30. Delete the items in the plist field and replace it with the XML below.

31. Click Save.

This will block all Major and Minor macOS updates for 90 days which is the maximum amount of days allowed by Apple. By adding the key “allowRapidSecurityResponseRemoval” to the xml, a user will NOT be able to remove Rapid Security Response updates.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/DTDs/PropertyList-1.0.dtd”>
<plist version=”1.0”>
<dict>
   <key>allowRapidSecurityResponseRemoval</key>
   <false/>
   <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
   <integer>90</integer>
   <key>forceDelayedMajorSoftwareUpdates</key>
   <true/>
   <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
   <integer>90</integer>
   <key>forceDelayedSoftwareUpdates</key>
   <true/>
</dict>
</plist>
```



Preference Domain
The name of the preference domain (com.company.application)

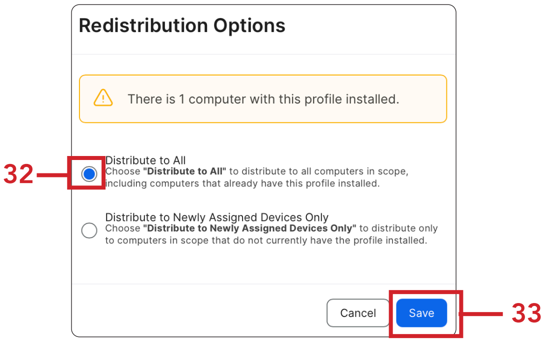
com.apple.applicationaccess

Property List
PLIST containing key value pairs for settings in the specified domain.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>allowRapidSecurityResponseRemoval</key>
      <false/>
      <key>enforcedSoftwareUpdateMajorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedMajorSoftwareUpdates</key>
      <true/>
      <key>enforcedSoftwareUpdateMinorOSDeferredInstallDelay</key>
      <integer>90</integer>
      <key>forceDelayedSoftwareUpdates</key>
      <true/>
</dict>
</plist>
```

32. Select the redistribution option for your needs. This guide will click Distribute to all.

33. Click Save.



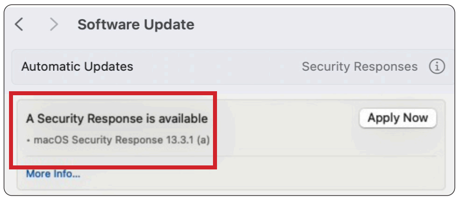
Redistribution Options

⚠ There is 1 computer with this profile installed.

● Distribute to All
Choose "**Distribute to All**" to distribute to all computers in scope, including computers that already have this profile installed.

○ Distribute to Newly Assigned Devices Only
Choose "**Distribute to Newly Assigned Devices Only**" to distribute only to computers in scope that do not currently have the profile installed.

34. There were no Rapid Security Response (RSR) updates at the time of this writing so the picture below is just a reference of what would happen if there was an available RSR update. The user would not be able to remove it.



Software Update

Automatic Updates — Security Responses ⓘ

A Security Response is available
• macOS Security Response 13.3.1 (a)

35. This key value pair can be added to any of the configuration profiles that we created in this section. We recommend adding this key to keep up with critical macOS security updates in your environment.

```
<key>allowRapidSecurityResponseRemoval</key>
<false/>
```

36. This key value pair can be added to any of the configuration profiles that we created in this section. We recommend adding this key to prevent users from enrolling in macOS Beta Programs.

```
<key>AllowPreReleaseInstallation</key>
<false/>
```

This completes this section. In the next section, we will discuss managing automatic updates in System Settings.

Section 2: Managing Automatic Software Updates with Jamf Pro

What You'll Need:

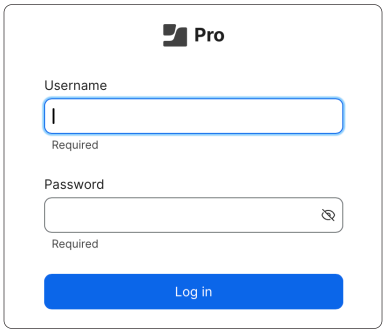
Learn what hardware, software, and information you'll need to complete the tutorials in this guide.

Hardware and Software:

- A Non-production Mac computer running a minimum of macOS 14.5 enrolled in Jamf Pro and supervised. This guide will use macOS 14.5 as it supports all of the key value pairs used in this section.
- A user with administrative credentials on a Non-production Mac computer. (Used to run terminal commands with elevated privileges)
- A Jamf Pro server with administrative user credentials

In this section, we will configure the Jamf Pro server with a managed automatic software update configuration profile that disables all automatic update settings. This approach is beneficial for organizations that need to thoroughly test updates before deploying them to all users, ensuring that the updates do not introduce any issues in the production environment.

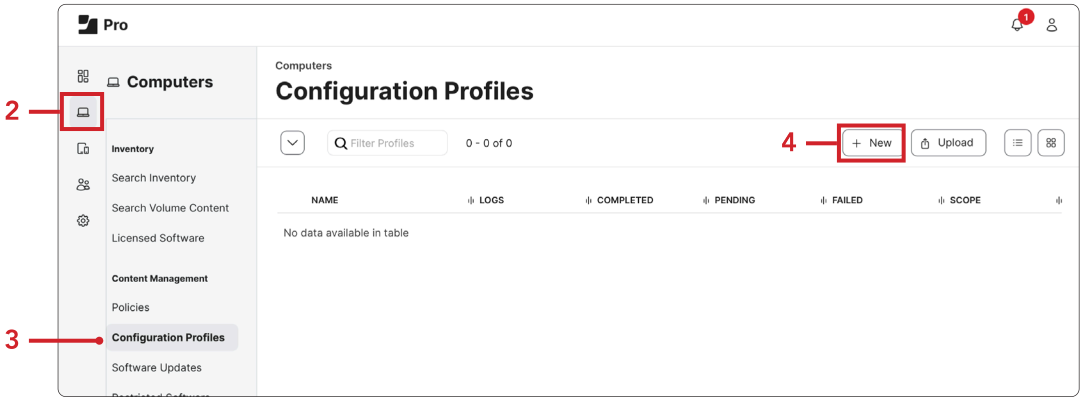
1. Log into your Jamf Pro server with administrative credentials.



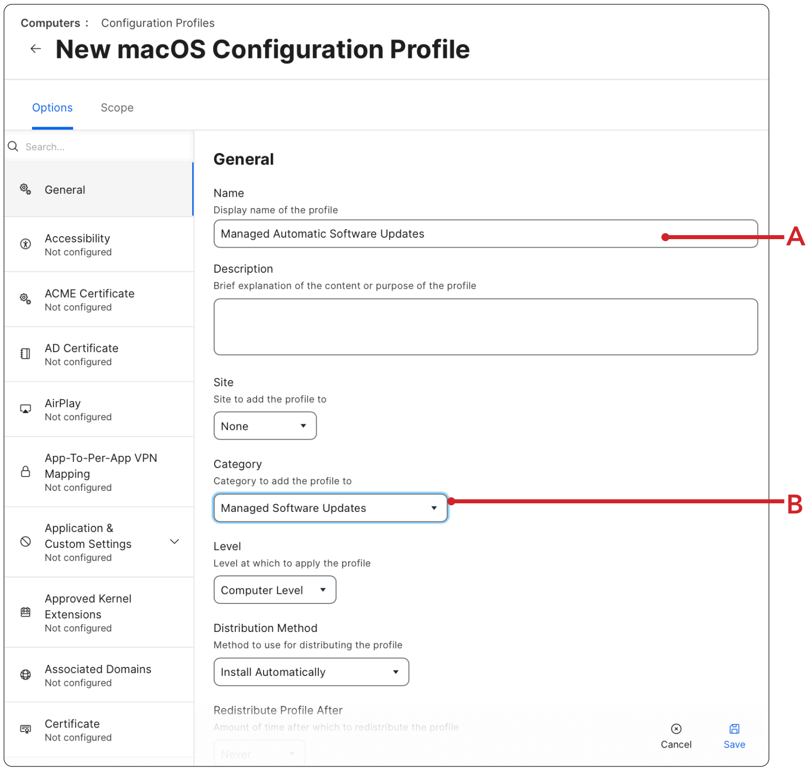
2. Click Computers .

3. Configuration Profiles.

4. Click New.



5. Configure the following:
   A. Name: Managed Automatic Software Updates
   B. Category: Select a category of your choosing. This guide will use Managed Software Updates.



Computers : Configuration Profiles

New macOS Configuration Profile

General

Name
Display name of the profile
Managed Automatic Software Updates

Description
Brief explanation of the content or purpose of the profile

Site
Site to add the profile to
None

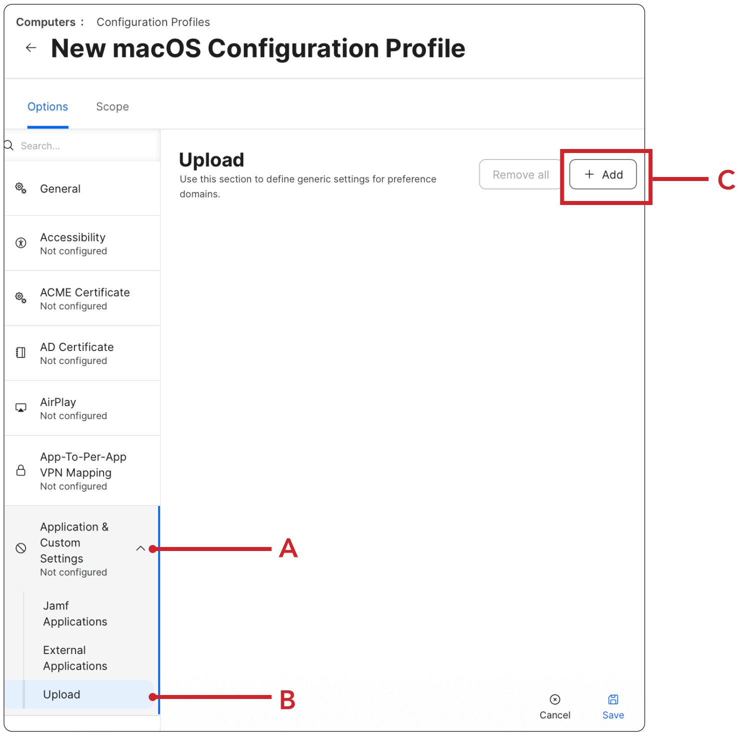
Category
Category to add the profile to
Managed Software Updates

Level
Level at which to apply the profile
Computer Level

Distribution Method
Method to use for distributing the profile
Install Automatically

Redistribute Profile After
Amount of time after which to redistribute the profile
Never

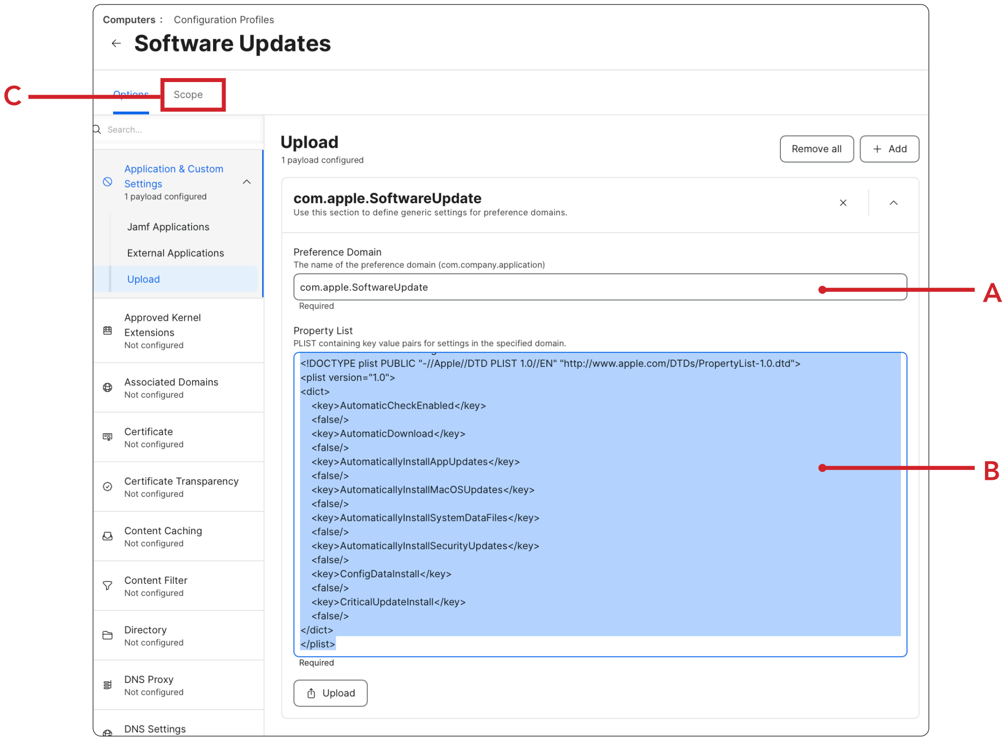
6. Configure the following:
   A. Select the Application & Custom Settings Payload. Expand to show the options.
   B. Select Upload
   C. Click Add.



7. Configure the following:
    A. Preference Domain: com.apple.SoftwareUpdate
    B. Property List: Copy the XML below and paste it into the Property List field.
    C. Click Scope

This property list will block users from enabling automatic software updates. All the values are set to false for the purposes of this guide. Feel free to set the value to true if you want certain keys to be enabled.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/DTDs/PropertyList-1.0.dtd”>
<plist version=”1.0”>
<dict>
   <key>AutomaticCheckEnabled</key>
   <false/>
   <key>AutomaticDownload</key>
   <false/>
   <key>AutomaticallyInstallAppUpdates</key>
   <false/>
   <key>AutomaticallyInstallMacOSUpdates</key>
   <false/>
   <key>AutomaticallyInstallSystemDataFiles</key>
   <false/>
   <key>AutomaticallyInstallSecurityUpdates</key>
   <false/>
   <key>ConfigDataInstall</key>
   <false/>
   <key>CriticalUpdateInstall</key>
   <false/>
</dict>
</plist>
```



com.apple.SoftwareUpdate
Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)
com.apple.SoftwareUpdate
Required

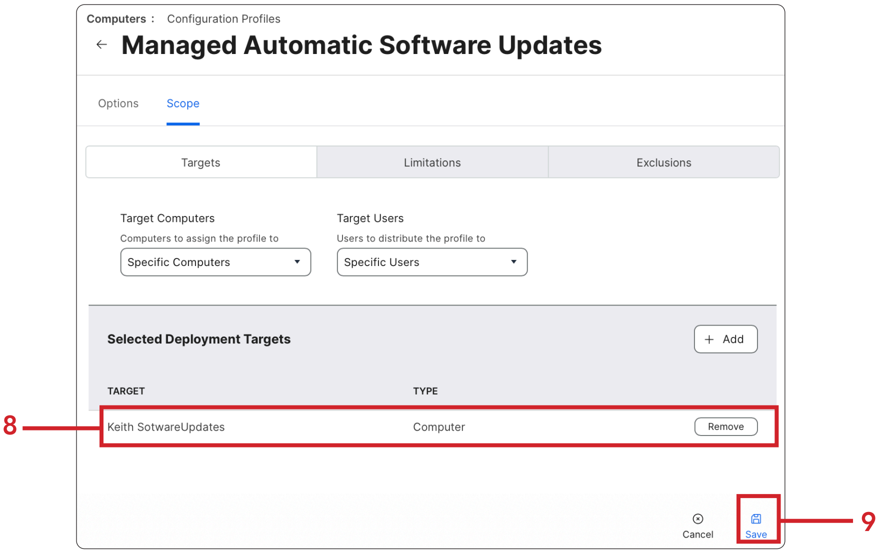
Property List
PLIST containing key value pairs for settings in the specified domain.

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>AutomaticCheckEnabled</key>
   <false/>
   <key>AutomaticDownload</key>
   <false/>
   <key>AutomaticallyInstallAppUpdates</key>
   <false/>
   <key>AutomaticallyInstallMacOSUpdates</key>
   <false/>
   <key>AutomaticallyInstallSystemDataFiles</key>
   <false/>
   <key>AutomaticallyInstallSecurityUpdates</key>
   <false/>
   <key>ConfigDataInstall</key>
   <false/>
   <key>CriticalUpdateInstall</key>
   <false/>
</dict>
</plist>
```

Required

8. Scope to your non-production test Mac computer.

9. Click Save.



Computers : Configuration Profiles

← Managed Automatic Software Updates

Options | Scope

Targets	Limitations	Exclusions

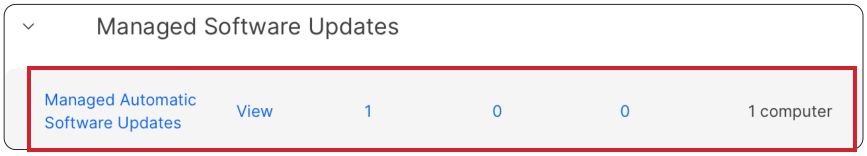
Target Computers
Computers to assign the profile to
Specific Computers ▾

Target Users
Users to distribute the profile to
Specific Users ▾

Selected Deployment Targets + Add

TARGET	TYPE	
Keith SotwareUpdates	Computer	Remove

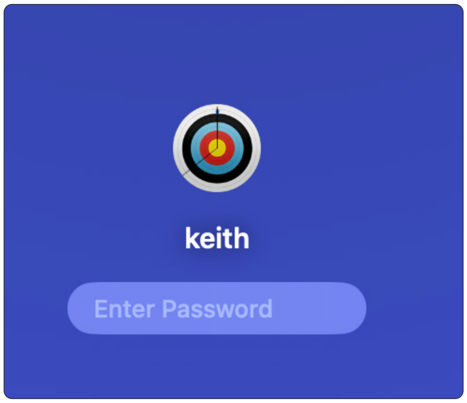
10. Confirm the Managed Automatic Software Updates configuration profile was created and scoped to your non-production Mac computer.



Managed Software Updates

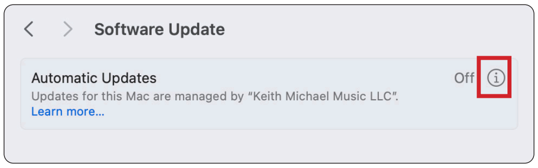
Managed Automatic Software Updates	View	1	0	0	1 computer

11. Log into your non-production test Mac computer with administrative credentials.



12. Open System Settings under the Apple menu.

13. Select General > Software Update and select info (ⓘ) for Automatic Updates.

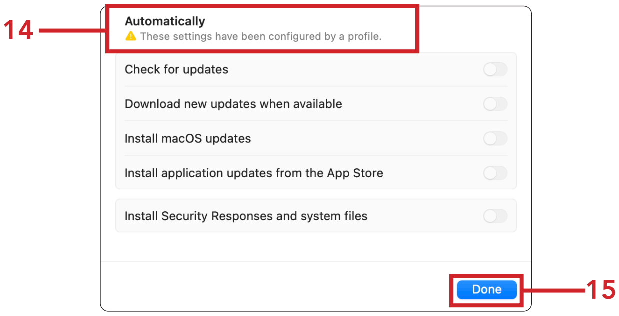


Automatic Updates
Updates for this Mac are managed by "Keith Michael Music LLC".
Learn more...

Off ⓘ

14. Confirm a warning that indicates the settings have been configured by a profile.

15. Click Done.



Automatically
⚠ These settings have been configured by a profile.

Check for updates ○
Download new updates when available ○
Install macOS updates ○
Install application updates from the App Store ○
Install Security Responses and system files ○

This completes the guide.