Creating Blueprints and Provisioning Workflows with Apple Configurator 2

Contents

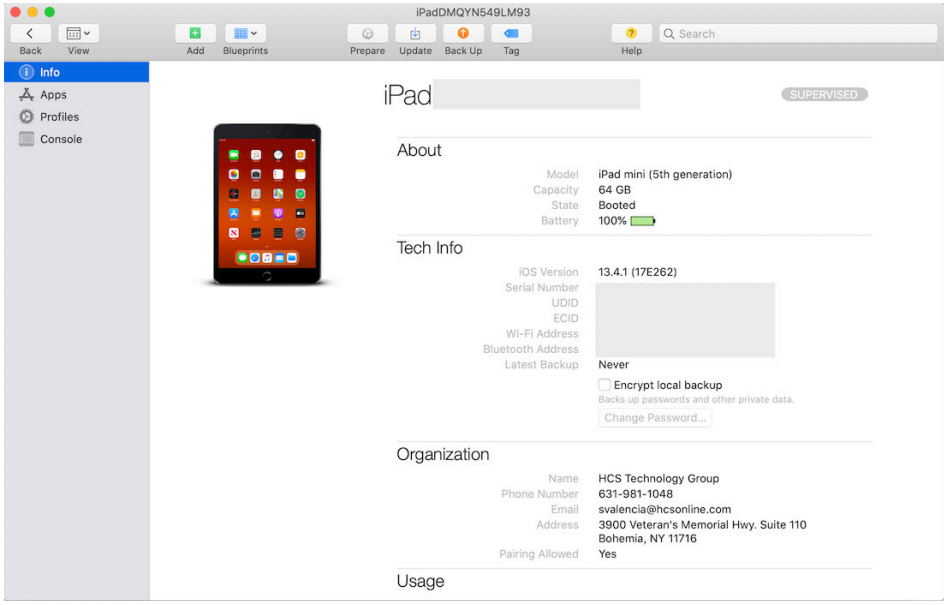
Apple Configurator 2 is a macOS app that allows IT to deploy one or many iOS, iPadOS, and tvOS devices in an organization. Although you might be aware of some of the well-known features of Apple Configurator 2, this guide shows you how to use Blueprints to not only create a templated workflow but to use additional Actions built in to the product. Beyond simply setting a name and wallpaper, Apple Configurator 2 can also interact with Apple's Apps and Books program to distribute content you purchase in bulk. When used in conjunction with content caching, you can create a powerful method of deployment that can ease strain on a network. Lastly, this guide explores a feature called tethered caching, which can share the internet connection and cached content of a Mac with iOS devices that are connected using USB.

When used in conjunction with Apple Business Manager and a mobile device management (MDM) solution, Apple Configurator 2 can perform many tasks out of the gate without you and your staff tapping on the devices. You can get devices in the hands of your users more quickly and efficiently.

There are a number of workflows you can consider when provisioning iOS, iPadOS, and tvOS devices, including but not limited to:

- Option 1: Devices that are in Apple Business Manager and can be provisioned in MDM using Automated Device Enrollment
- Option 2: Devices that are in Apple Business Manager and not currently enrolled in MDM
- Option 3: Devices that are not in Apple Business Manager and not currently enrolled in MDM
- Option 4: Devices that are not in Apple Business Manager and no MDM solution exists

This guide explores option 1 in detail.



Here's an example of Apple Configurator 2 displaying information about a connected iPad.

Apple Configurator 2 allows you to connect multiple iOS, iPadOS, and tvOS devices to a single Mac in order to deploy a workflow. A variety of hubs or carts are available for mass deployment.

Some example manufacturers include Cambrionix for quality USB hubs and Bretford for charging carts. Although this guide uses a single iPadOS device, the steps can apply no matter the size of your deployment.

Some examples of products are below:

Cambrionix ThunderSync2-16:
https://www.cambrionix.com/products/thundersync2-16-industrial-usbhub

Bretford PowerSync+ Cart:
https://www.bretford.com/product/powersyncplus-cart
NOTE: Be aware that some carts support only charging and do not support syncing data. Confirm the cart in use is capable of syncing.

If you use more than one Apple Configurator 2 computer, we recommend that you use a Managed Apple ID to store various Apple Configurator 2 settings in iCloud Drive. This way you can keep your configuration profiles and other settings consistent across multiple Apple Configurator 2 computers. We recommend that you use a Managed Apple ID instead of a personal Apple ID, so your organization can retain ownership and control of the Apple ID. Ensure that the Managed Apple ID has the role of Content Manager at the minimum. Go to Section 4 for more information about creating Managed Apple IDs.

A supervision identity allows you to have additional management capabilities for a connected iOS or iPadOS device. You can share the supervision identity with multiple Mac computers, and even your MDM solution. Sharing a supervision identity is a task that is outside the scope of this guide.

This guide was created using the following:

- Apple Configurator 2.12.1
- iPad mini (5th generation) (unsupervised, at Setup Assistant) with iPadOS 13.4.1
- USB-C Lightning cable
- macOS Catalina 10.15.4
- Jamf Pro 10.20.1
- Apple Business Manager credentials for a user that has at least Content Manager privileges

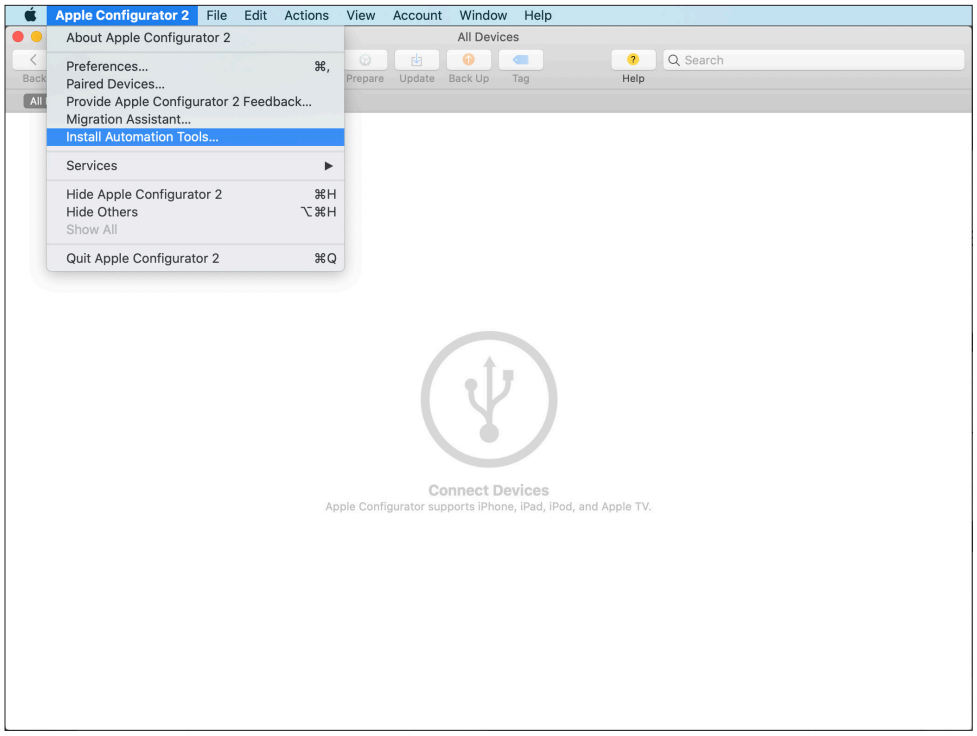
Articles & Documentation

- Apple Configurator 2 User Guide:
  https://support.apple.com/guide/apple-configurator-2/welcome/mac
- Enrolling in Apple Business Manager/Apple School Manager:
  https://hcsonline.com/support/white-papers/enrolling-your-organization-in-apple-business-manager-apple-school-manager
- Set Up content caching on Mac:
  https://support.apple.com/guide/mac-help/set-up-content-caching-on-mac-mchl3b6c3720/mac
- Preserve or Migrate Data for Apple Configurator 2:
  https://support.apple.com/en-us/HT207434
- Use the Apple Configurator 2 command-line tool on Mac:
  https://support.apple.com/et-ee/guide/apple-configurator-2/cad856a8ea58/mac

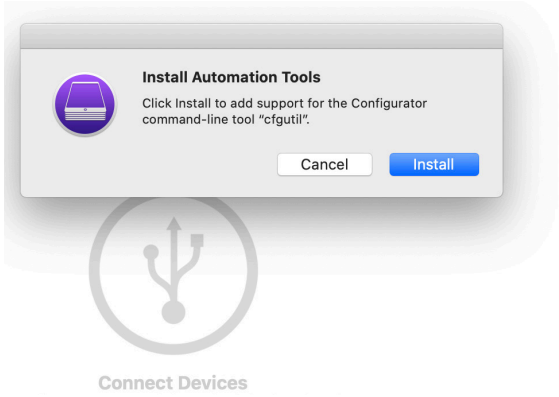
Section 1: Install Automation Tools and review the cfgutil man page

Apple Configurator 2 includes hidden treasures in command-line automation tools. You can use these tools to write shell scripts and automate processes. Use the following steps to install the automation tools and the **cfgutil** tool.

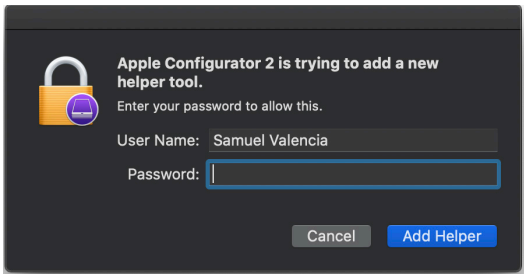
1. If you haven't already installed Apple Configurator 2, use the App Store to get Apple Configurator 2.
2. Open Apple Configurator 2.
3. Click the Apple Configurator 2 menu and choose Install Automation Tools.



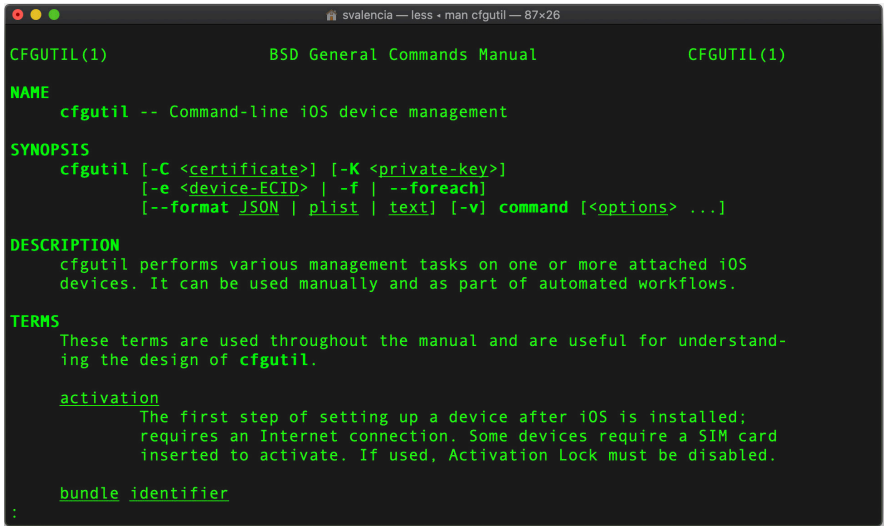
4. At the prompt to "Install Automation Tools," click Install.



5. Provide administrator user credentials then click Add Helper.



6. Open Terminal.
7. To review the man page for the cfgutiil command, at the Terminal prompt, enter **man cfgutil** then press Return.



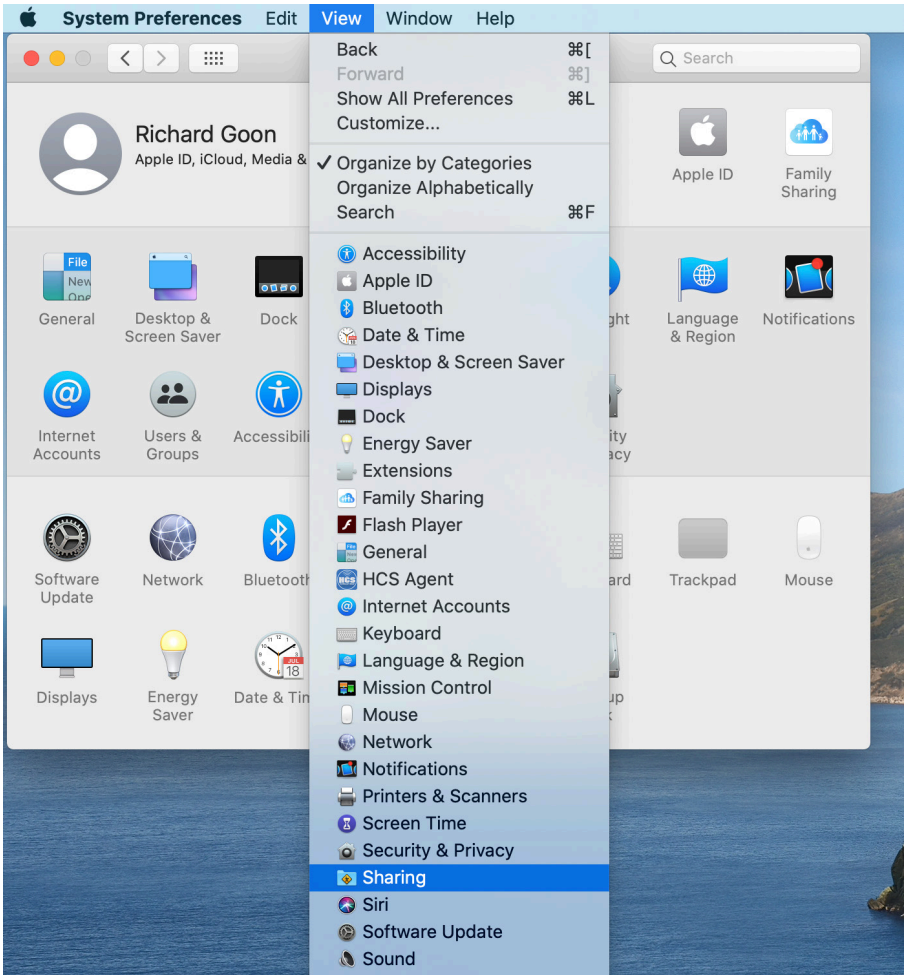
8. When you are reviewing the man page:
   - Press the Space bar to advance a page
   - Press the B key to go back a page
9. Press the Q key to exit the man page.

Section 2: Configure Content Caching in macOS

Configure the options in the following steps to ensure more efficient deployment of apps (content caching) and to allow the devices connected via USB to share the internet connection of the Mac (tethered caching)

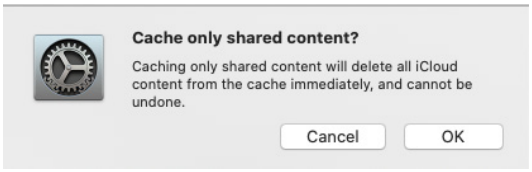
1. Click the Apple menu then choose select System Preferences.

2. From the View menu, choose Sharing.

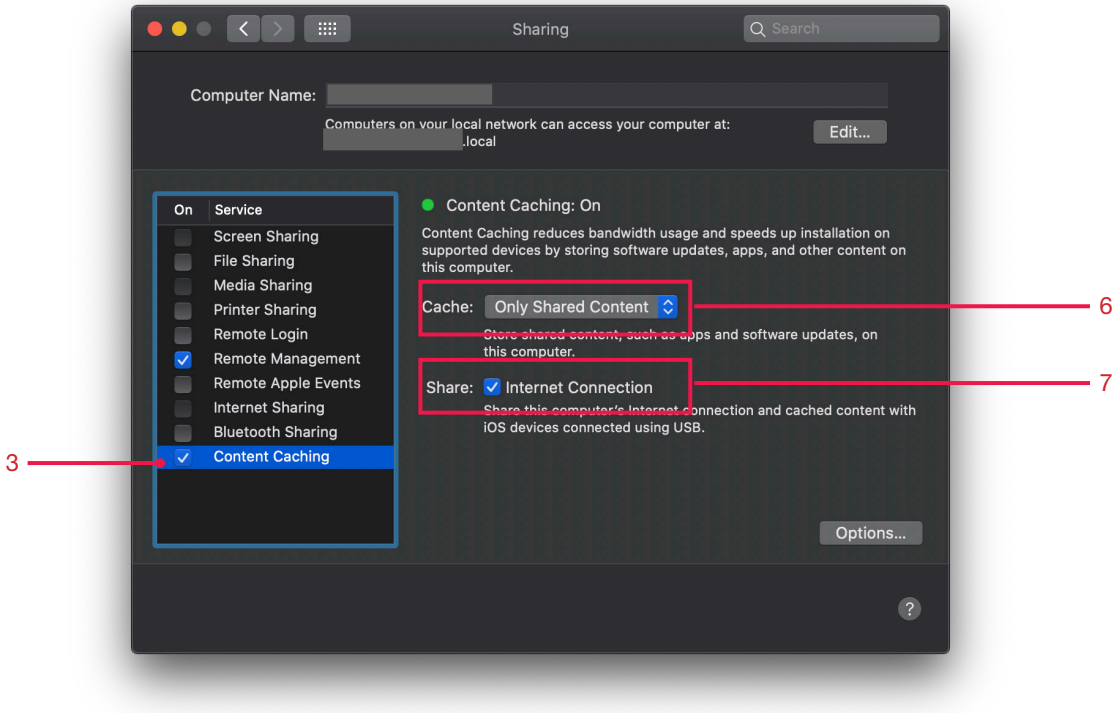


3. In the left column, select the checkbox for Content Caching.
4. The following message may appear. Decide if you want to see this message again and click OK.

5. In the dialog that appears, click OK.



6. If necessary, click the Cache menu and choose Only Shared Content. This allows for content caching of apps and books and keeps your Mac from caching iCloud content.
7. Next to Share, select the checkbox for Internet Connection. This allows for tethered caching.



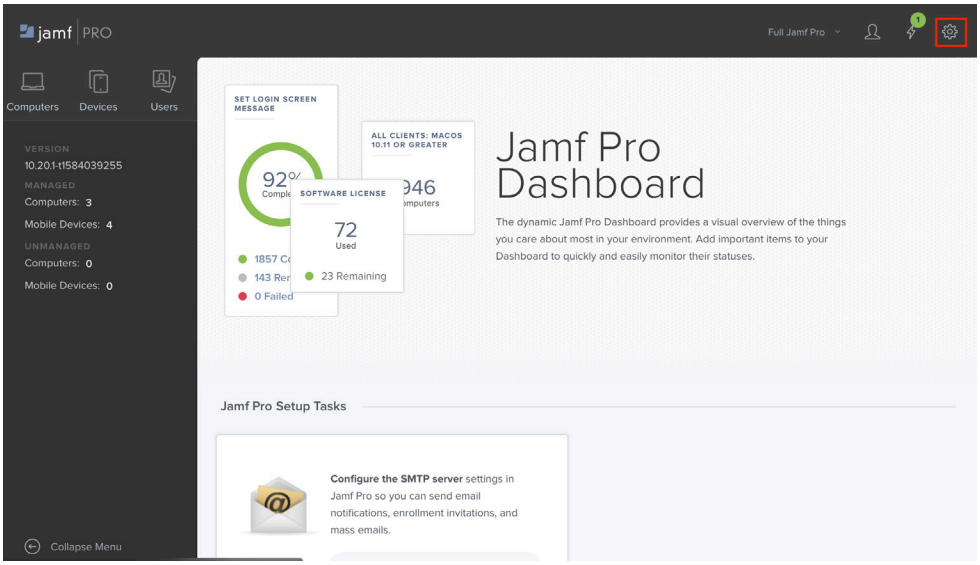
8. Quit System Preferences.

Section 3: Create a Supervision Identity in MDM

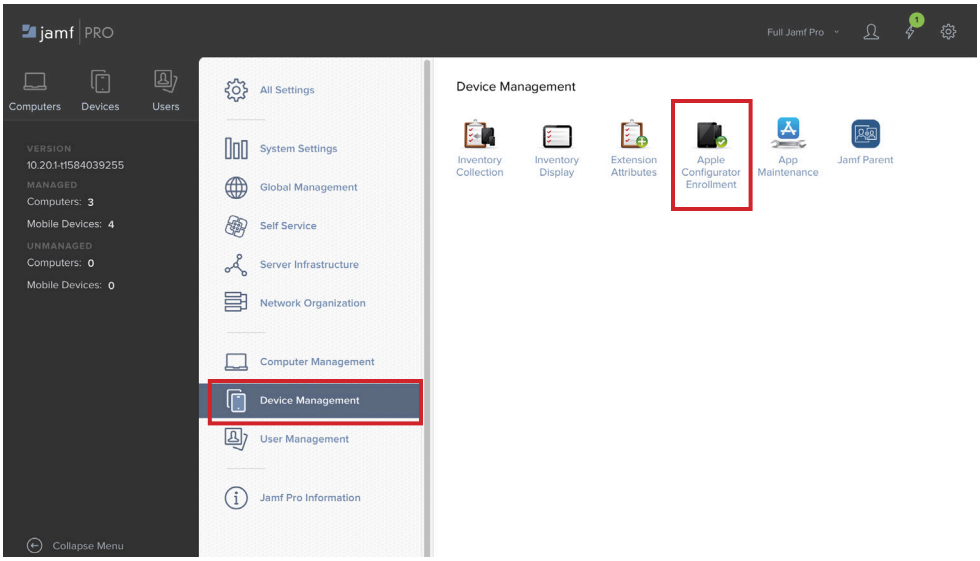
In Apple Configurator 2, Supervision Identities can be used to ensure devices can be paired with multiple Apple Configurator 2 workstations. The same Supervision Identity and identity certificate must be used for this purpose. This identity can also be used in conjunction with an MDM. That Supervision Identity is applied to devices during automated enrollment. Supervision allows for items like Wallpaper to be applied in Apple Configurator 2.

In this example, Jamf Pro is the MDM in use.

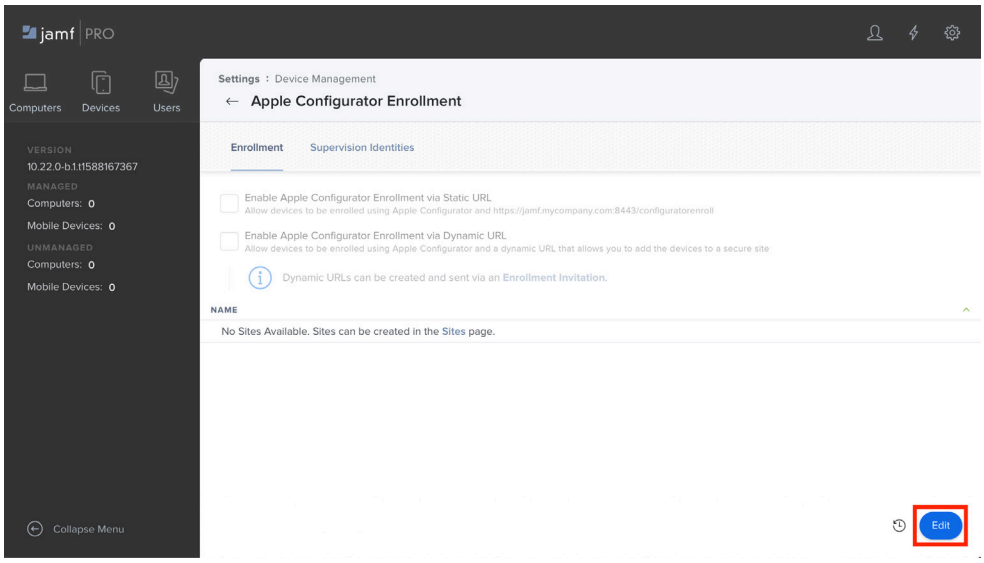
1. Sign in to Jamf Pro.
2. Click on the Settings on the upper right.



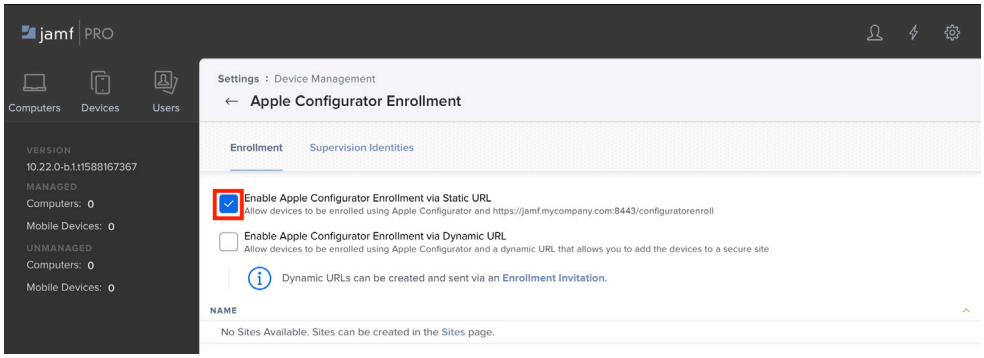
3. Click on Device Management and select Apple Configurator Enrollment.



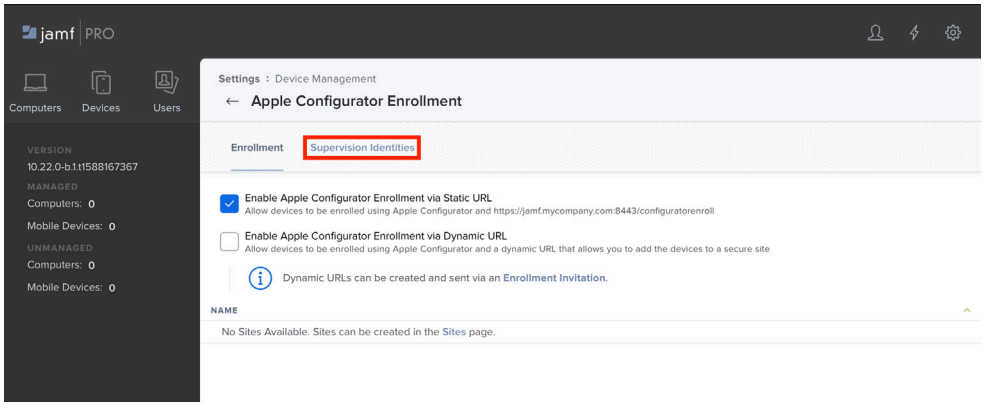
4. Click Edit on the bottom right.



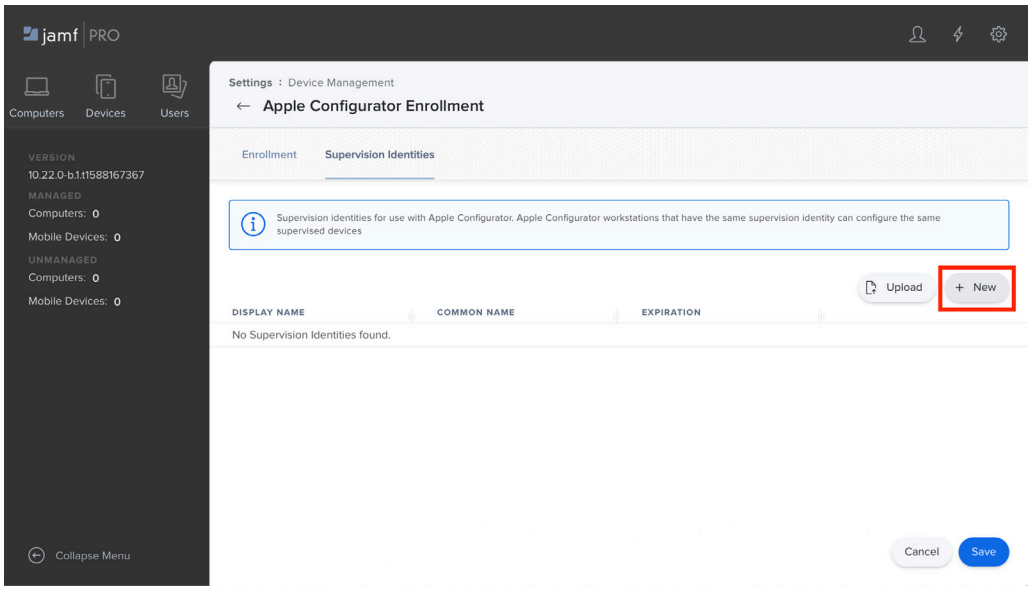
5. Check the box to Enable Apple Configurator Enrollment via Static URL.



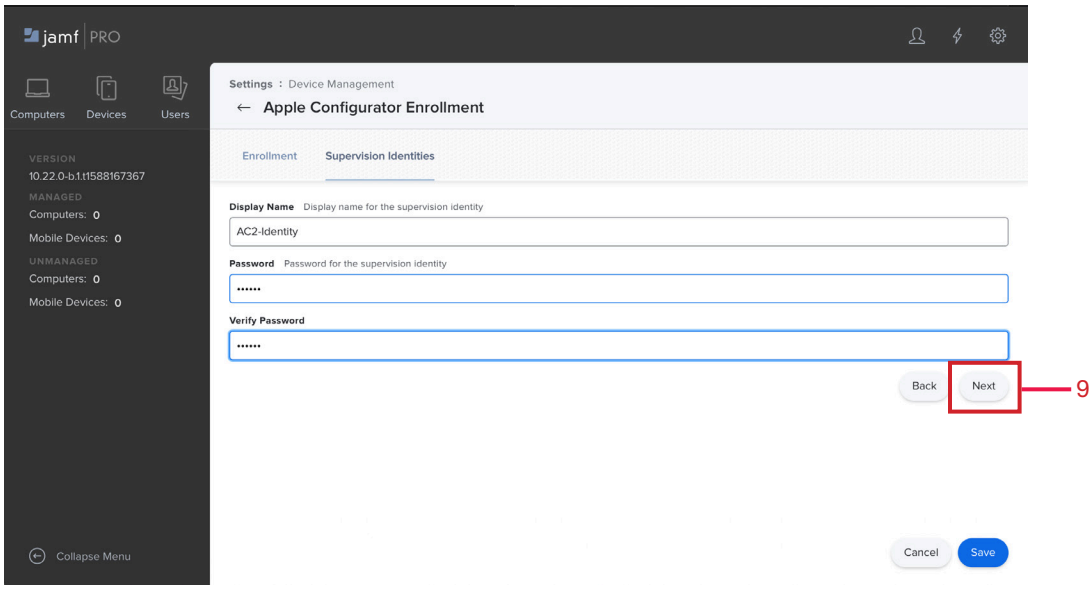
6. Click Supervision Identities.



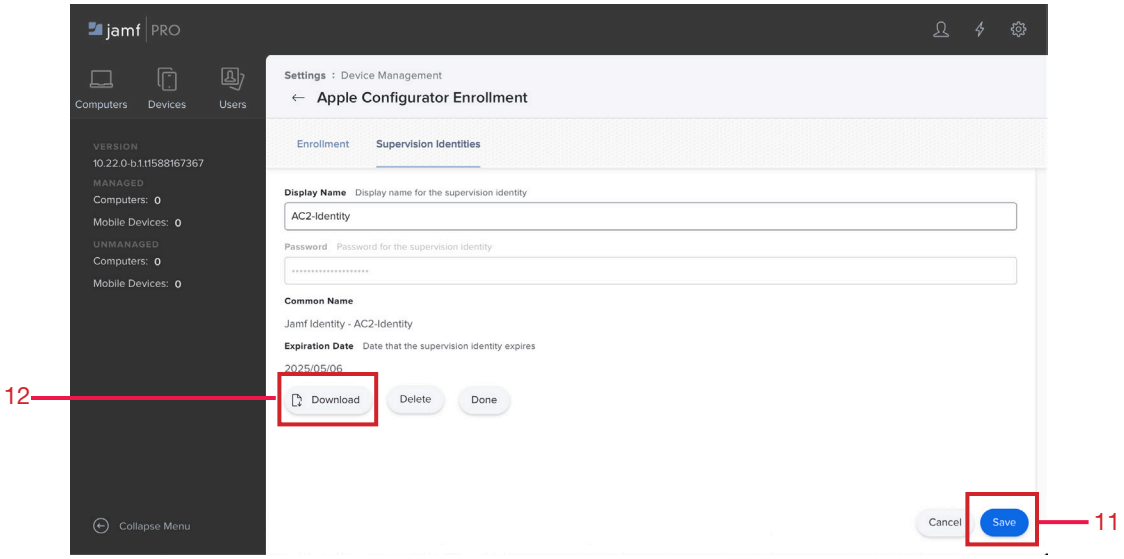
7. Click the New button.



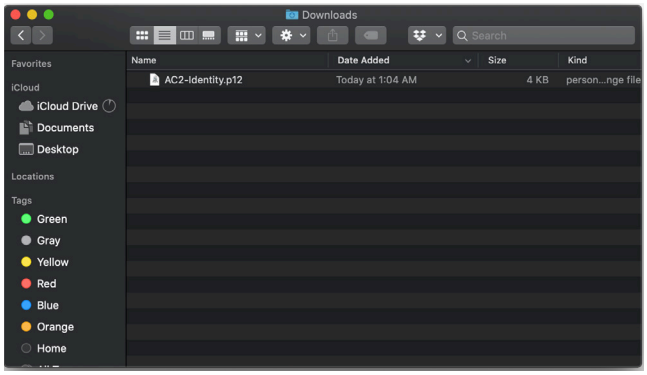
8. Enter details for Display Name, Password, and Verify Password. Keep track of this password. It will be used in a later step.
9. Click Next.



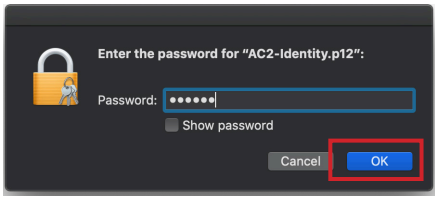
10. Click the Download button. This will download the Supervision Identity to the Downloads folder.
11. Click Save.



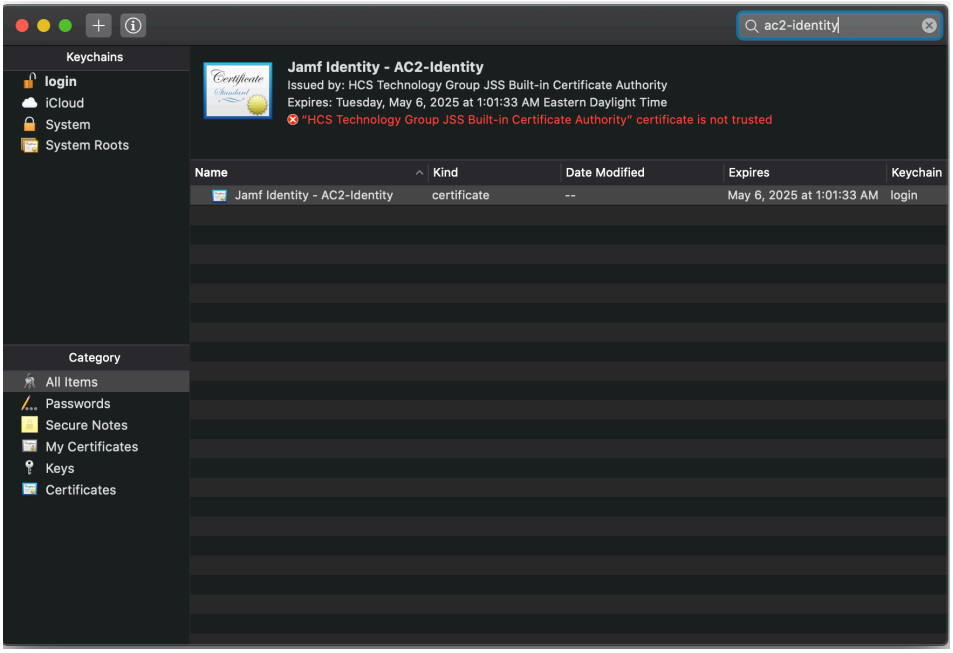
12. Log out of Jamf Pro.
13. Open your Downloads folder and double-click the Supervision Identity downloaded in the earlier step.



14. Enter the password created in Jamf Pro and click OK.



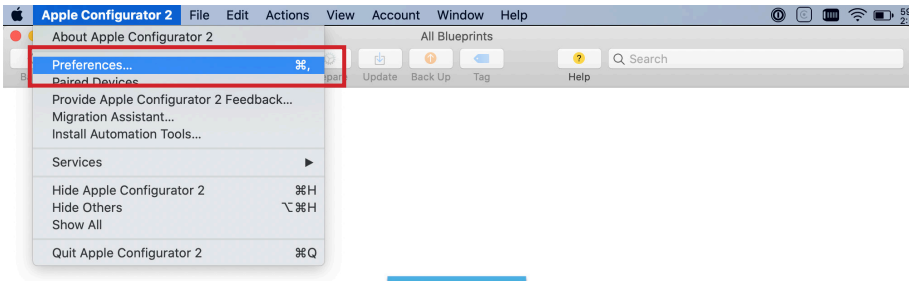
15. Observe the new Supervision Identity in Keychain Access.



16. Quit Keychain Access.

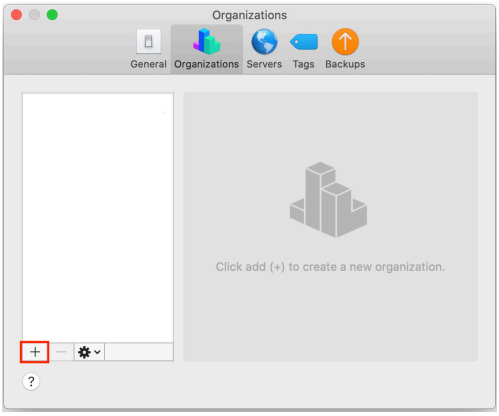
Section 4: Create an Organization and Import Supervision Identity

1. Open Apple Configurator 2.
2. Select the Apple Configurator 2 menu and choose Preferences.

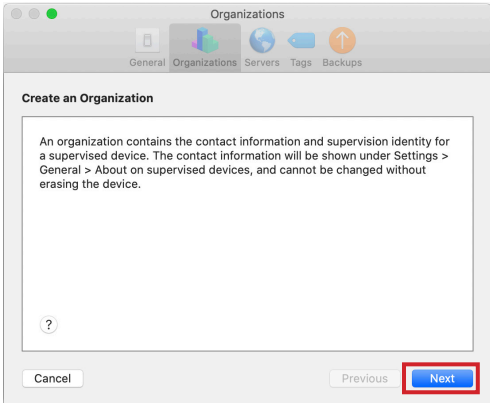


Supervised iPad Devices

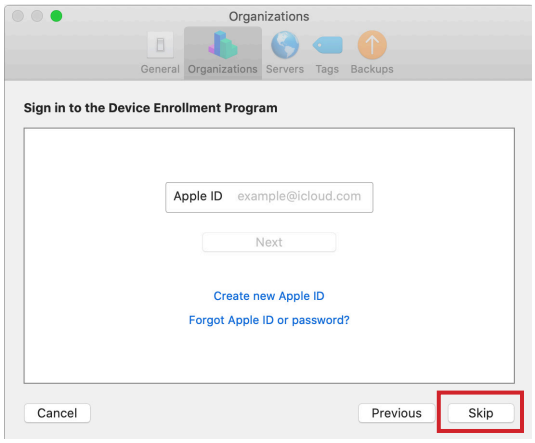
3. Select the Organizations pane.
4. Click Add (+) to Create an Organization.



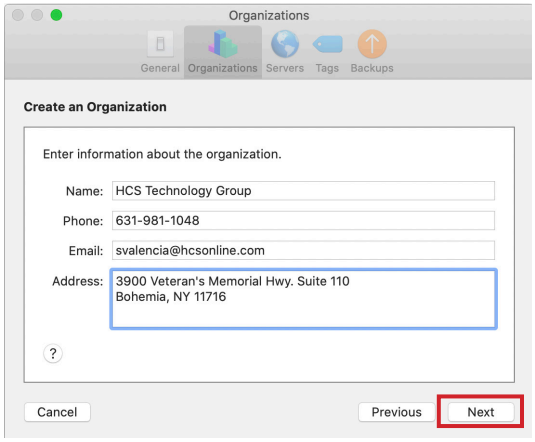
5. Read the information and click Next.



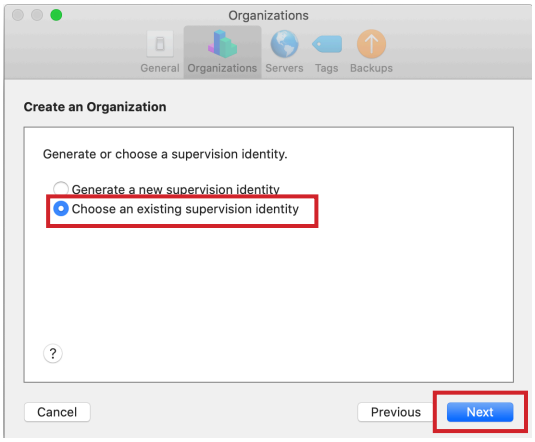
6. You can choose to sign in to the Device Enrollment Program. Click Skip.



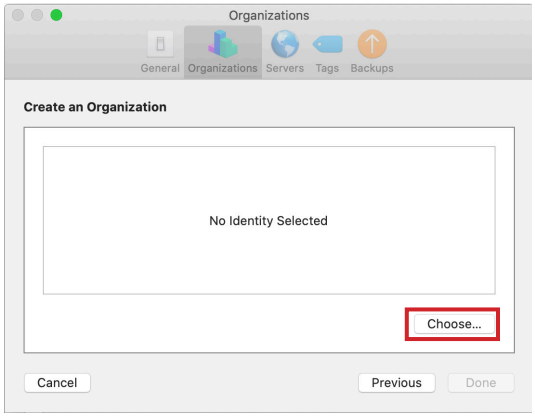
7. Enter the information relevant to your organization and click Next.



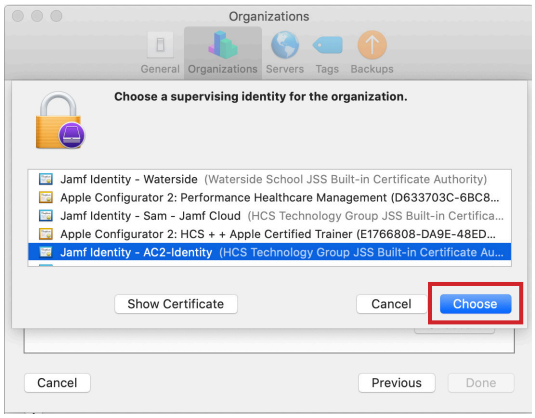
8. Select to Choose an existing supervision identity.
9. Click Next.



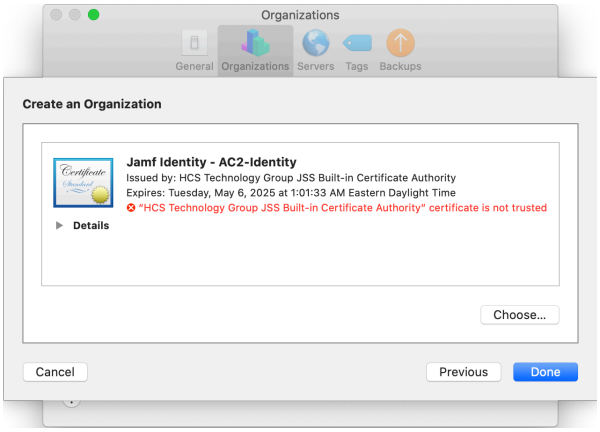
9. Click the Choose button.



10. Select the Supervision Identity created in Jamf Pro earlier and click Choose.



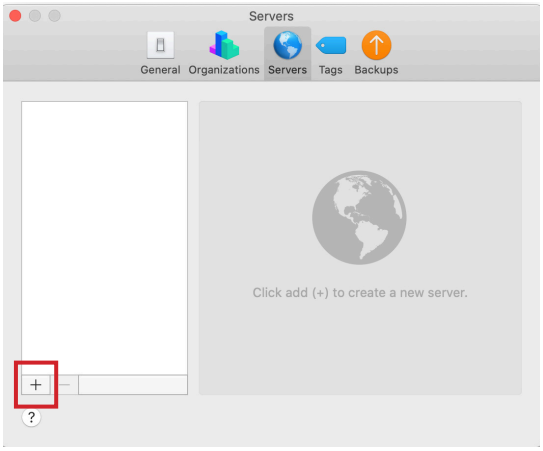
11. Click Done.



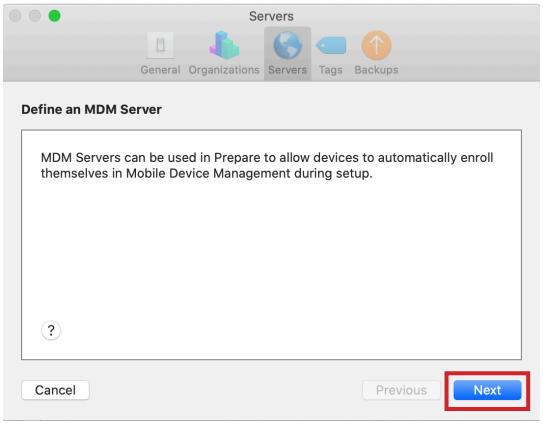
Section 5: Adding an MDM Server

Devices can be enrolled into an MDM as part of the Prepare phase.

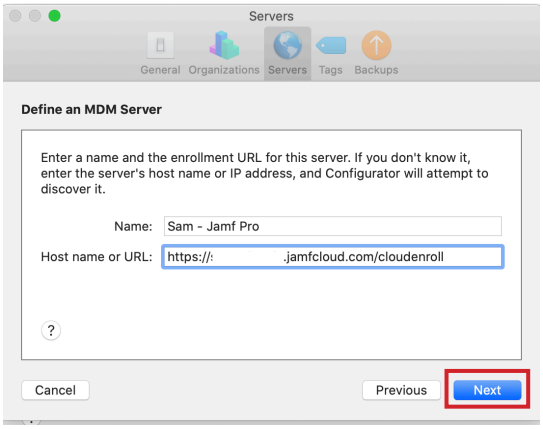
1. Open Apple Configurator 2.
2. Select the Apple Configurator 2 menu and choose Preferences…
3. Select the Servers pane.
4. Click Add (+).



5. At the Define an MDM Server window, click Next.



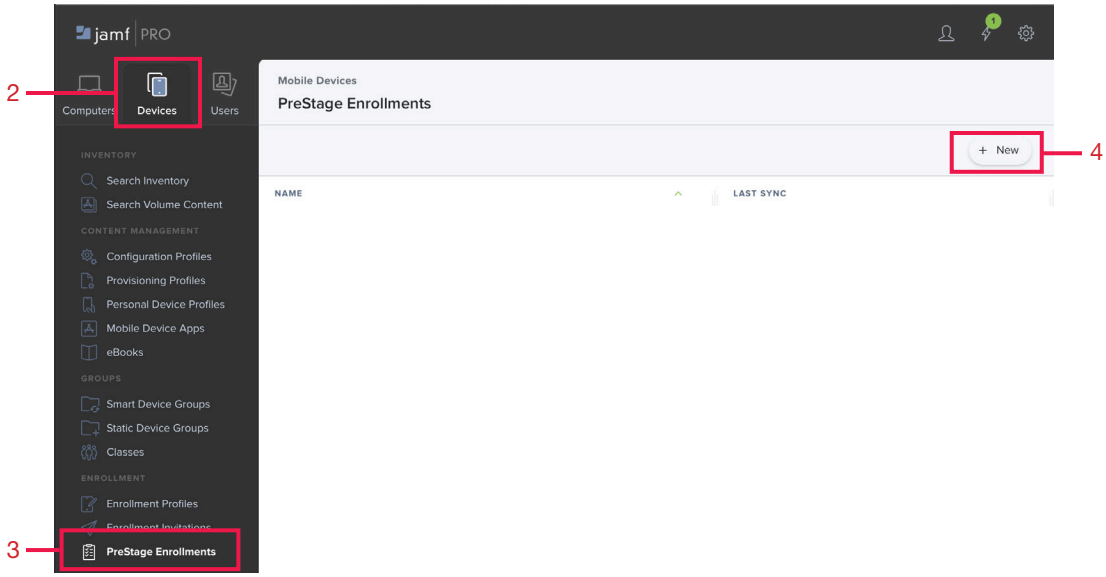
6. Enter a friendly name and enrollment URL from your MDM solution. Click Next.



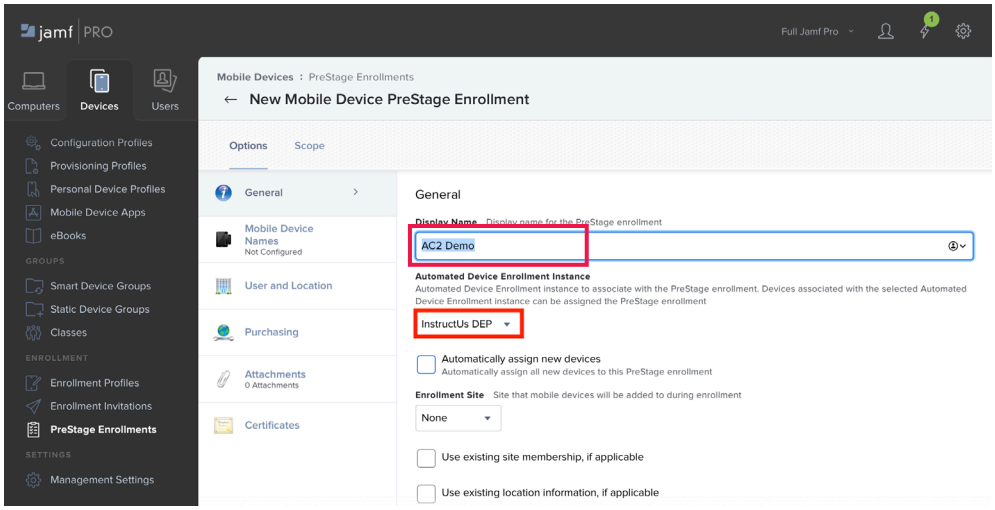
Section 6: Provision Devices for Automated Device Enrollment

This guide focuses on using Apple Configurator 2. It's outside the scope of this guide to configure your organization's MDM solution for Automated Device Enrollment. As an example, this guide uses Jamf Pro, which uses the concept of PreStage Enrollments to enable Automated Device Enrollment for comptuers and devices.

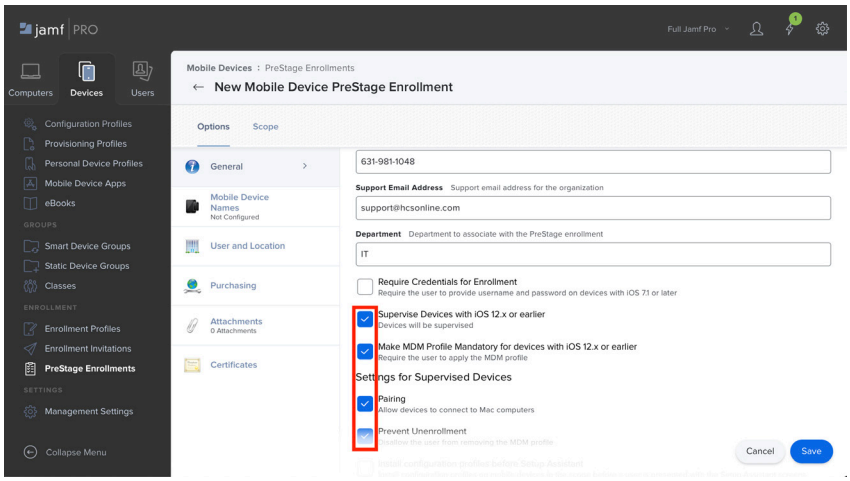
1. Log in to Jamf Pro.
2. In the upper-left corner, click Devices.
3. In the sidebar, click PreStage Enrollments.
4. In the upper-right corner, click New.



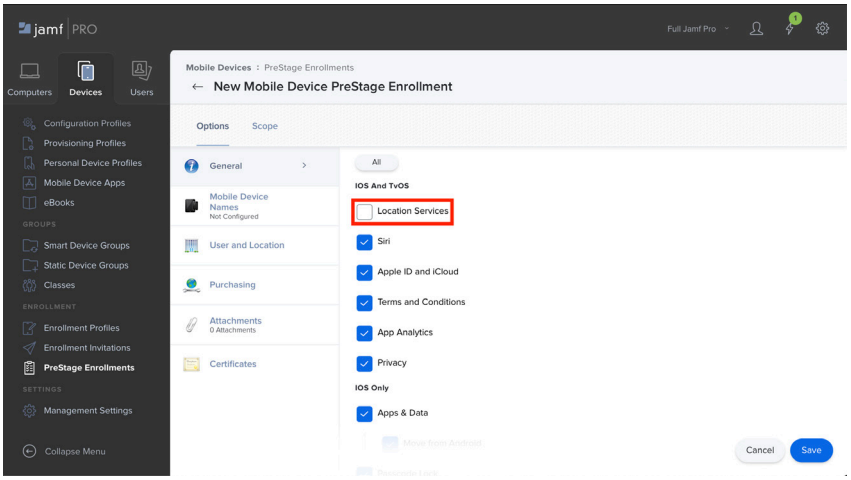
5. In the Display Name field, enter an appropriate value. This guide uses **AC2 Demo** as an example.
6. If your organization has more than one Automated Device Enrollment instance, click the Automated Device Enrollment menu and choose an appropriate instance.



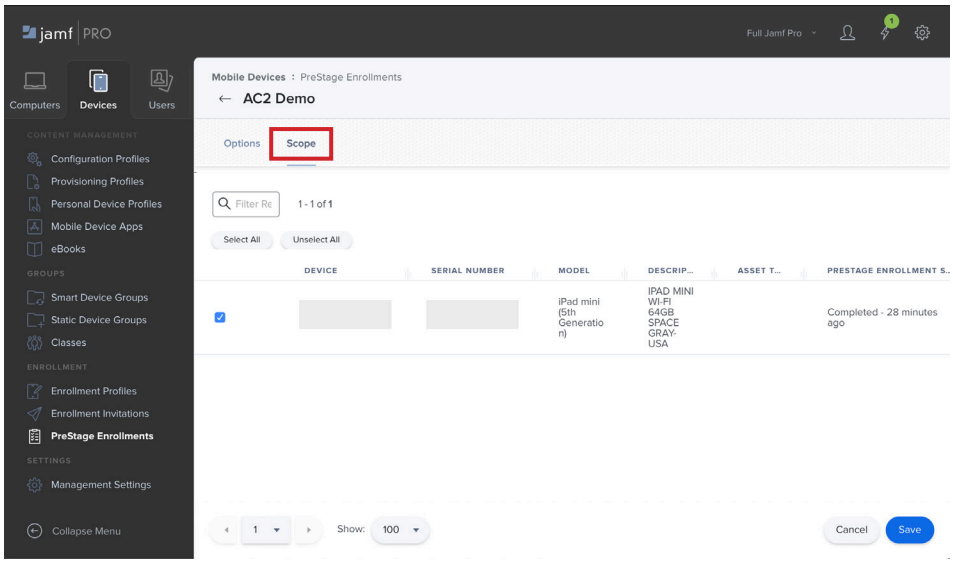
7. Configure the rest of the PreStage Enrollment with appropriate settings. We recommend that you select the checkbox for each of the following options:
   - Supervise Devices with iOS 12.x or earlier
   - Make MDM Profile Mandatory for devices with iOS 12.x or earlier
   - Pairing
   - Prevent Unenrollment



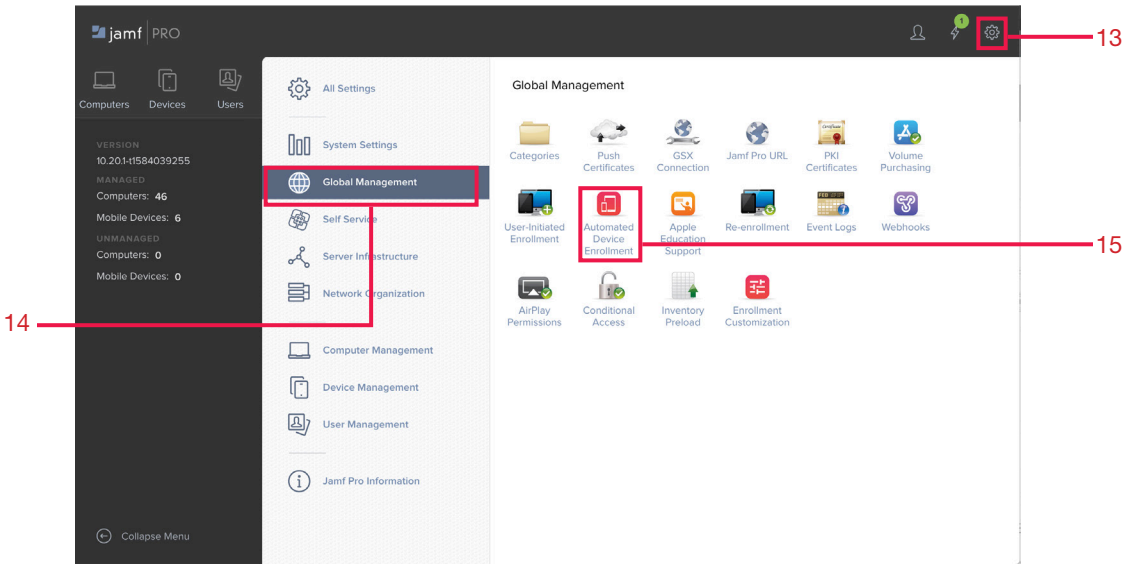
8. In the "iOS and TvOS" section, click All.
9. Deselect the checkbox for the option "Location Services." We recommend that you display the Location Services screen to a user because a user must opt-in to Location Services in order for your iPad to turn on Location Services.



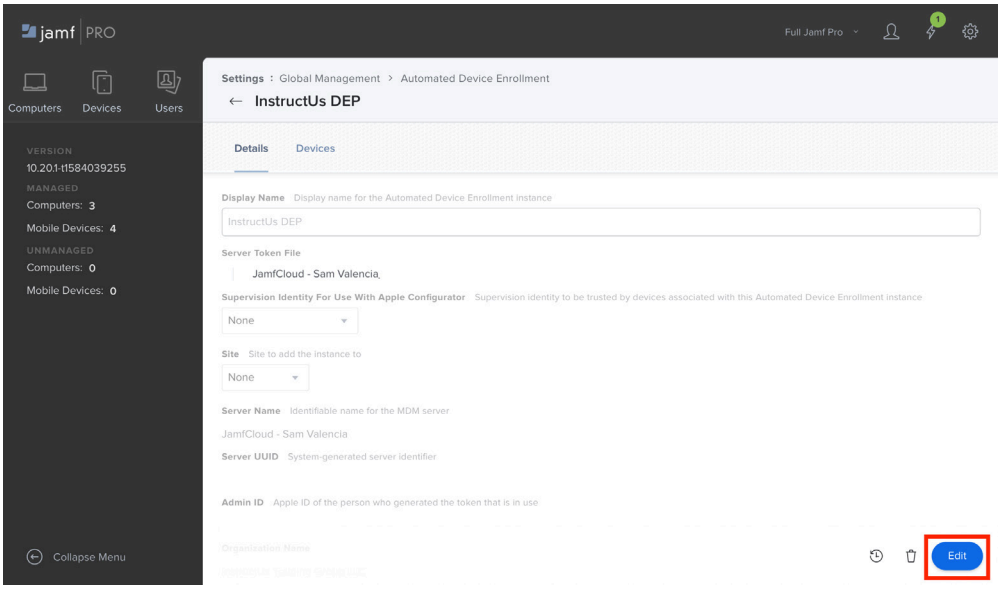
10. Click on the scope tab.



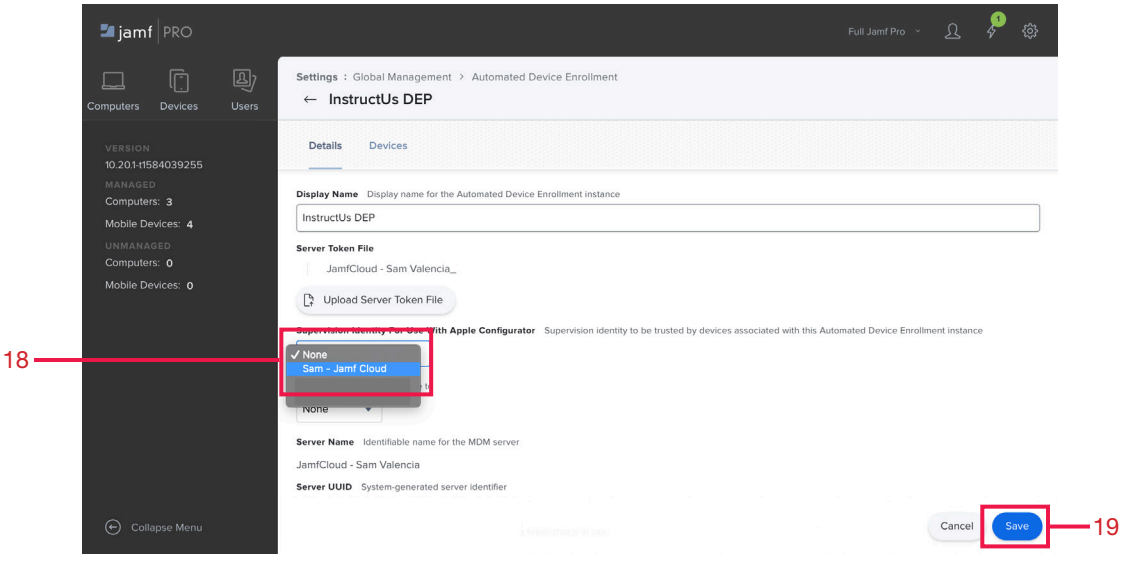
11. Make sure your iPad device(s) are selected in the scope.
12. Click Save.
13. Click on Settings.
14. Click on Global Management.
15. Automated Device Enrollment.



16. Select your Automated Device Enrollment instance.
17. Click Edit.



18. Select the Supervision Identity created in the earlier section.
19. Click Save.



20. Log out of Jamf Pro.

Section 7: Create a Blueprint

Blueprints allow predefined actions that can be applied to connected devices. In this section you will create a Blueprint to do the following:

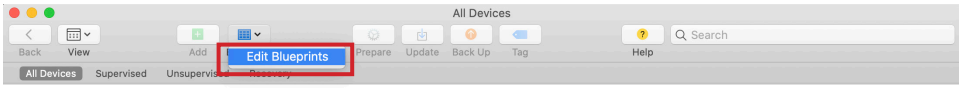
- Name devices
- Set each iPad to display its serial number and a QR code of its serial number on its lock screen, to help with inventory tasks
- Restore devices
- Deploy apps in volume from Apps and Books

A device can be supervised in one of two ways: over-the-air supervision from Automated Device Enrollment, or over USB, using Apple Configurator 2. Although you'll use Apple Configurator and USB to provision your devices, the workflow will use Automated Device Enrollment, so the supervision will be considered to be applied over-the-air.

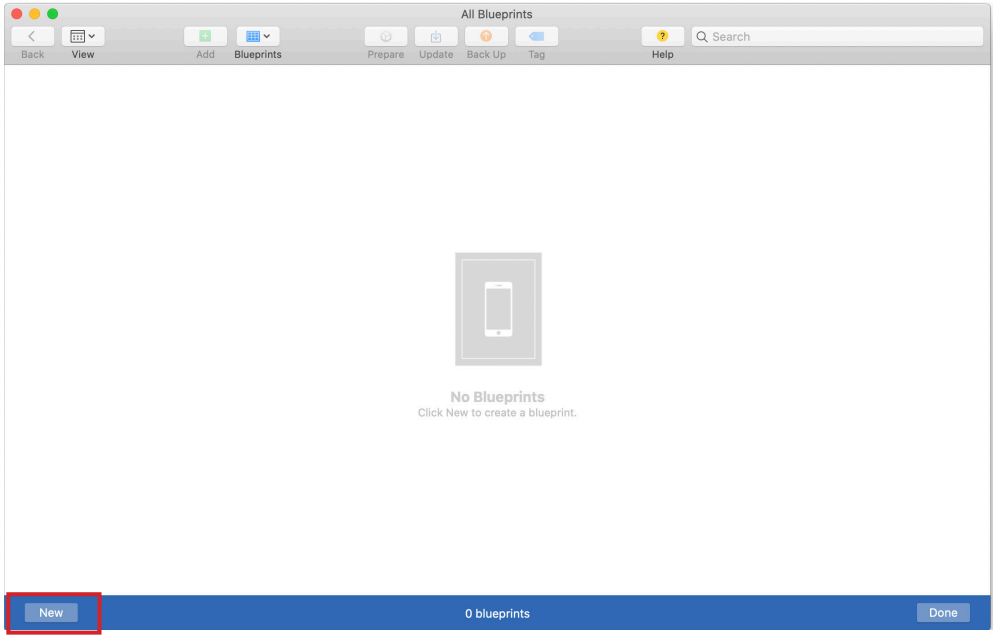
NOTE: If an iOS, iPadOS, or tvOS device has already been activated, the device must be wiped before supervision can occur. The device used in this guide has been restored to factory defaults.

Create and Prepare a Blueprint

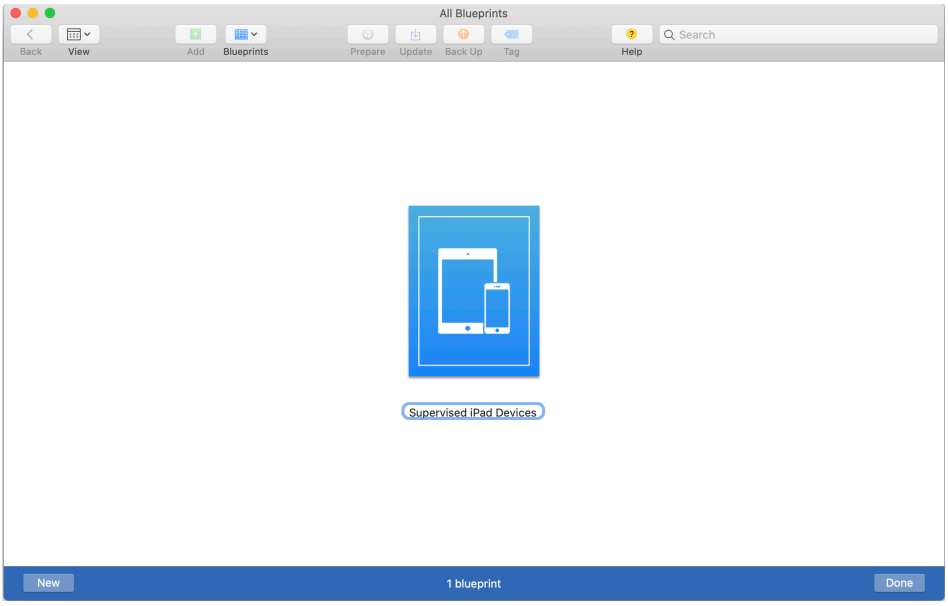
1. In the Apple Configurator 2 toolbar, click Blueprints and choose Edit Blueprints.



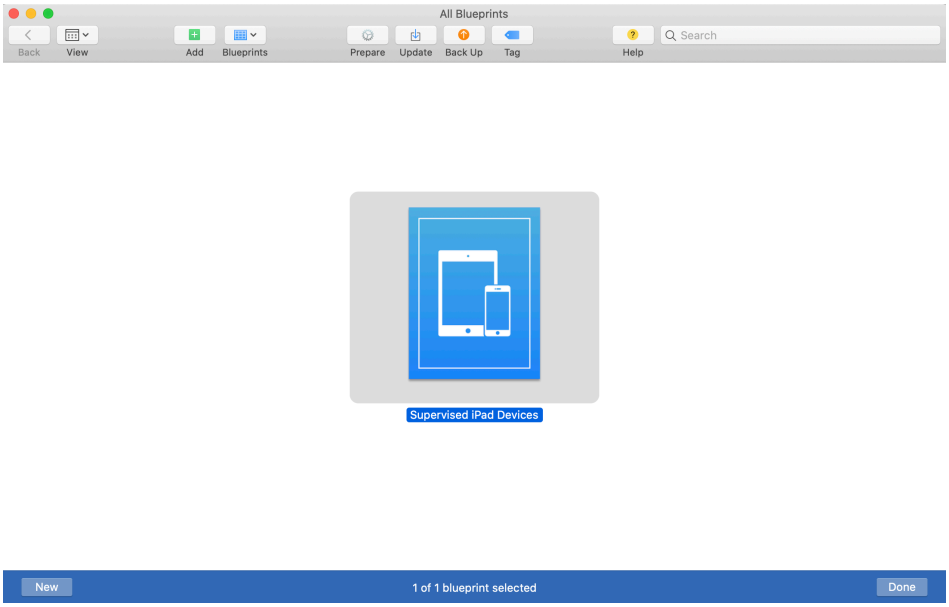
2. In the lower-left corner, click New.



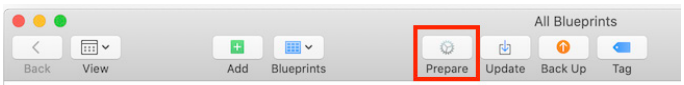
3. Under the new Blueprint icon, enter a name for the Blueprint then press Return. This guide uses **Supervised iPad Devices** as an example.



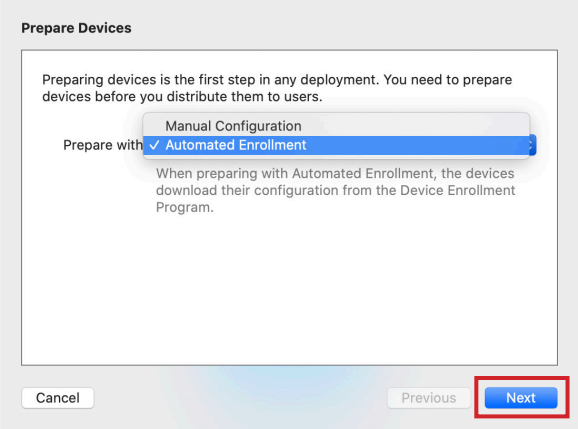
4. Click your newly-created Blueprint to select it.



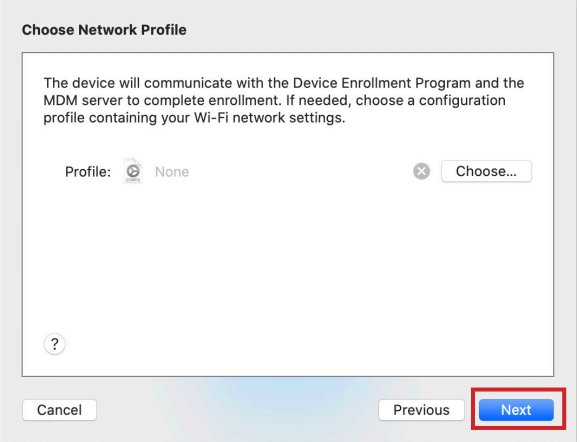
5. In the toolbar, click Prepare.



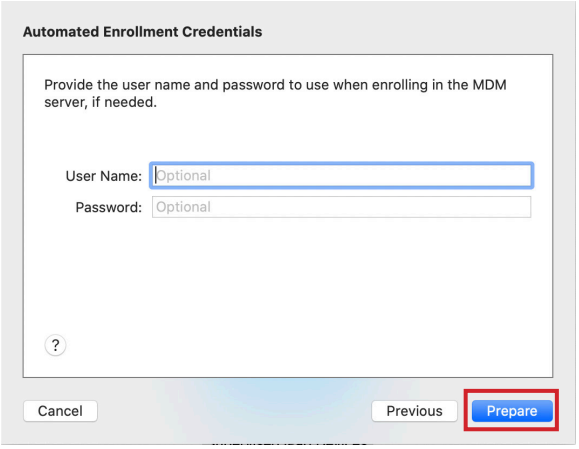
6. In the Prepare Devices screen, click the "Prepare with" menu and choose Automated Enrollment.
7. Click Next.



8. In the Choose Network Profile screen, click Next. Because you're using tethered caching, you don't need to create or install a Wi-Fi profile.



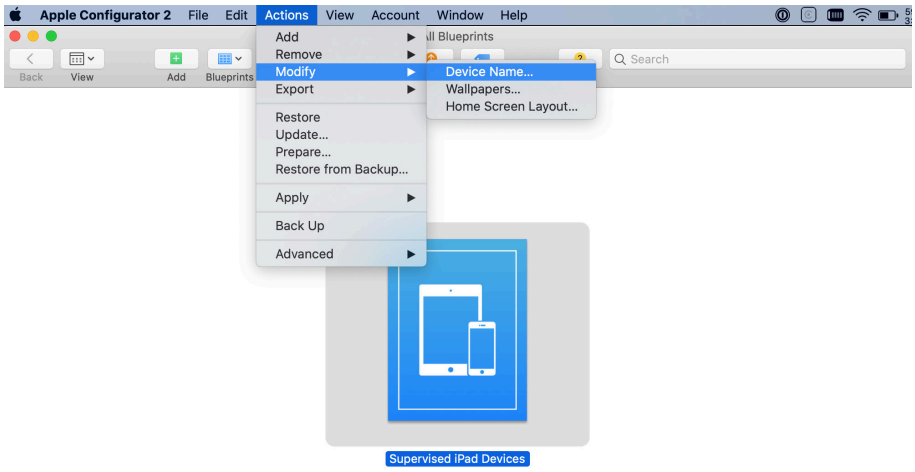
9. In the Automated Enrollment Credentials screen, leave the fields blank then click Prepare. Although it is possible to enter user credentials, this guide leaves the credentials blank as an example.
10. Click Prepare.



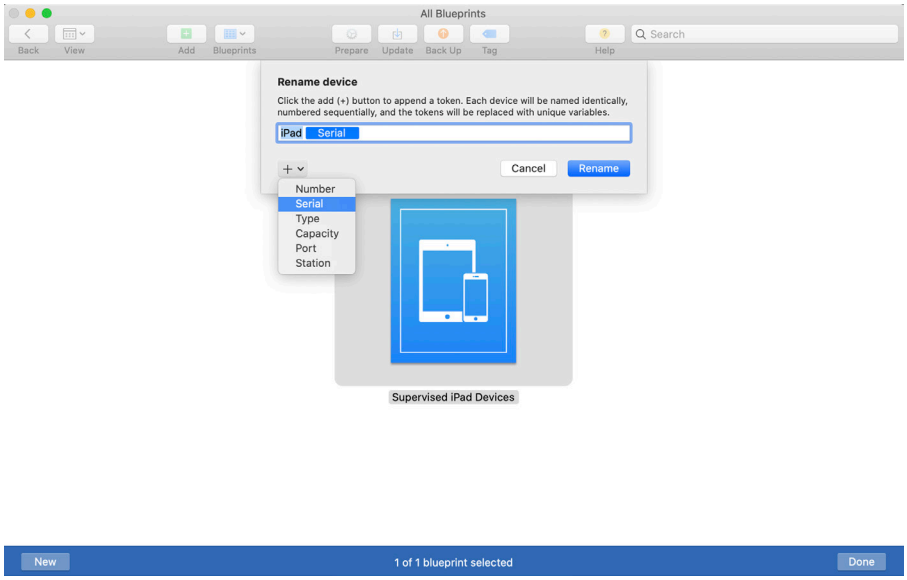
Change the name and Wallpaper

You can use Apple Configurator 2 to use a static value or dynamic values based on hardware identifiers on the device (ie. iPad-SerialNumber). Here, you'll use both.

1. In Apple Configurator 2, if your Blueprint isn't already selected, click it to select it.
2. Click the Actions menu and choose Modify > Device Name.

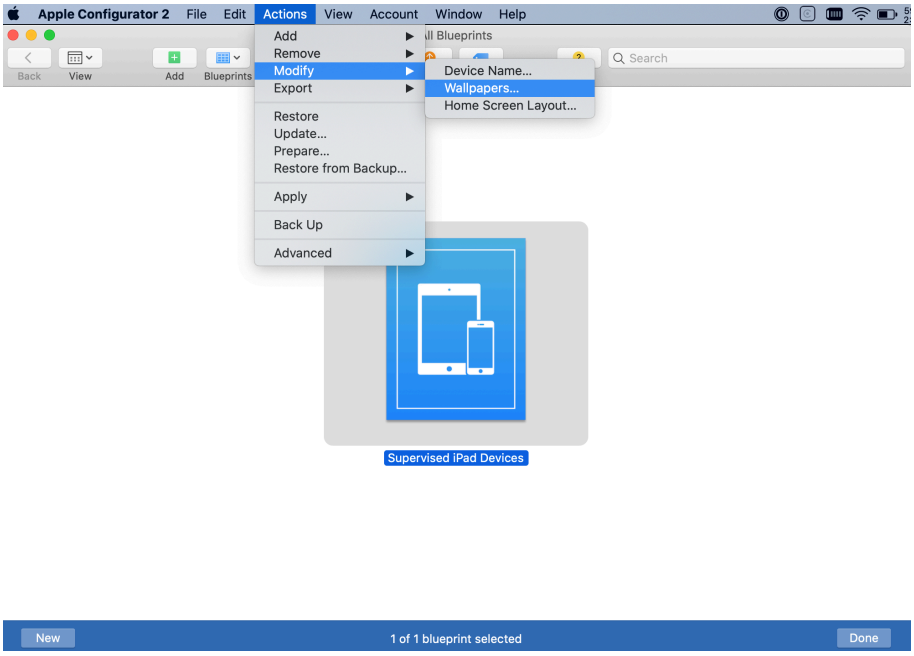


3. Enter the word **iPad**.
4. In the lower-left corner, click the Add (+) menu and choose Serial.
5. Click Rename. Apple Configurator 2 displays a progress bar indicating that it is updating the Blueprint.

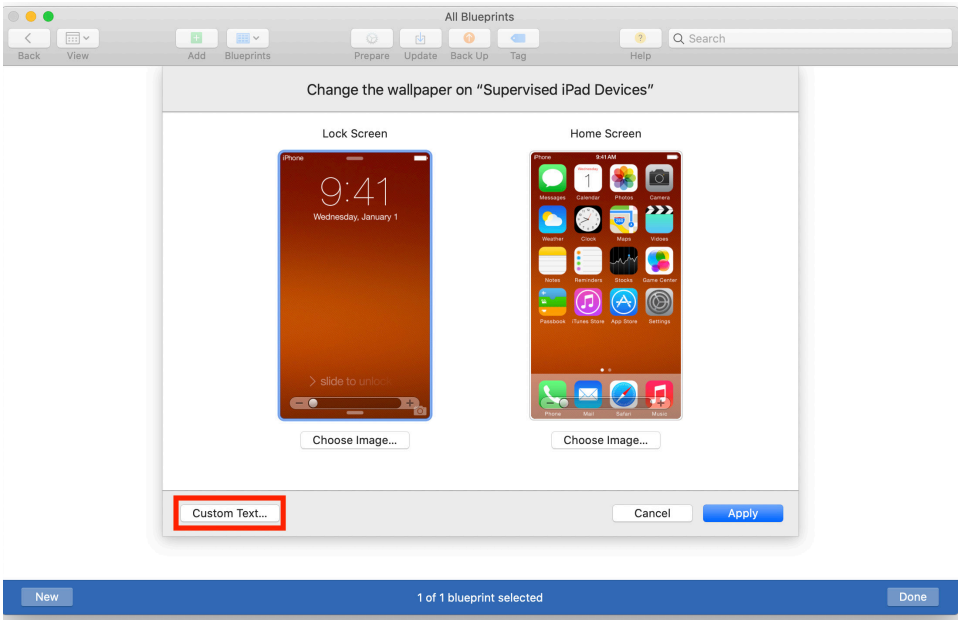


Change Wallpaper

1. In Apple Configurator 2, if your Blueprint isn't already selected, click it to select it.
2. Click the Actions menu and choose Modify > Wallpapers.

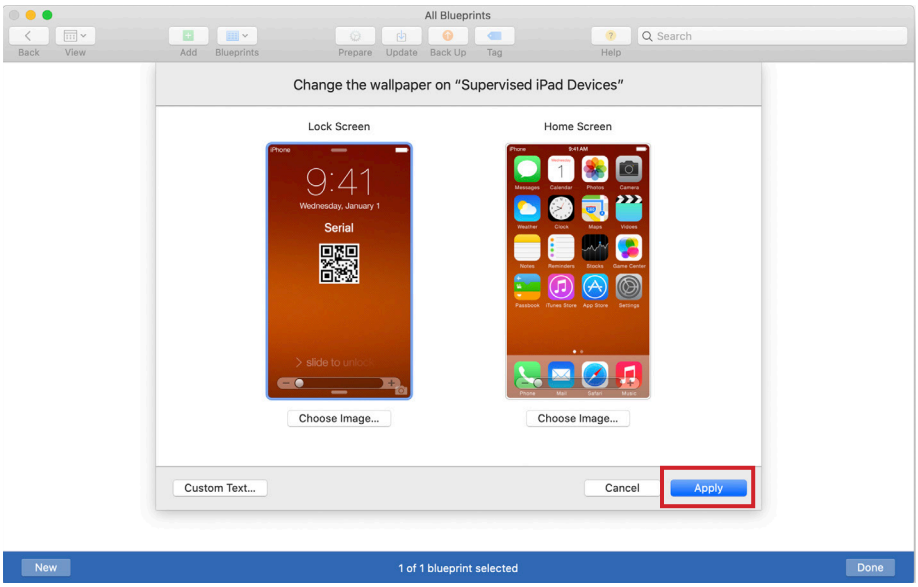


3. Optional: Under the Lock Screen image, click the Choose Image button and follow the prompts to choose an image, or drag an image of your choice over the Lock Screen image.
4. Optional: For the Home Screen image, use the same procedure as the last step.
5. In the lower-left corner, click Custom Text.



6. Select the checkbox for “Display text as QR code”.
7. Click Add then choose Serial.

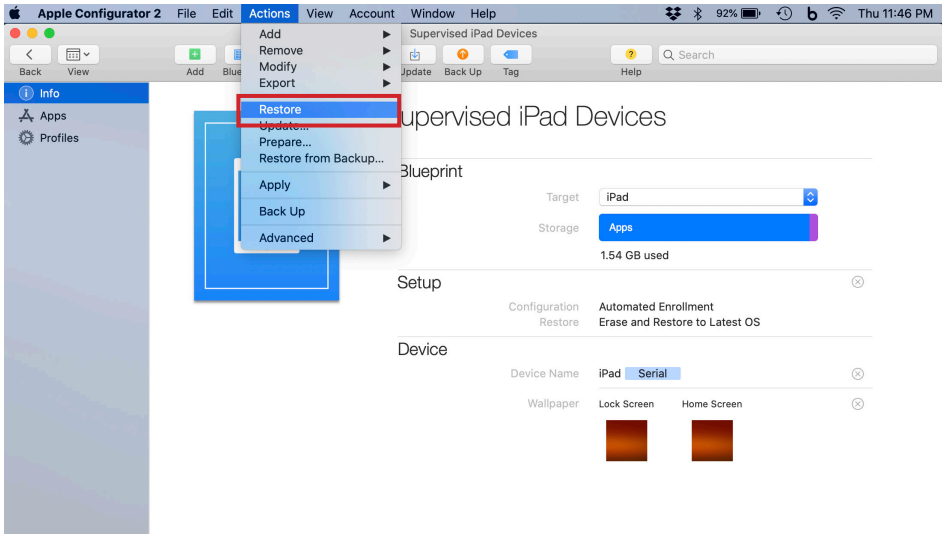
8. Click Done.
9. Confirm that the preview of the lock screen is similar to the following image, specifically, that it includes a QR code.
10. Click Apply to apply these changes to the Blueprint.



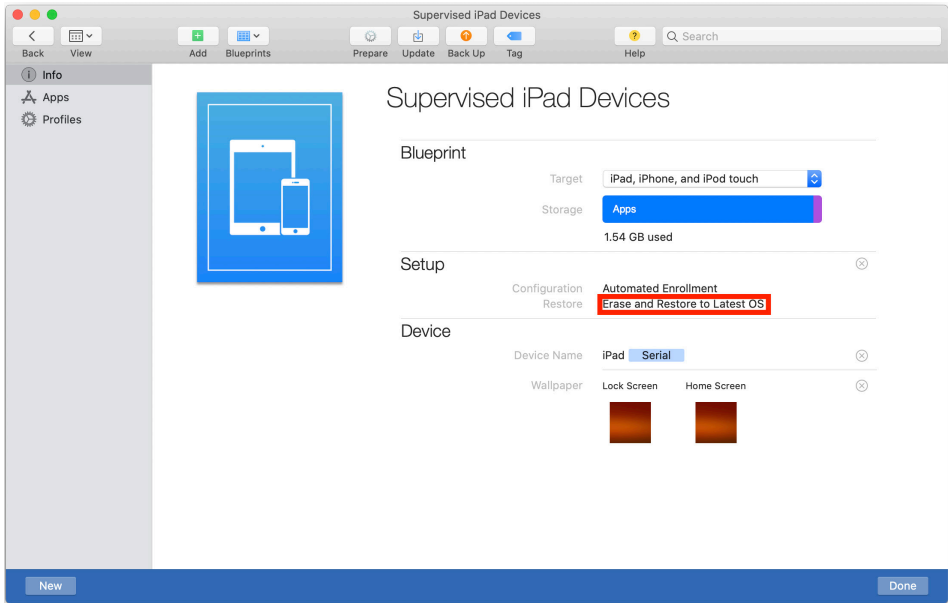
Restore Devices

The Actions menu offers some commands that are very similar. Actions > Restore and Actions > Advanced > “Erase All Content and Settings” both result in a device that seems new and out-of-the-box. Both commands erase all content and settings on the device, including supervision. The “Erase All Content and Settings” command preserves the existing operating system (OS) of the device. In contrast, the Restore command also ensures that the device has the latest available version of the OS for the device. When you use the Restore command, be prepared to wait for Apple Configurator 2 to download the latest available version of the OS the first time you run the Blueprint. If Apple Configurator 2 already downloaded the appropriate version of the OS, it doesn’t need to download again. Double clicking on the Blueprint will reveal the details of the workflow. While in this view, additional and useful changes can be made as well.

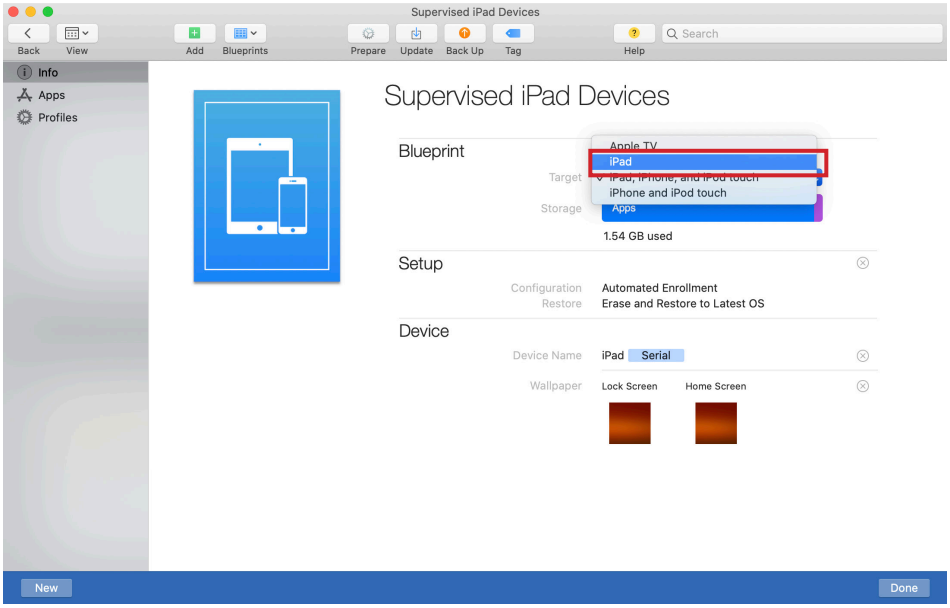
1. Click the Actions menu and choose Restore.



2. Confirm that the Setup section displays “Erase and Restore to Latest OS."



3. In the Blueprint section, click the Target menu and choose iPad. This ensures that you do not accidentally perform the restore operation on the wrong device type.



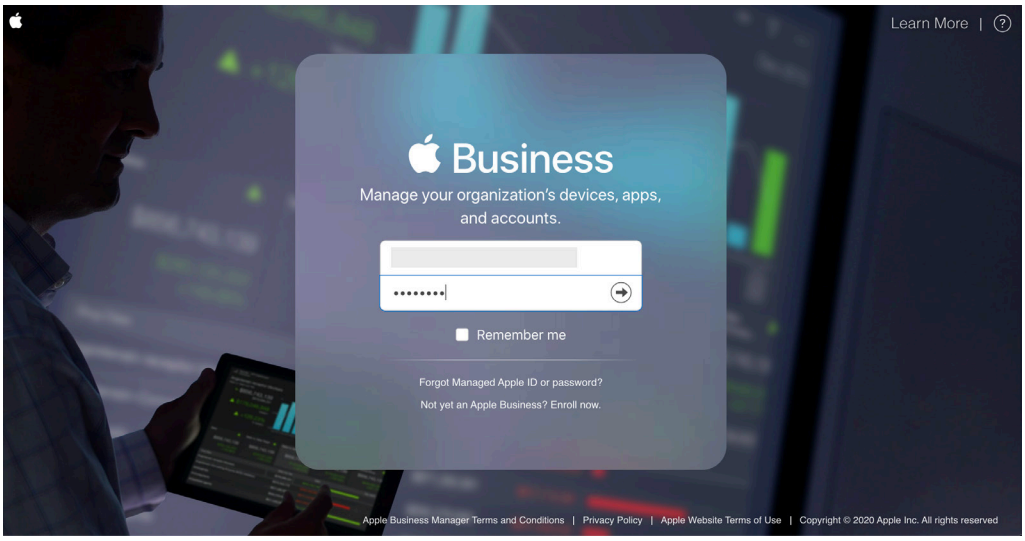
4. Don't click Done yet, because you'll continue editing this Blueprint later in this document.

Section 8: Create a Content Manager account in Apple Business Manager

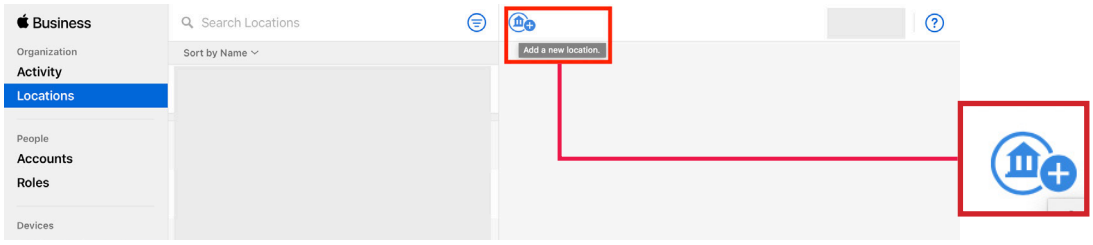
An account will be required within Apple Business Manager that has the ability to purchase volume licenses of apps. The steps below detail creating a Location in Apple Business Manager and creating a Content Manager account assigned to that location. A best practice would be to create a Content Manager account that has access to a specific location.

IMPORTANT NOTE: It is critical to use a token from a location that is different than the one currently used by your production MDM solution, or it may create a conflict over licenses.

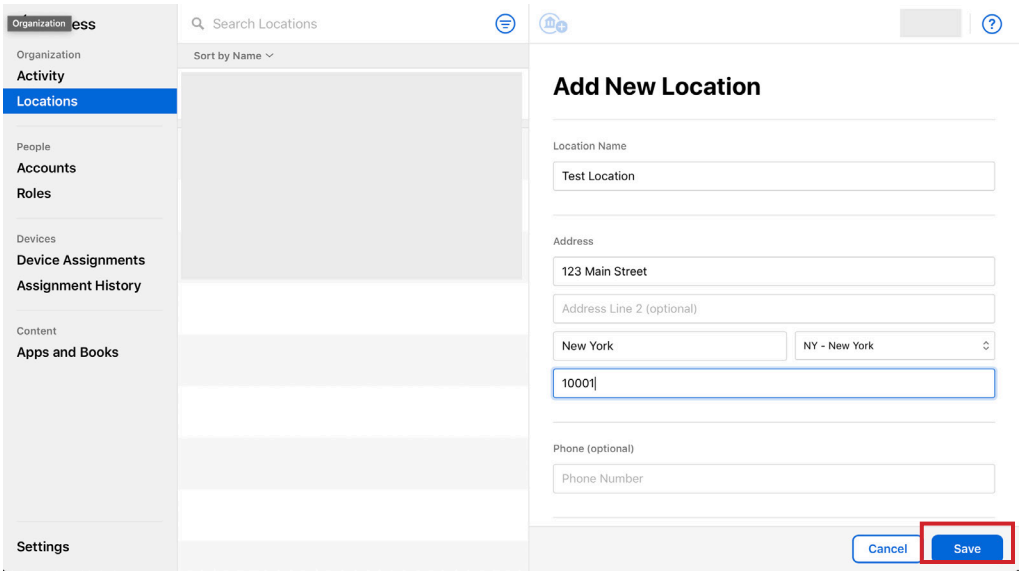
1. Sign in to Apple Business Manager at https://business.apple.com.



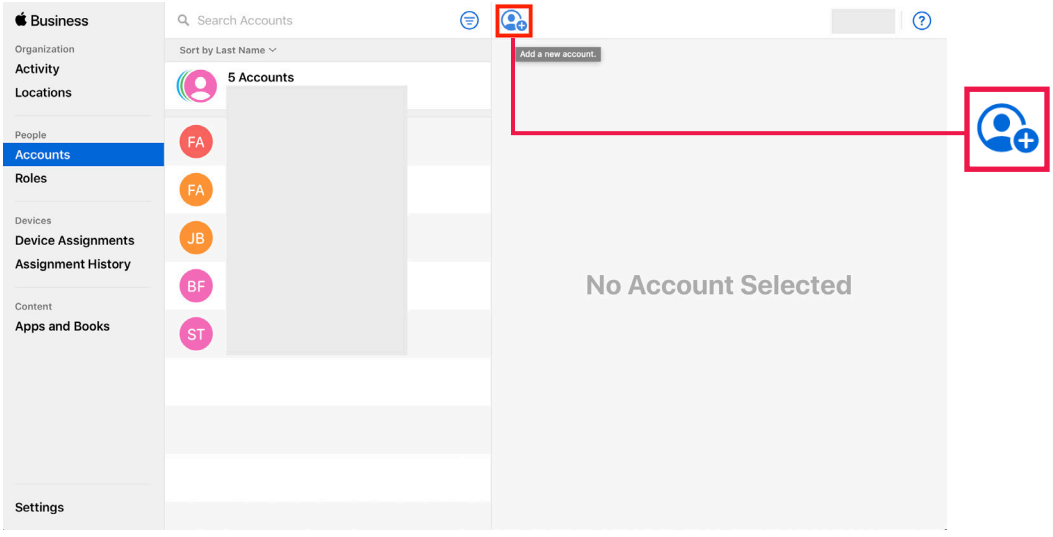
2. In the sidebar, click Locations.
3. click "Add a new location."



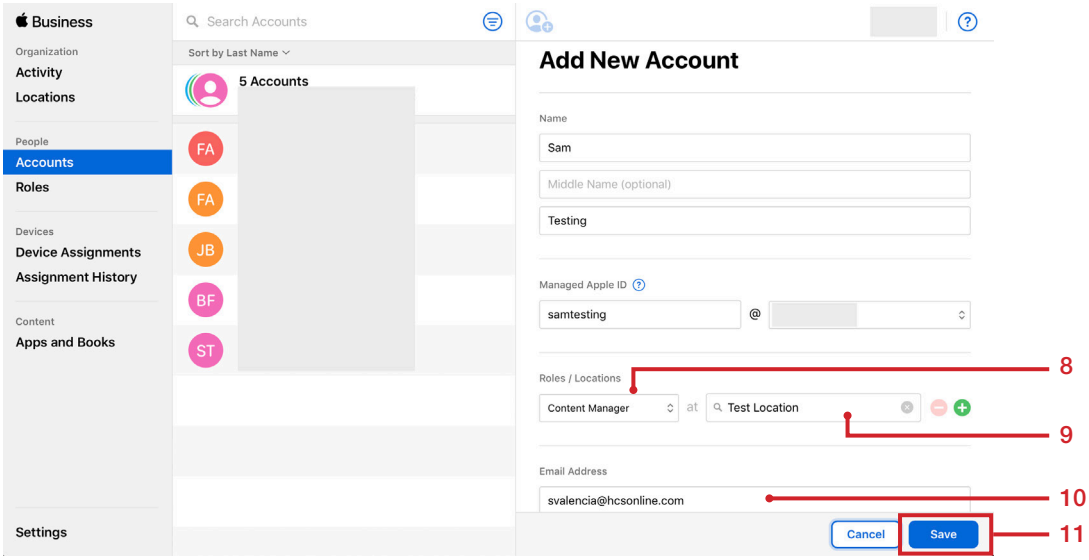
4. Enter relevant location details and click Save.



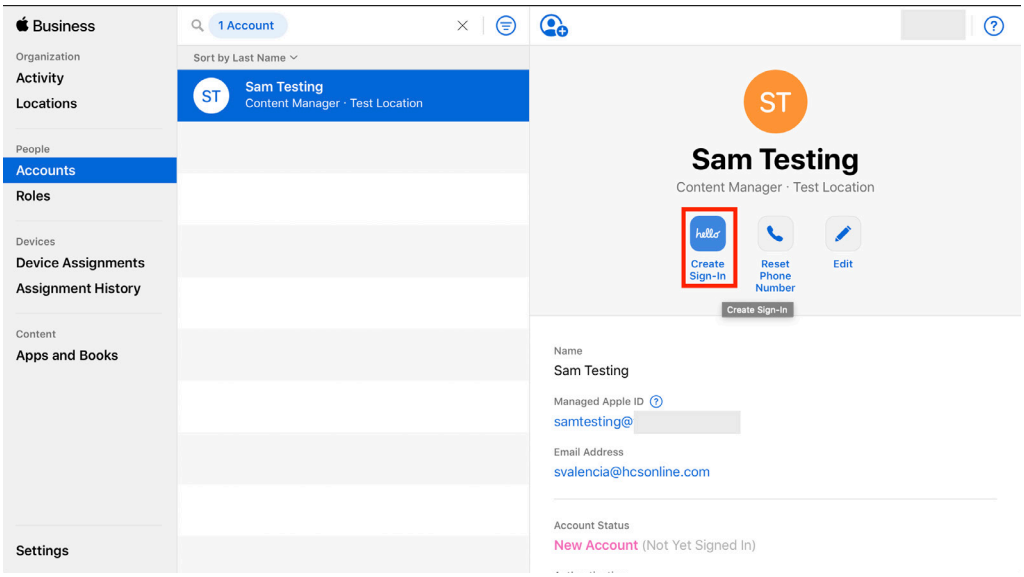
5. In the sidebar, click Accounts.
6. Click "Add a new account."



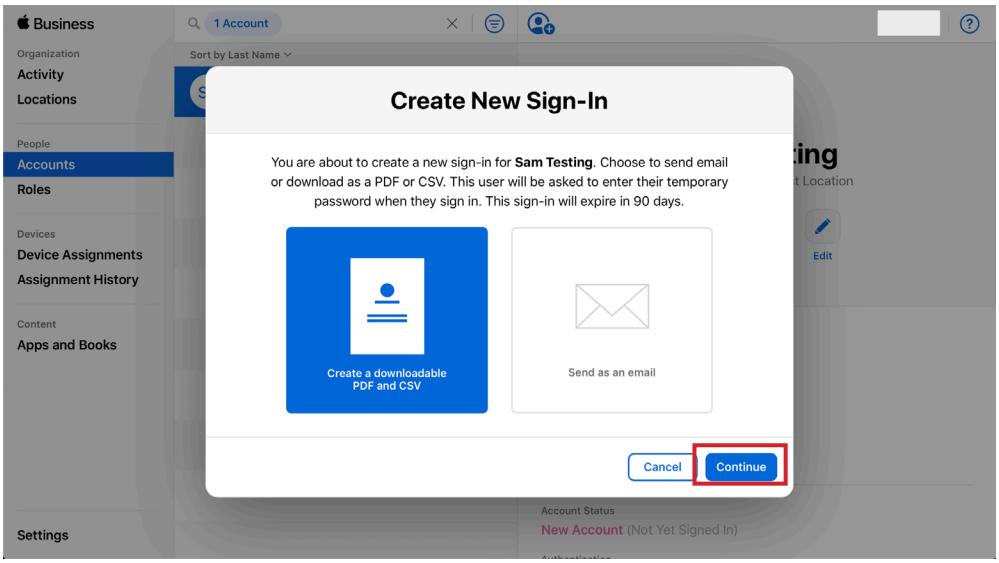
7. Enter relevant account details for the Name and Managed Apple ID sections.
8. Click the Roles menu and choose Content Manager.
9. In the Location field, start entering the name of the location you just created, then choose it from the menu that appears.
10. In the Email Address, enter an appropriate address.
11. Click Save.



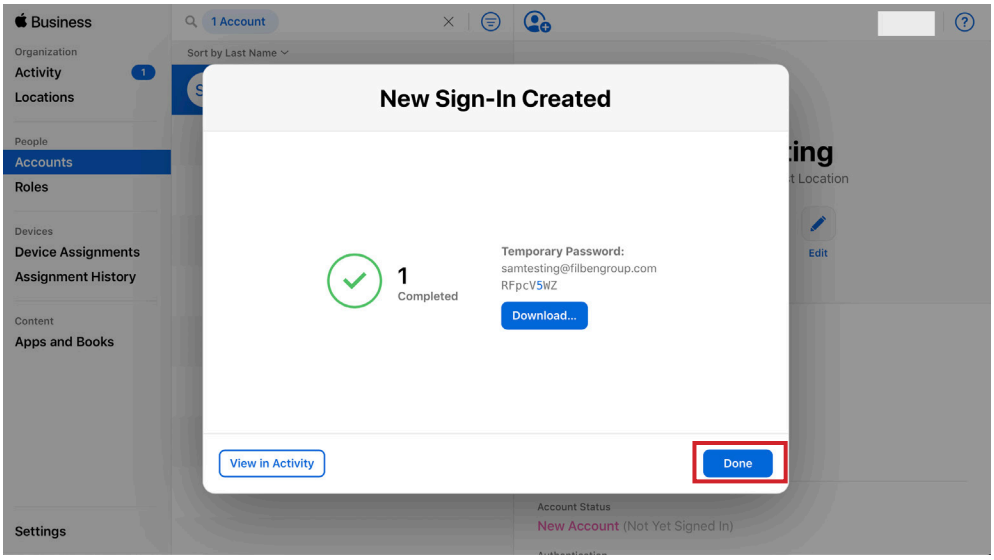
12. After saving, a page will reveal the ability to create a sign in for this new account. Click Create Sign-In.



13. Select one of the displayed options, click Continue. This guide uses "Create a downloadable PDF and CSV" as an example.

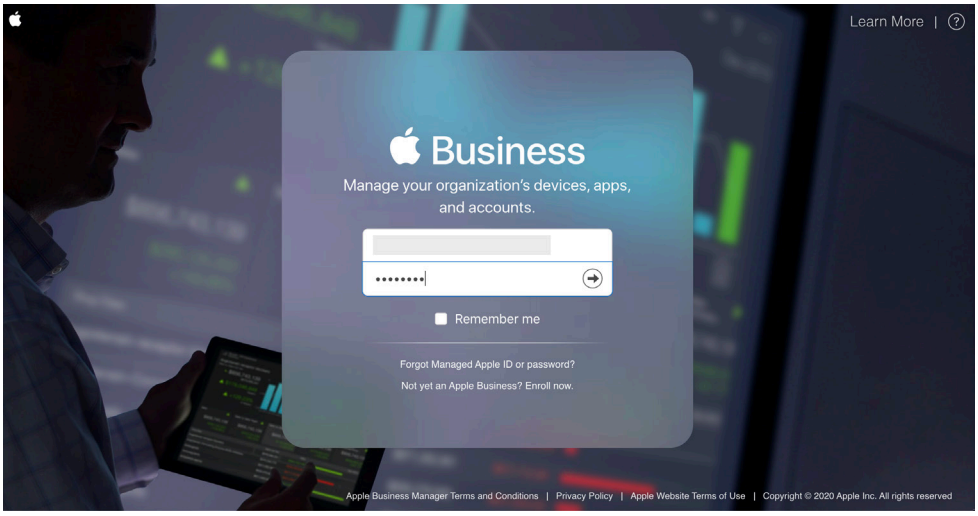


14. Note the temporary password . Optionally, click Download, then select an appropriate file format, then click Done, or just click Done.

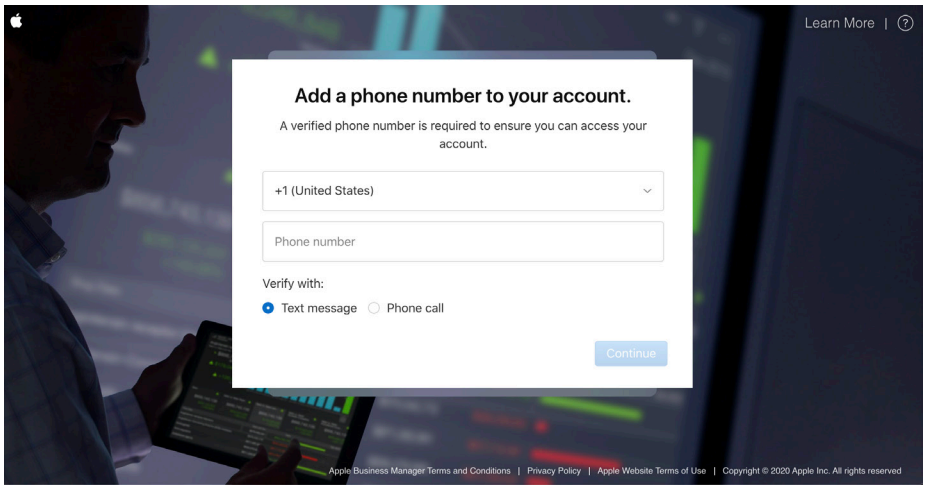


Because you're already signed in to the Apple Business Manager site, in this section you'll use a private window or incognito window to sign in to Apple Business Manager with the Managed Apple ID you just created. If using Google Chrome, go the the File menu and select New Incognito Window. If using Safari, go the the file menu and select New Private Window.

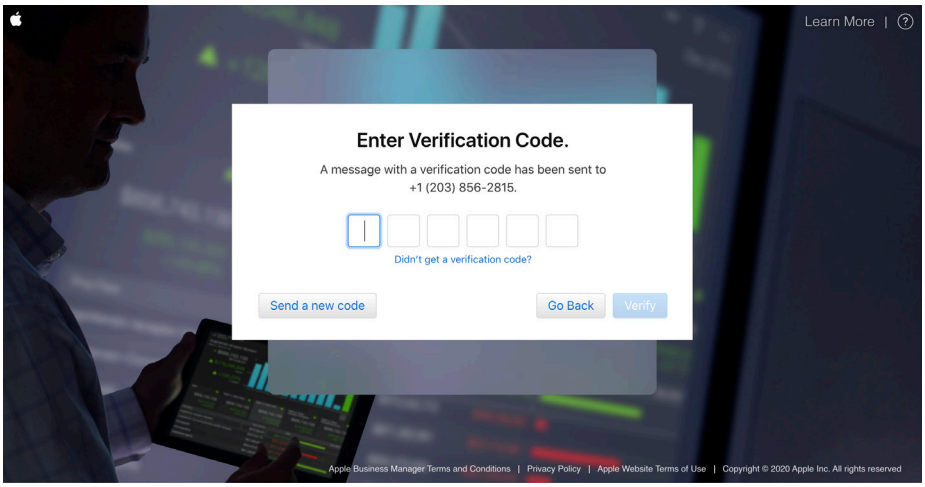
1. In Safari, choose File > New Private Window.
2. Navigate to https://business.apple.com.
3. Sign in to Apple Business Manager using the newly created Managed Apple ID with Content Manager privileges.



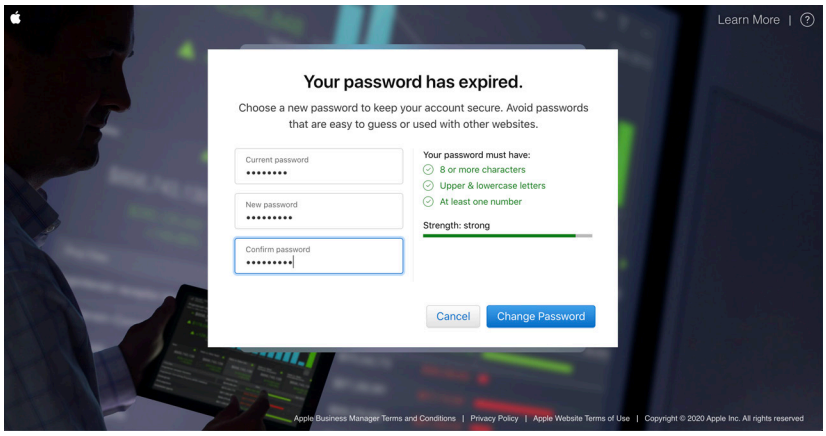
4. Enter a phone number for two-step authentication then click Continue.



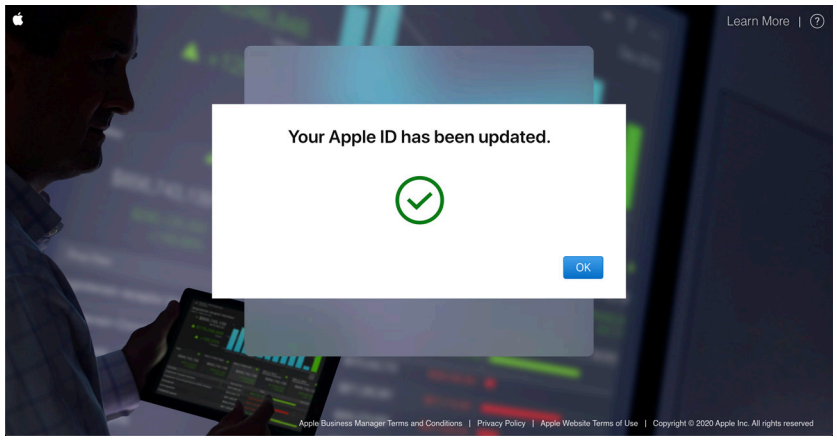
5. Enter the code sent to the phone then click Verify.



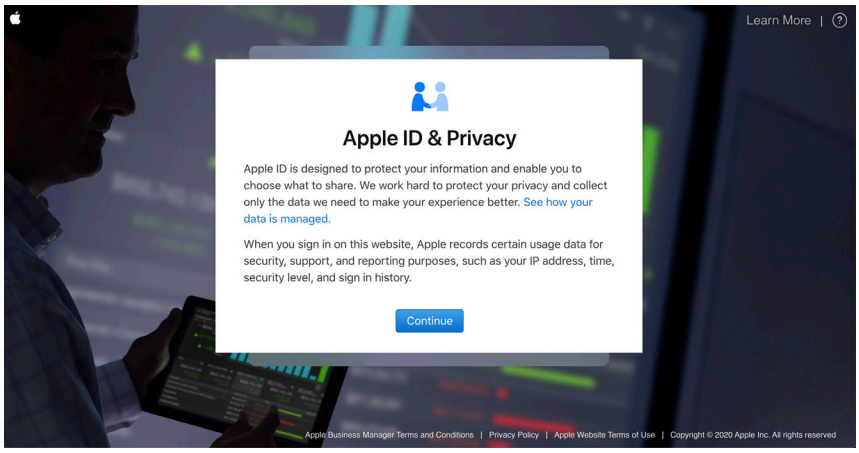
6. When prompted, enter the temporary password, then enter a new secure password, enter the new password again to verify it, then click Change Password.



7. Confirm that the web page displays that your Apple ID has been updated. Click Ok.

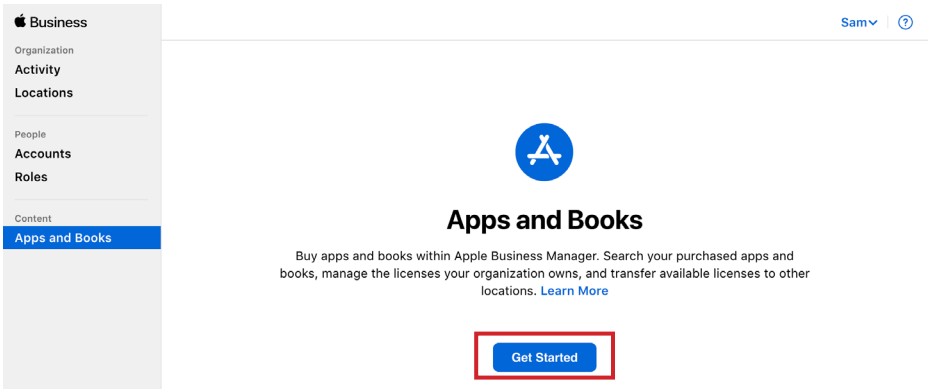


8. Review the Apple ID & Privacy information and click Continue when ready.

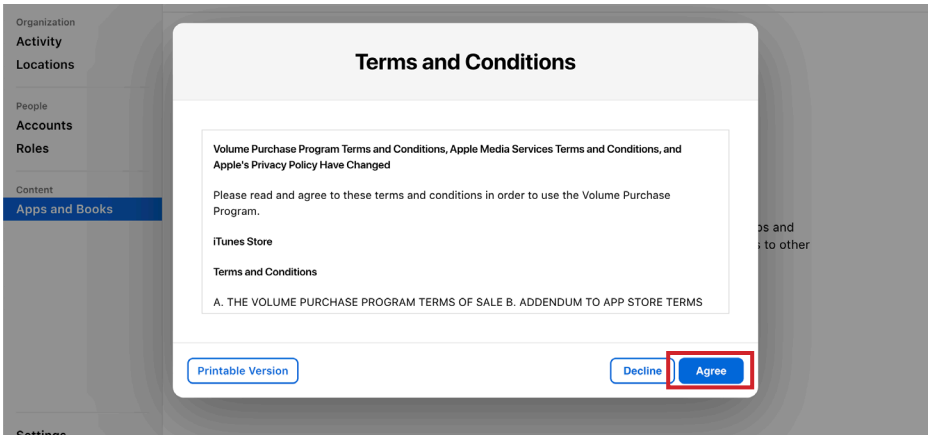


Section 9: Purchase App Store apps

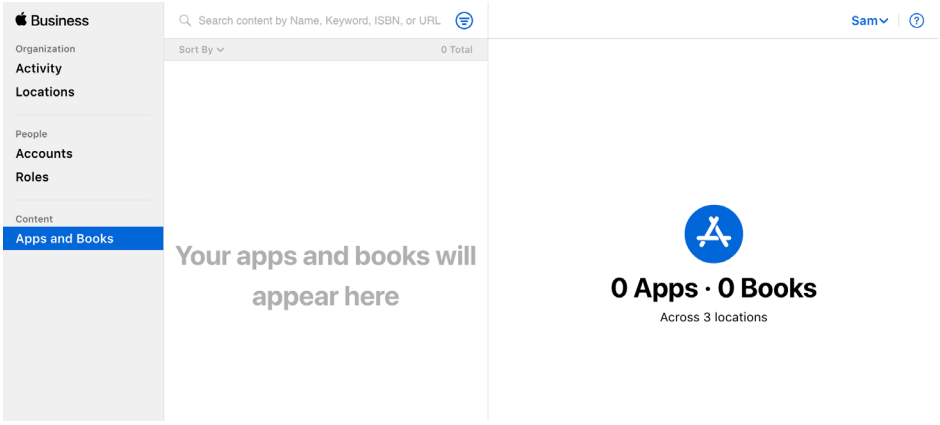
1. In the sidebar, click Apps and Books.
2. Click Get Started to begin the process of allowing this new account to purchase content.



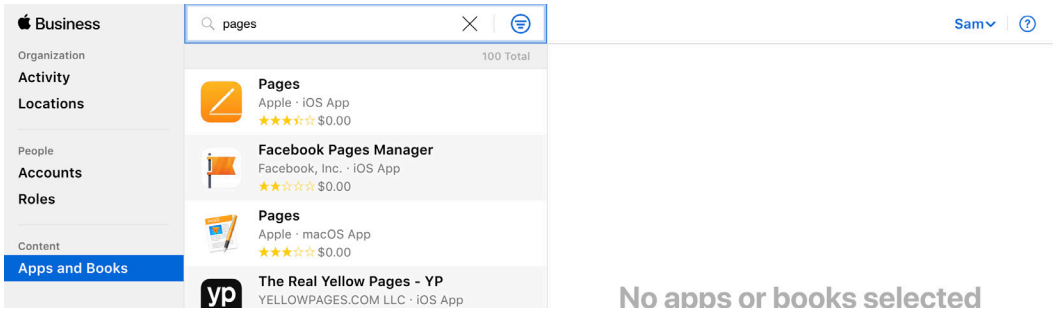
3. Review the Terms and Conditions and click Agree.



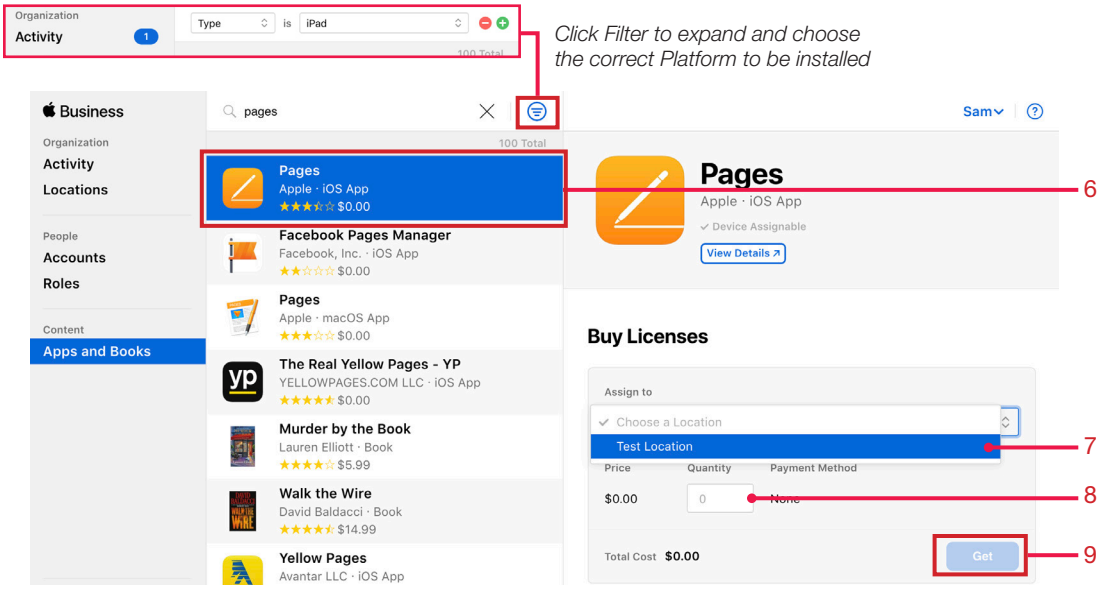
4. Confirm that the right column displays 0 Apps and 0 Books.



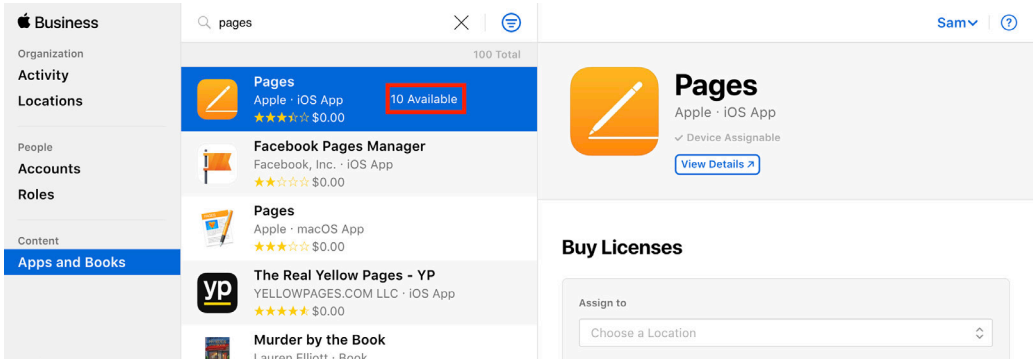
5. Click the search box and enter the name of an app to purchase. This guide uses Pages (a free app) as an example.



6. Find the Pages app for iOS in the list and select it.
   NOTE: Ensure the app for the correct platform (ie. iOS) is selected. Alternatively, the filter button can be used to narrow the search criteria.
7. In the right column, click the "Assign to" menu and choose your location.
8. In the Quantity field, enter a number. This guide uses 10 as an example.
9. Click Get.
10. Optional: Repeat steps 5-9 for any additional apps you'd like.



11. In the center column, confirm that after Apple processed your order for an app, the number of app licenses appears next to the app name.



12. Log out of Apple Business Manager.

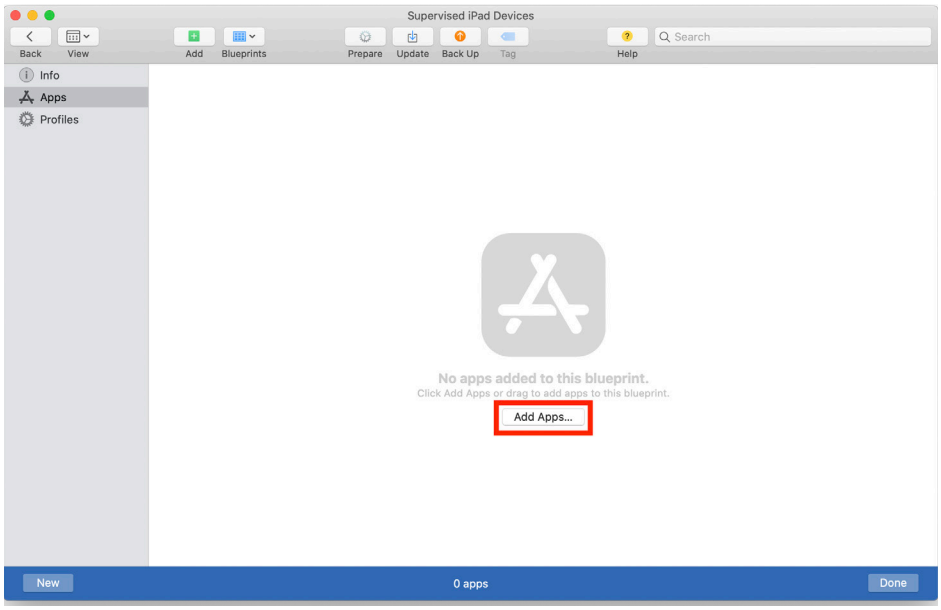
In the next section, Apple Configurator 2 will discover these newly acquired apps.

Section 10: Use Apps and Books

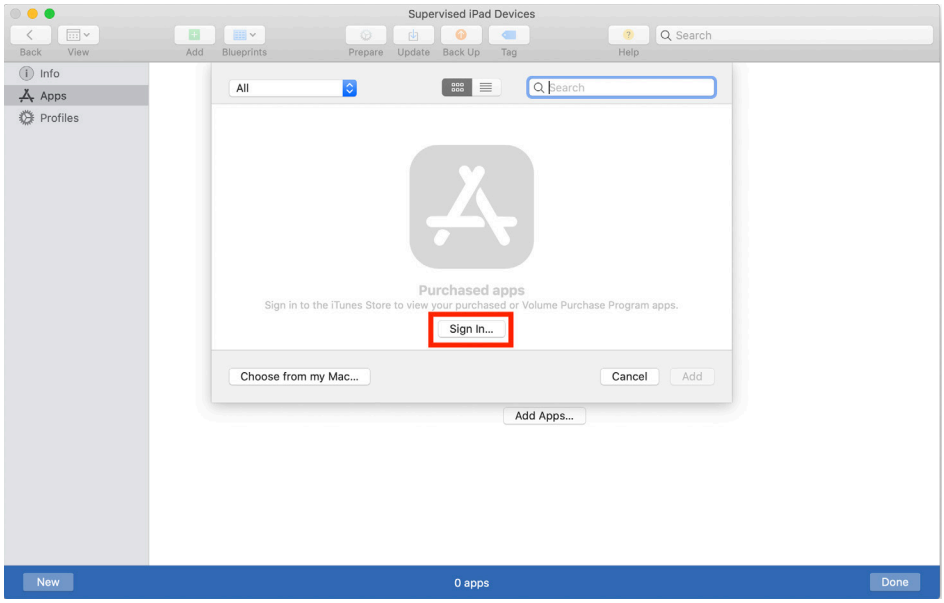
Apple Configurator 2 can leverage volume purchases via Apps and Books in Apple Business Manager. Using this method, apps can be “side loaded” from the App Store on to one or many devices, easing the burden for either IT or an end user during Setup Assistant. This is also an opportunity to use the content caching feature of macOS to cache App Store apps and deploy devices faster. Lastly, after you enroll the device in your MDM solution, your MDM solution can manage the apps that you installed in this section, even though the MDM solution didn't cause the apps to be installed.

1. In the the sidebar, click Apps.

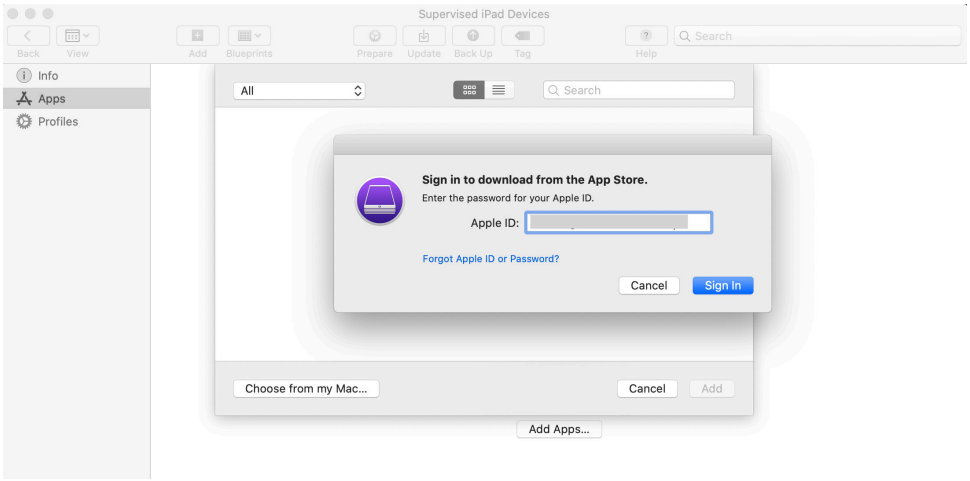
2. Click Add Apps.



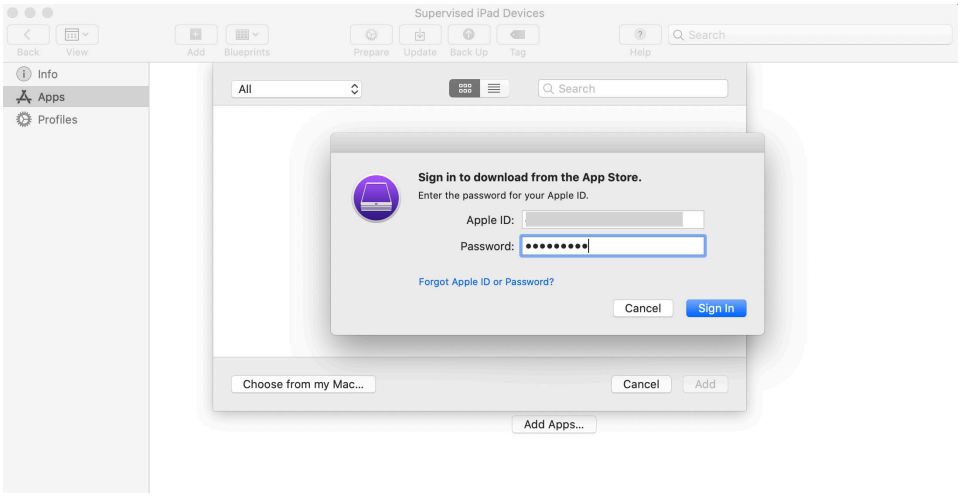
3. Click Sign In.



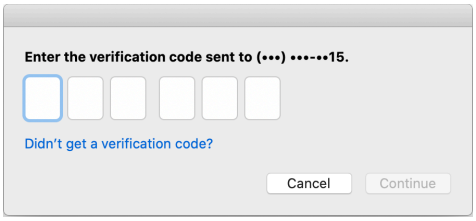
4. Enter the Apple ID of the Managed Apple ID that you just created. This Apple ID must have at least Content Manager access in Apple Business Manager.
5. Click Sign In.



6. In the Password field, enter the password for that Apple ID and click Sign In.

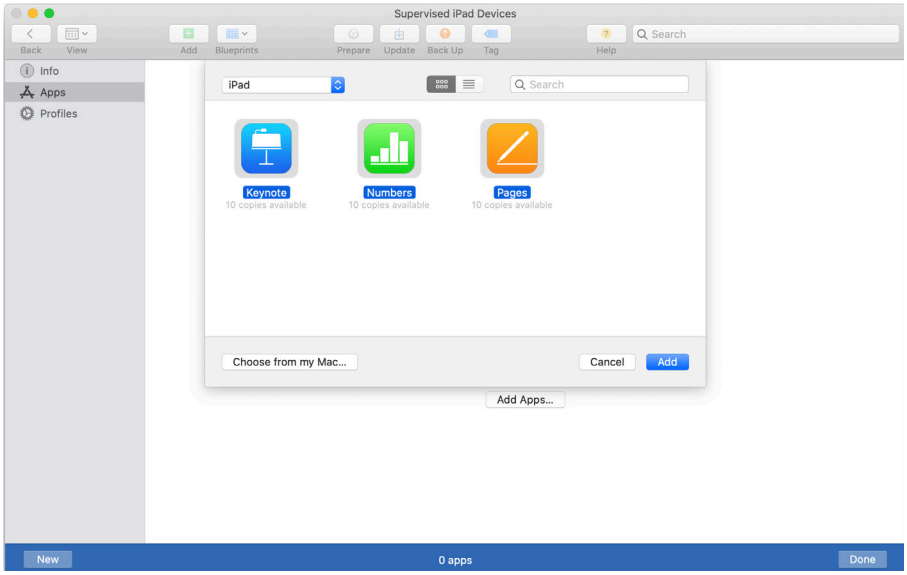


7. Enter the verification code sent to your mobile device and click Continue.

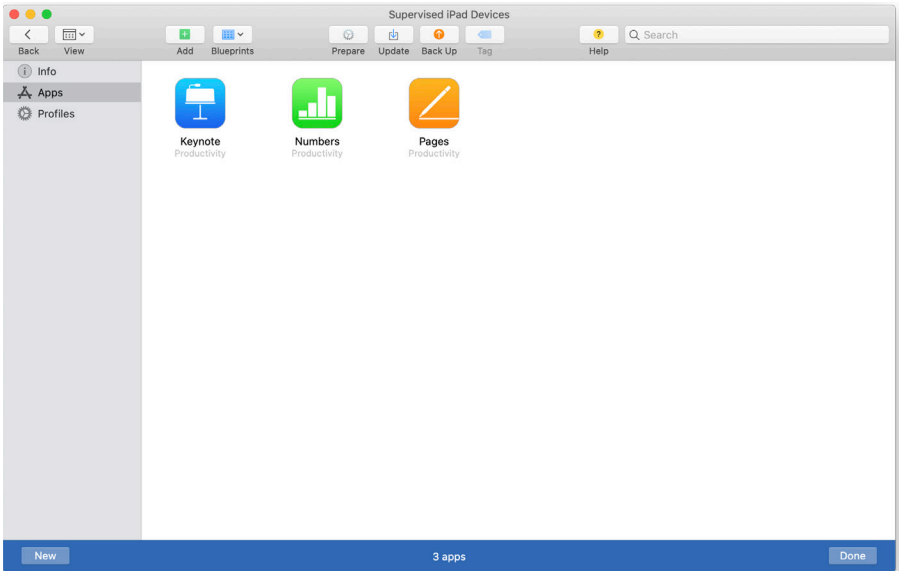


8. Confirm that Apple Configurator 2 displays the apps that you just acquired through Apps and Books in Apple Business Manager.
9. Select the apps you would like to deploy (you can press and hold the Command key to select multiple apps) and click Add.

   NOTE: Verify you have enough licenses for the amount of devices you would like to deploy to.



10. Verify the apps have been added to the Blueprint.

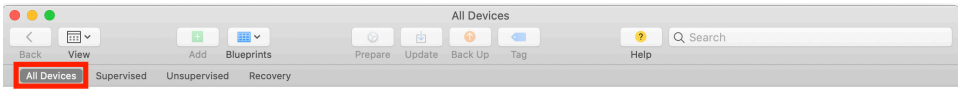


11. Click Done to stop modifying the Blueprint.

Section 11: Apply a Blueprint to devices

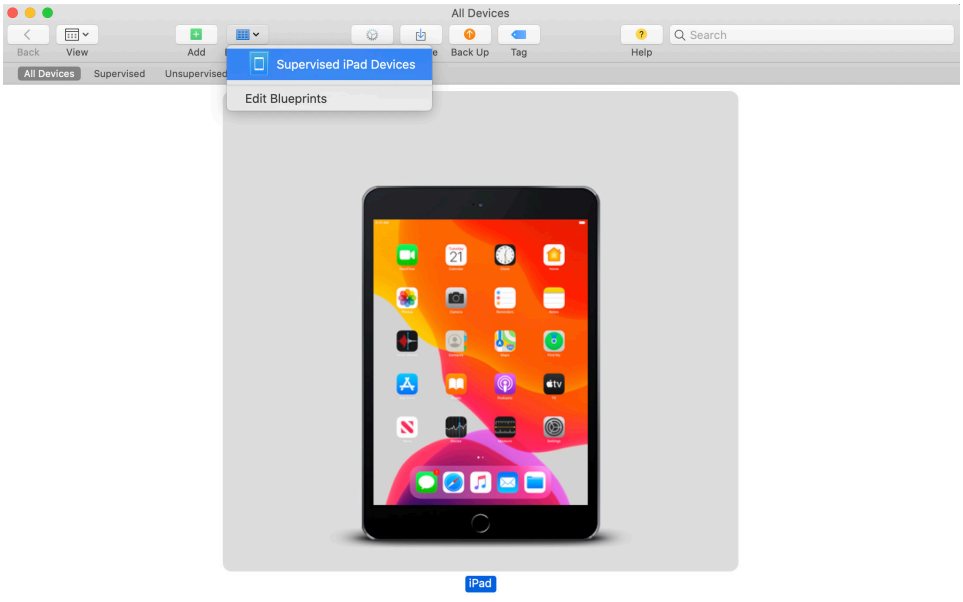
Now that you created your Blueprint you can apply it to your device(s).

1. Plug the device(s) in to the Apple Configurator 2 workstation.
2. In Apple Configurator 2, in the upper-left corner, confirm that All Devices is selected. If it isn't selected, click All Devices.



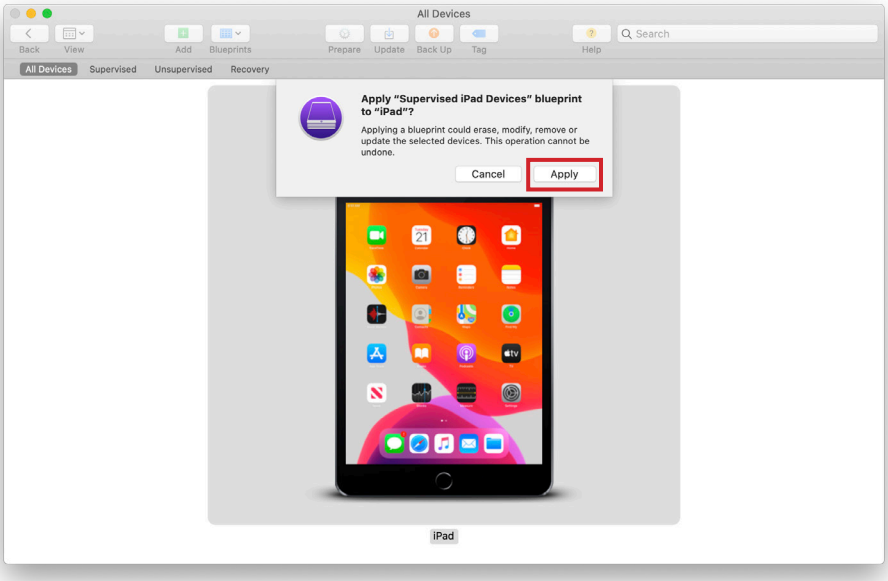
iPad

2. Select one, many, or all of the devices connected to Apple Configurator 2. As a reminder, you may want to invest in a USB hub or syncing cart for many devices.
3. In the toolbar, click Blueprints and choose the Blueprint you just created.



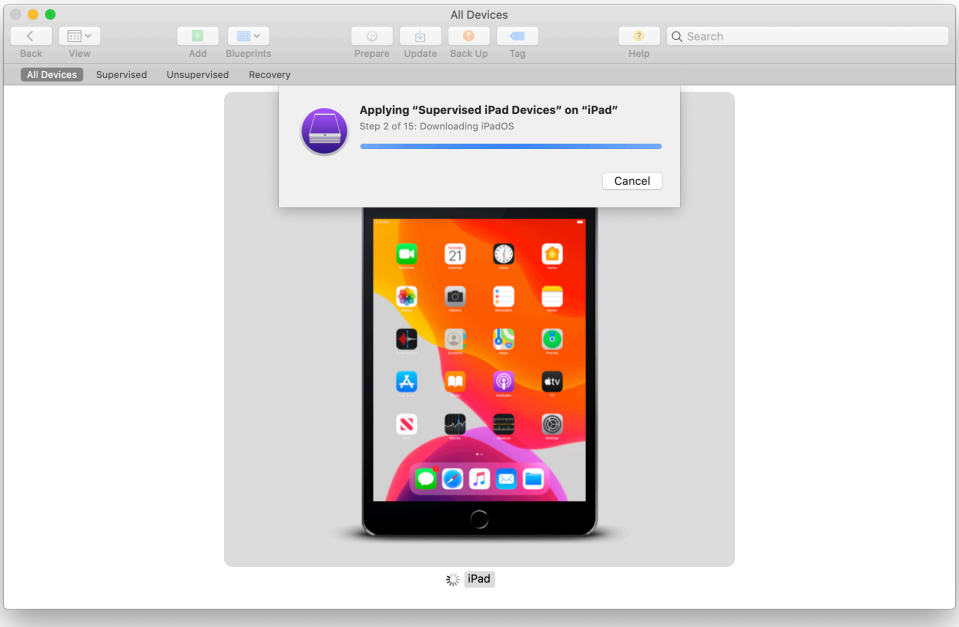
4. In the prompt that appears to confirm to want to apply the Blueprint, confirm that the only devices connected to your Mac are devices that you are OK with erasing, then click Apply. If a License Agreement window appears, click Accept to dismiss the window.

   NOTE: Ensure that there is no connected device that has sensitive information that cannot be retrieved after the device is erased.

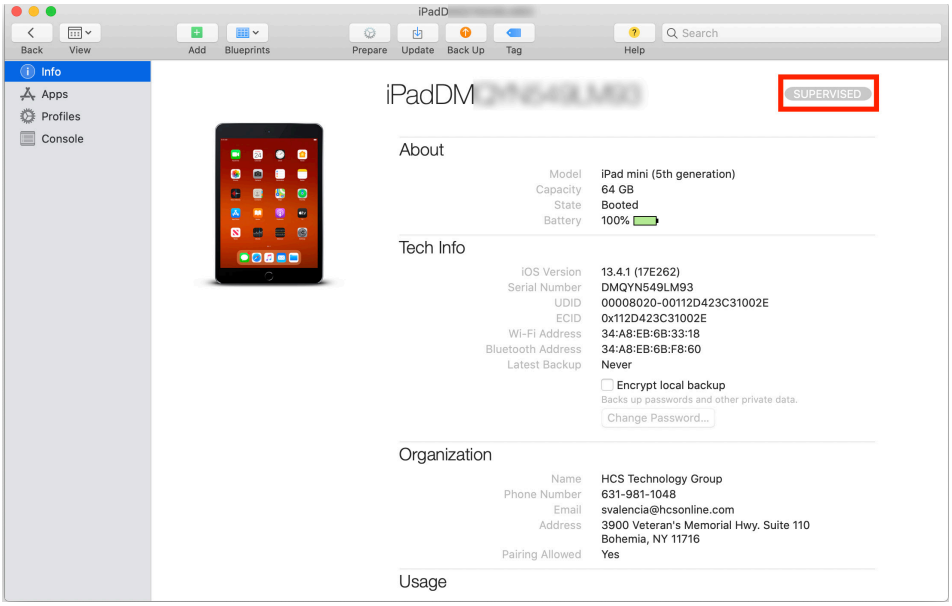


5. Confirm that Apple Configurator 2 displays a progress bar with a series of steps to install iPadOS, activate the device(s) and download and install apps.

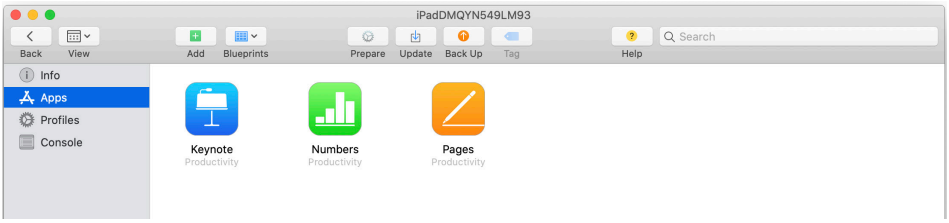
   NOTE: With content caching in place, the time it takes to download iOS, iPadOS, tvOS, and App Store apps is significantly decreased for each item after the first time that item is downloaded from Apple and cached on your Mac.



6. After Apple Configurator 2 completes applying the Blueprint, double-click any one of the iPad devices to reveal details.
7. In the upper-right corner, confirm that Apple Configurator 2 displays the word Supervised to indicate that this device is supervised.



8. In the sidebar, click Apps.
9. Confirm that Apple Configurator 2 displays that the apps you added to your Blueprint are installed on this device.



Section 12: Set Up Device(s) & Enroll in MDM

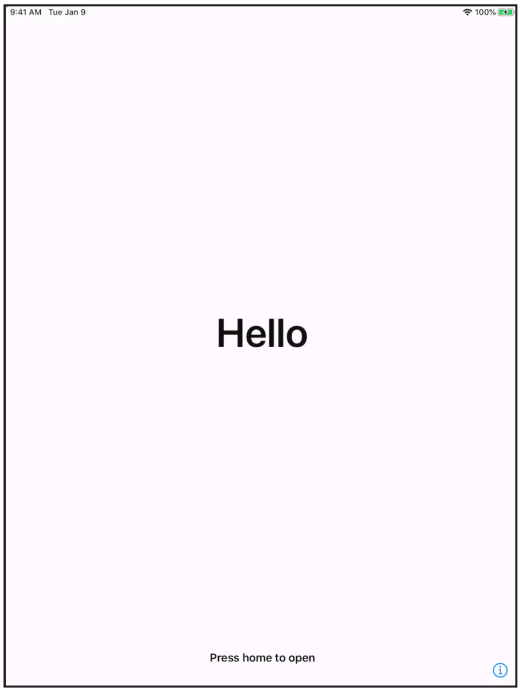
There are a few requirements to complete this next section and finalize the setup of iPad devices, which are outside the scope of this guide:

- Apple Business Manager MDM token
- MDM solution with above token in place
- iOS/iPadOS device must be configured in MDM for automated enrollment

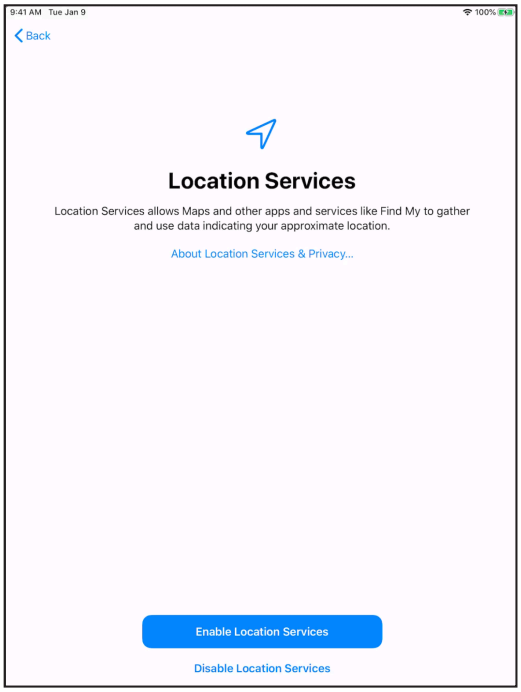
Tap through Setup Assistant steps and confirm expected settings.

Note: In the upper-right corner of the device, the Wi-Fi symbol is displayed with full signal strength indicators, even though you have not connected the device to Wi-Fi. This is because your device has an active USB connection to your Mac. In the upper-left corner, the device always displays the time as 9:41 AM. The reason for this is interesting and outside the scope of this guide.

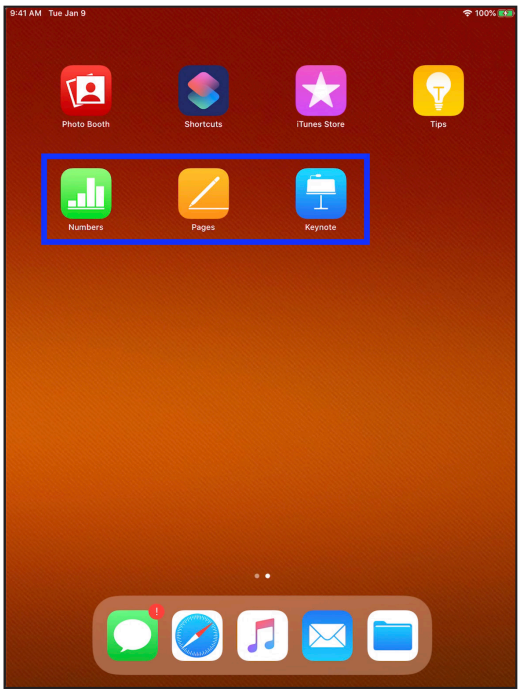
1. At the Hello screen, press the Home Button or swipe, depending on model.



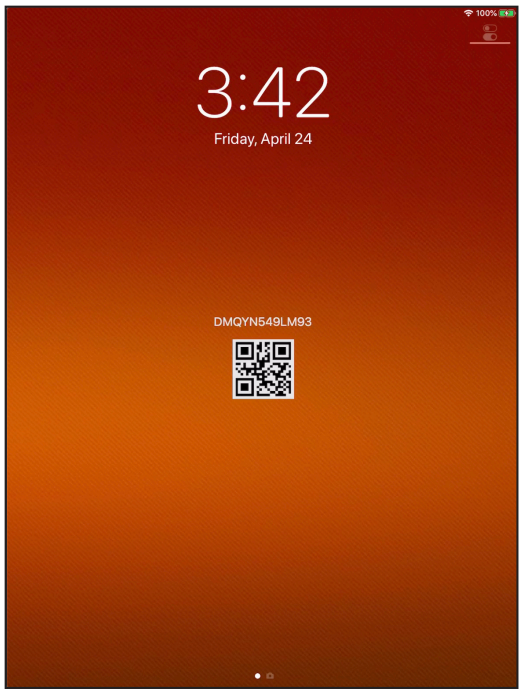
2. As you configured in the Blueprint, Location Services is the only Setup Assistant step that the device shows the user. Tap Enable Location Services. (Note that no wireless was required since tethered caching is in use).



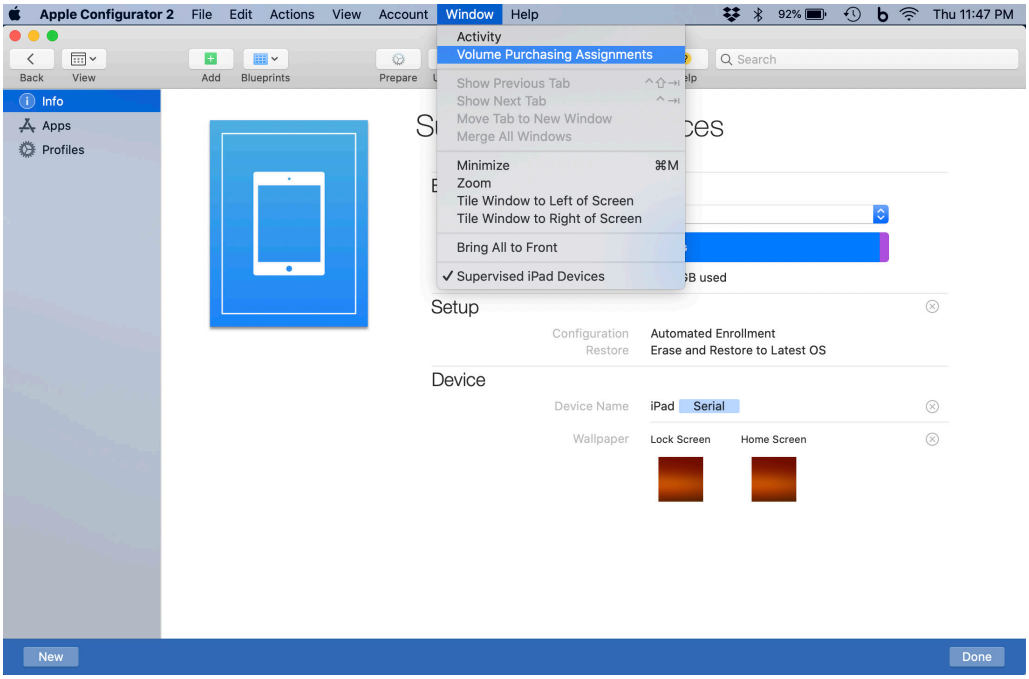
3. At this point, the iPad will be at the Home Screen. Swipe left to reveal a second page, which will have the apps deployed using Apple Configurator 2. These apps can now be managed by MDM.



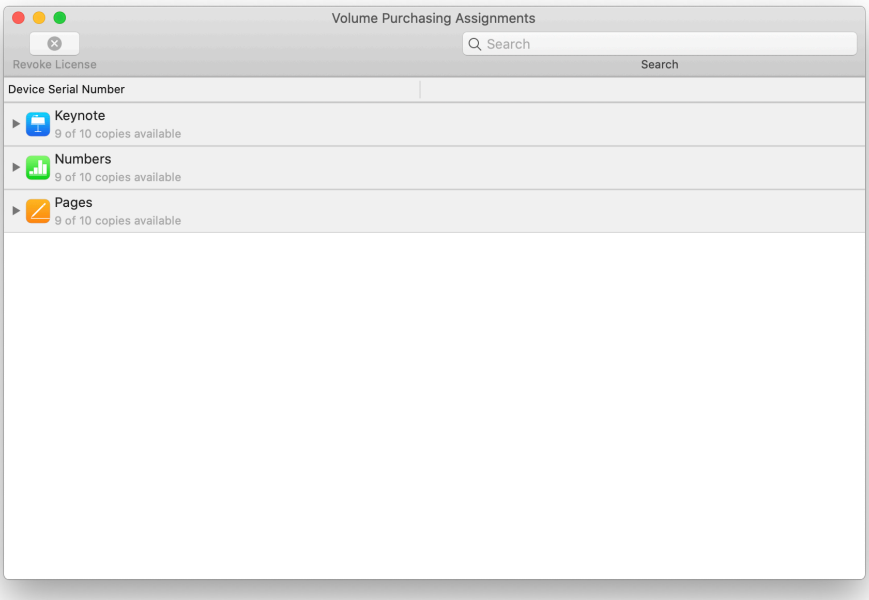
4. Press the sleep/wake button to bring the iPad to the lock screen.
5. Confirm that the iPad displays a serial number and a QR code.



6. In Apple Configurator 2, click the Window menu and choose Volume Purchasing Assignments.



7. Confirm that the appropriate number of licenses have been assigned to the devices that you provisioned.



7. For each app, click the disclosure triangle to reveal the serial number(s) of devices that apps were assigned to.

Section 13: Troubleshoot Tethered Caching

A known issue with tethered caching is that each device connected to the Mac creates a new network interface. Over time, a growing number of network interfaces are created in /Library/Preferences/SystemConfiguration/NetworkInterfaces.plist. This can causing extended delays when switching networks on the Mac and may cause the content caching service to stop functioning. As a result, you may need to remove the interfaces, which will automatically be re-created as needed. You can use the following script to remove the the NetworkInterfaces plist file, along with other associated plist files that are affected by the previously connected devices. IMPORTANT: This will remove existing network settings, including Wi-Fi and VPN configurations.

```
#!/bin/bash
# If your Mac is set to use tethered caching the iOS device UUID's can eventually
cause a slow down. This will remove key files to resolve.

# Elevated privileges will be needed to execute this script.

/bin/rm /Library/Preferences/SystemConfiguration/com.apple.nat.plist
/bin/rm /Library/Preferences/SystemConfiguration/NetworkInterfaces.plist
/bin/rm /Library/Preferences/SystemConfiguration/preferences.plist
```

The HCS team developed an app that removes the appropriate files to remediate this issue.. You can find this tool on our site, available here:

https://hcsonline.com/support/apps/fixtetheredcaching

This completes the guide.

If you'd like help implementing the solution in this white paper, we are ready to help; contact us at info@hcsonline.com or (866) 518-9672.

If you have corrections please send them to info@hcsonline.com.

For more white papers, visit https://hcsonline.com/support/white-papers.

For more information about HCS, visit https://hcsonline.com.