dataJAR
Beyond Device Management

Managing iPads, for the Mac Admin

virtual JNUC 2021

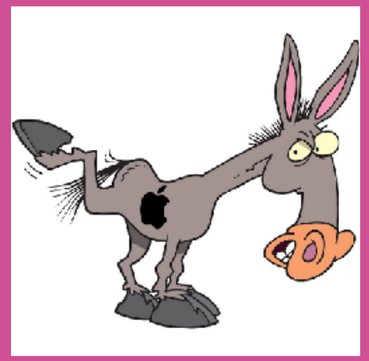
dataJAR
Beyond Device Management

Ben Toms

Head of Innovation and Platform

dataJAR Ltd | ben@datajar.co.uk

virtual JNUC 2021



macmule

macmule.com | macmule | @macmuleblog

dataJAR
Beyond Device Management

Managing iPads, for the Mac Admin

- Apple Deployment Programmes
- Jamf Pro Settings
- Application Deployment and Configuration
- Automated Device Enrollment
- Device Management Settings
- Remote Commands
- Additional Tips

virtual JNUC 2021

https://github.com/dataJAR/JNUC2021-Managing-iPads-for-the-Mac-Admin/

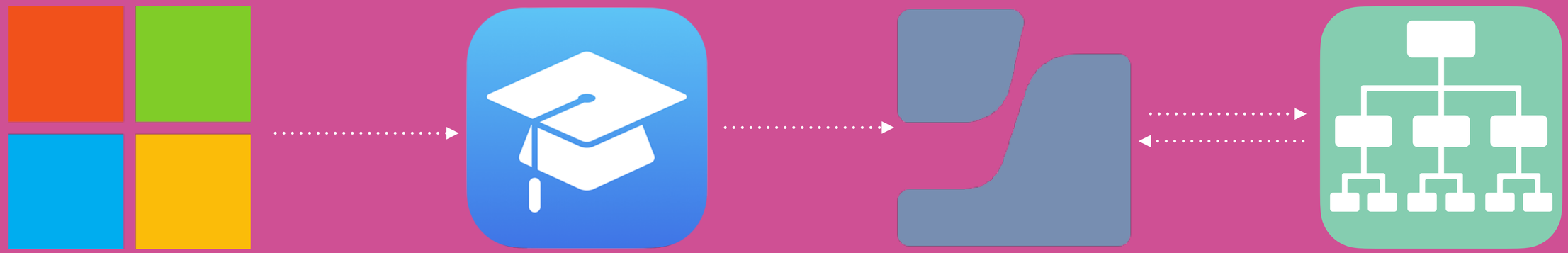
virtual JNUC 2021

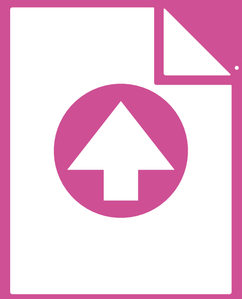
dataJAR
Beyond Device Management

Apple Deployment Programmes

virtual JNUC 2021

dataJAR
Beyond Device Management





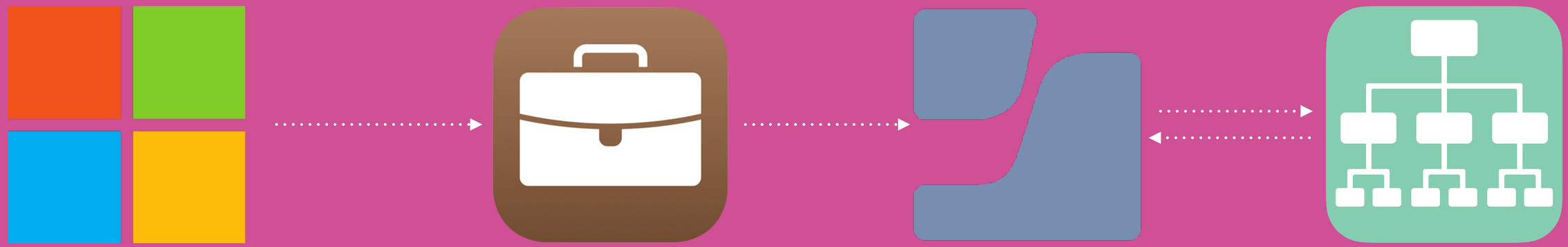
jappleseed@townshipschools.org

jappleseed@townshipschools.org

jappleseed@townshipschools.org

jappleseed@townshipschools.org

virtual JNUC 2021



jappleseed@myco any.com

jappl eed@ ompany.com

japples nycompany.com

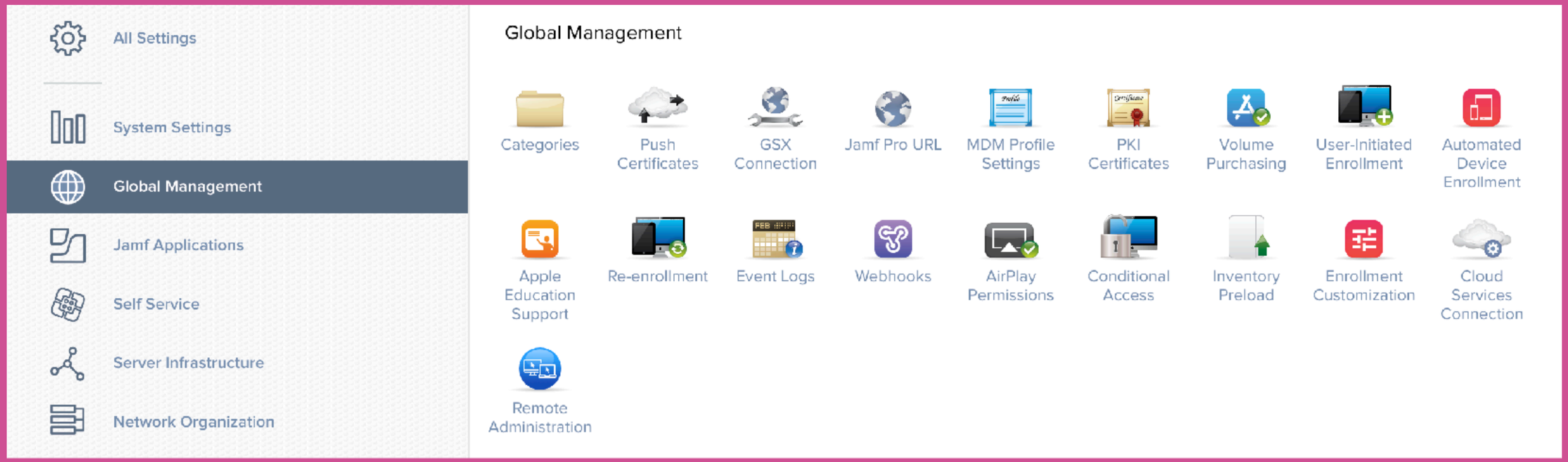
Important: Federated authentication requires that a user's User Principal Name (UPN) match their email address. User Principal Name aliases and Alternate IDs are not supported.

https://support.apple.com/en-gb/guide/apple-school-manager/apdb19317543/web

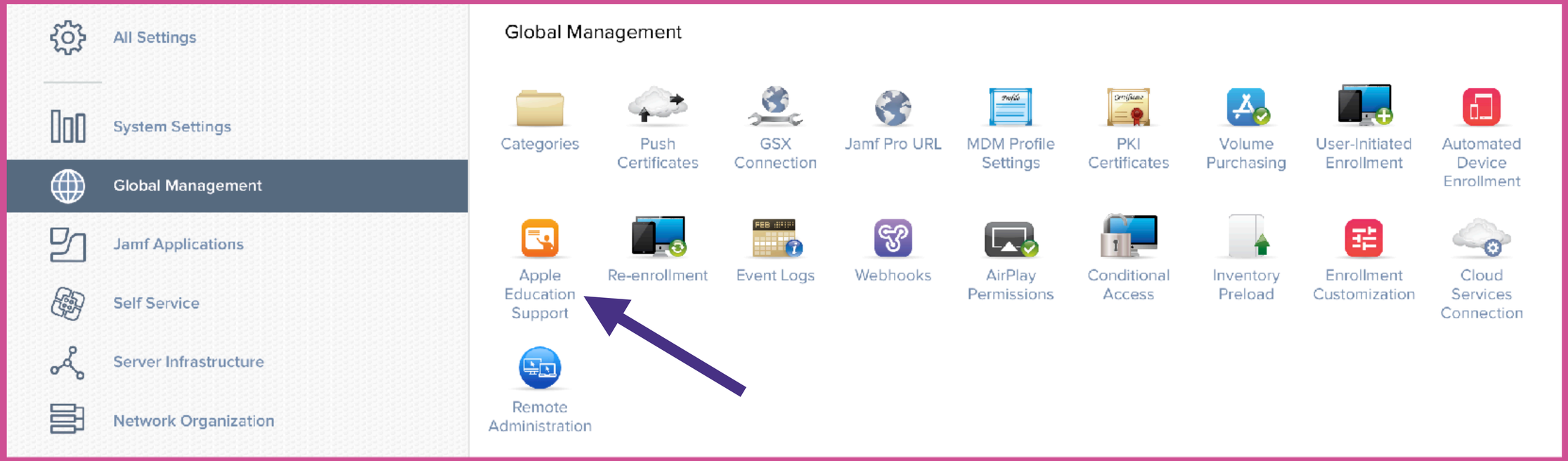
https://support.apple.com/en-gb/guide/apple-business-manager/apdb19317543/web

https://macmule.com/2019/05/27/modern-deployment-workflows-for-education/

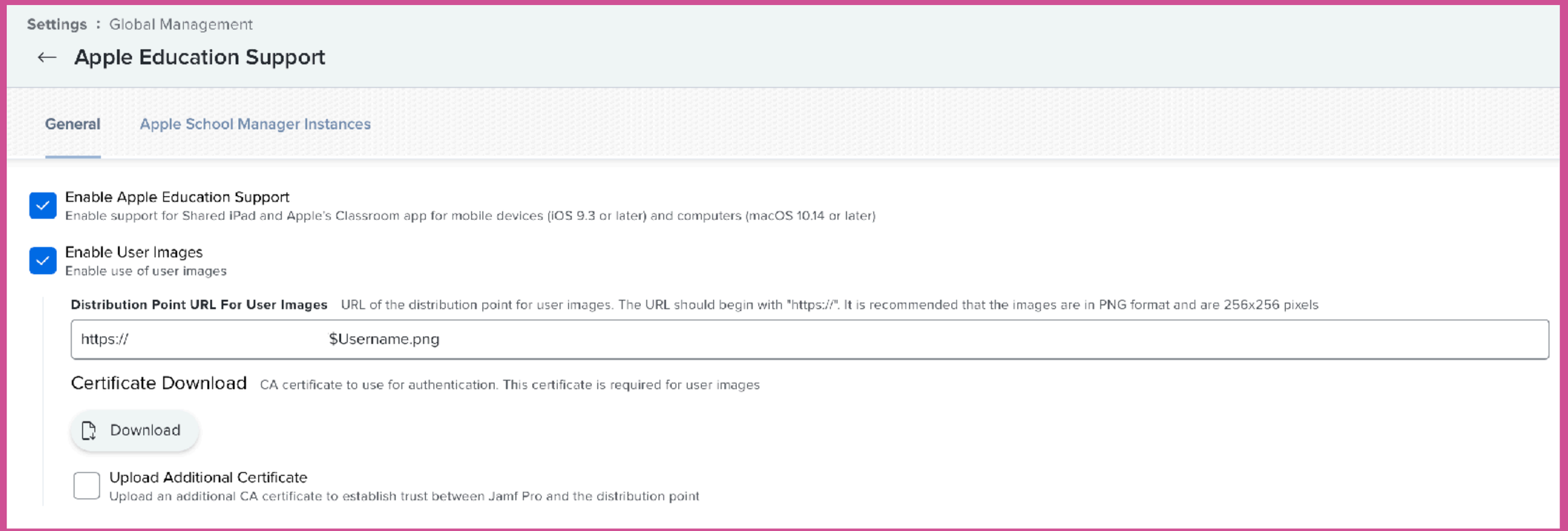
https://www.salamandersoft.co.uk/free-utilities/



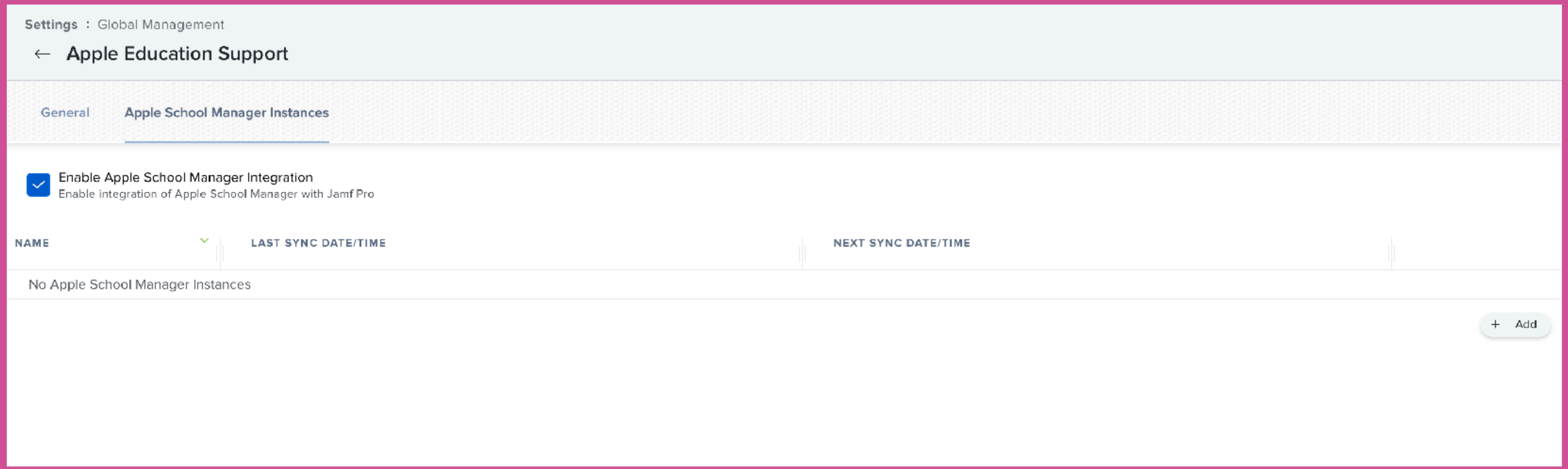
https://docs.jamf.com/jamf-pro/administrator-guide/Apple_Education_Support_Settings.html



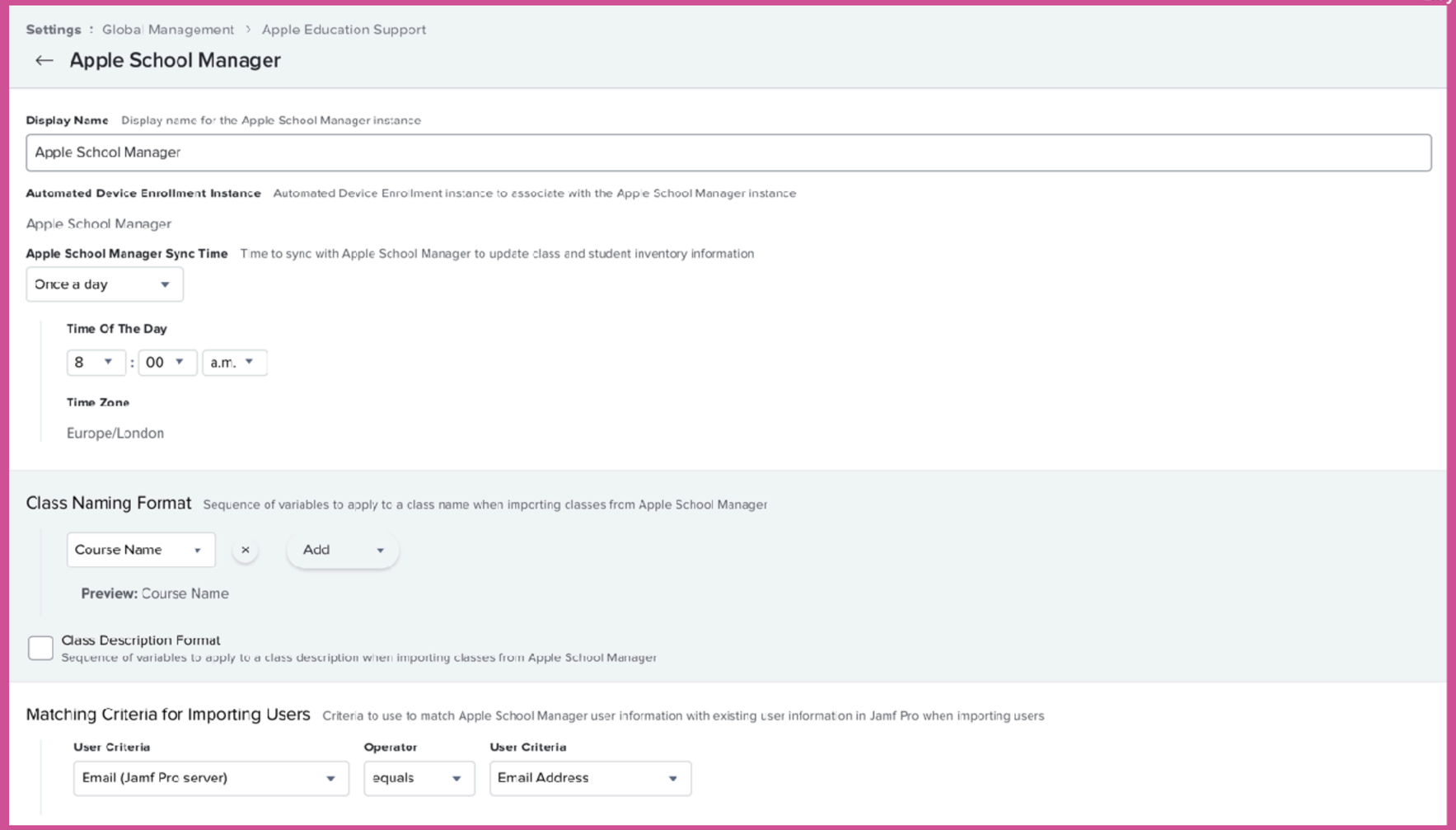
https://docs.jamf.com/jamf-pro/administrator-guide/Apple_Education_Support_Settings.html



https://docs.jamf.com/jamf-pro/administrator-guide/Apple_Education_Support_Settings.html



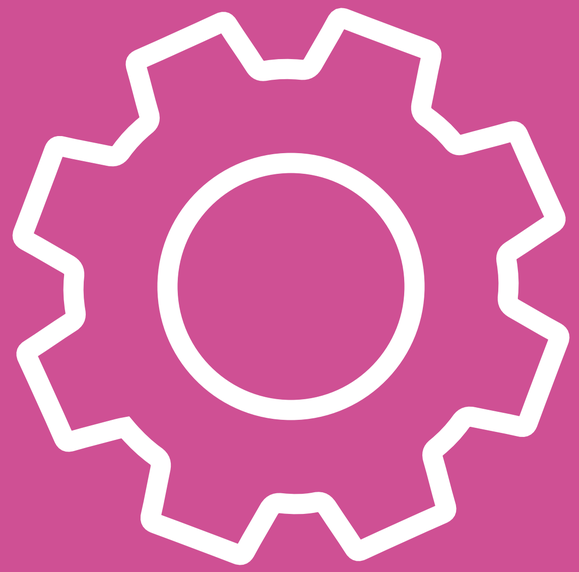
https://docs.jamf.com/jamf-pro/administrator-guide/Apple_Education_Support_Settings.html



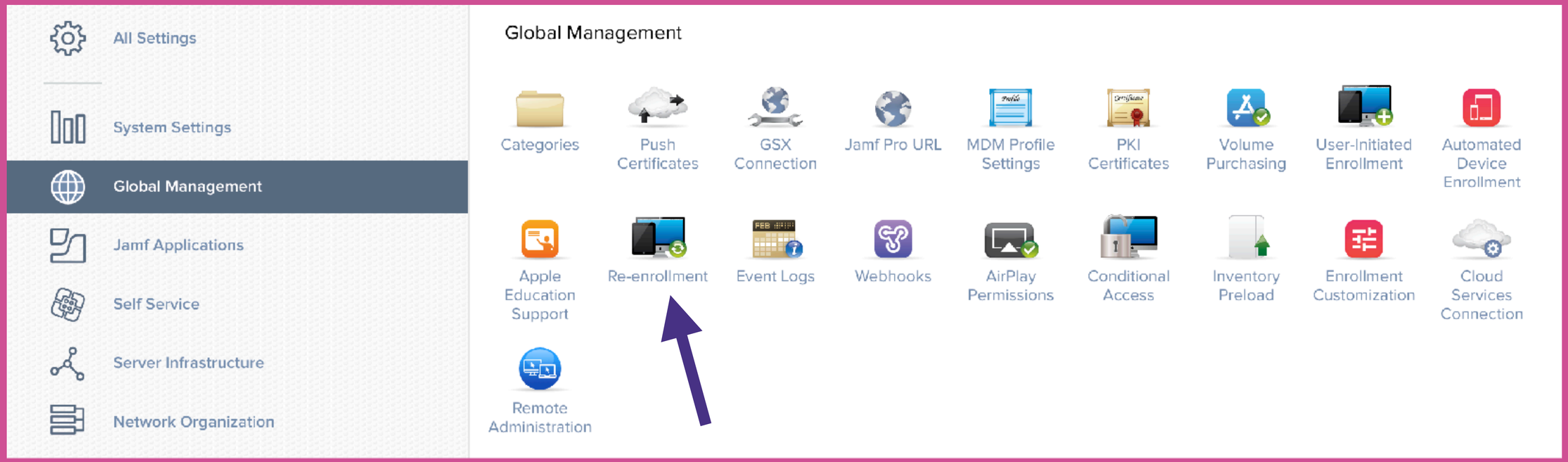
https://docs.jamf.com/jamf-pro/administrator-guide/Apple_Education_Support_Settings.html

dataJAR
Beyond Device Management

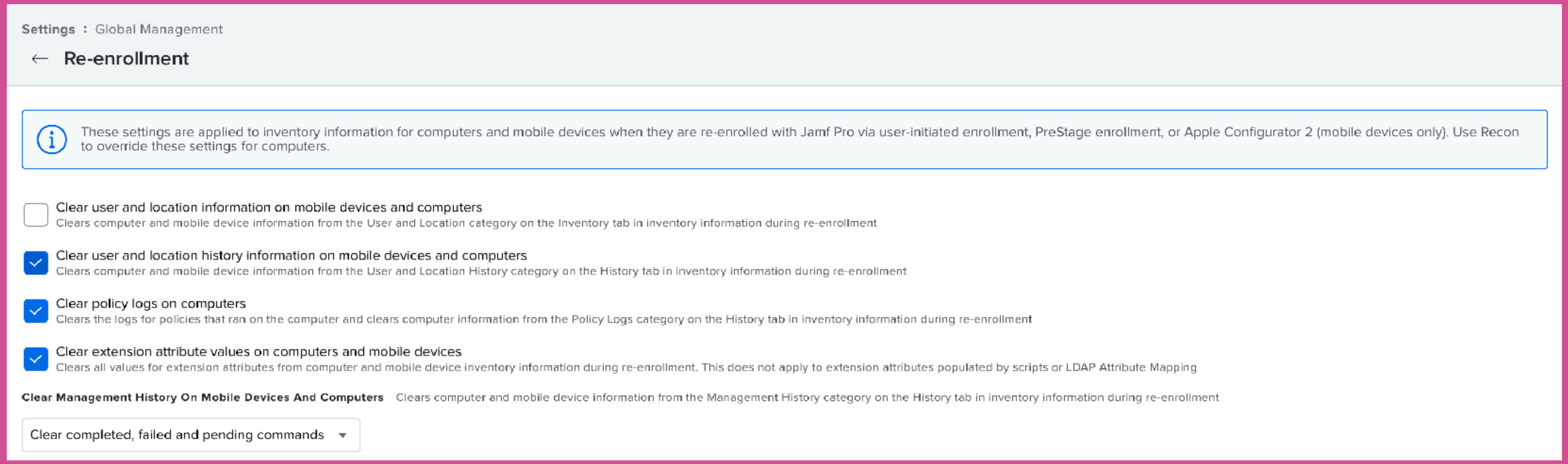
Jamf Pro Settings



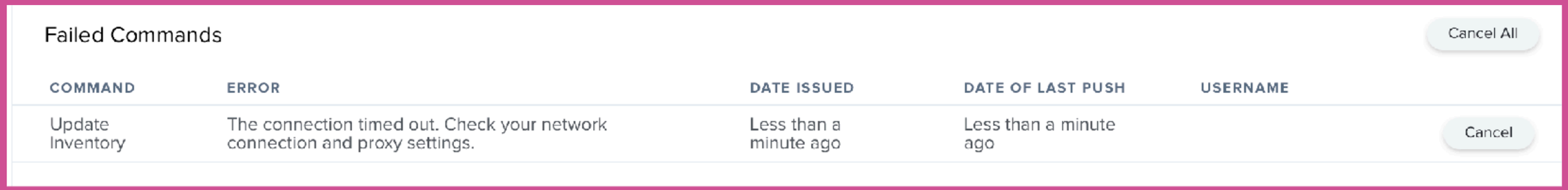
virtual JNUC 2021



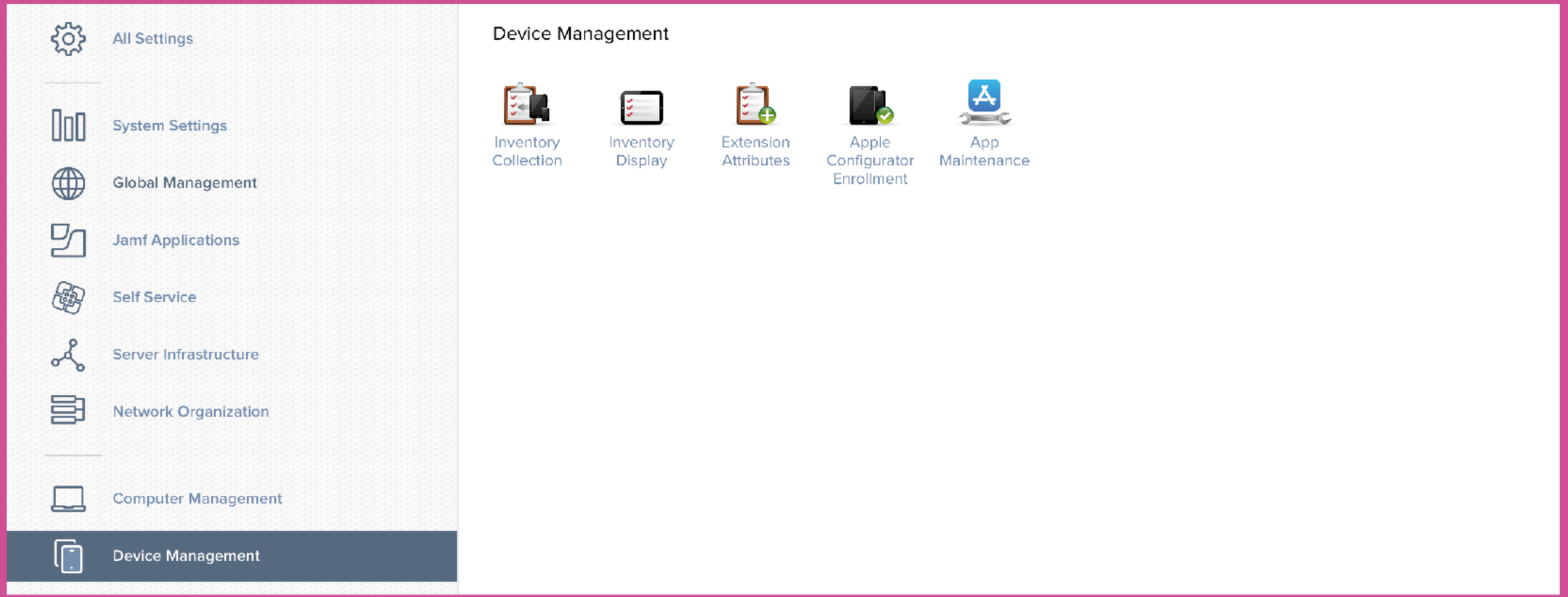
https://docs.jamf.com/jamf-pro/administrator-guide/Re-enrollment_Settings.html

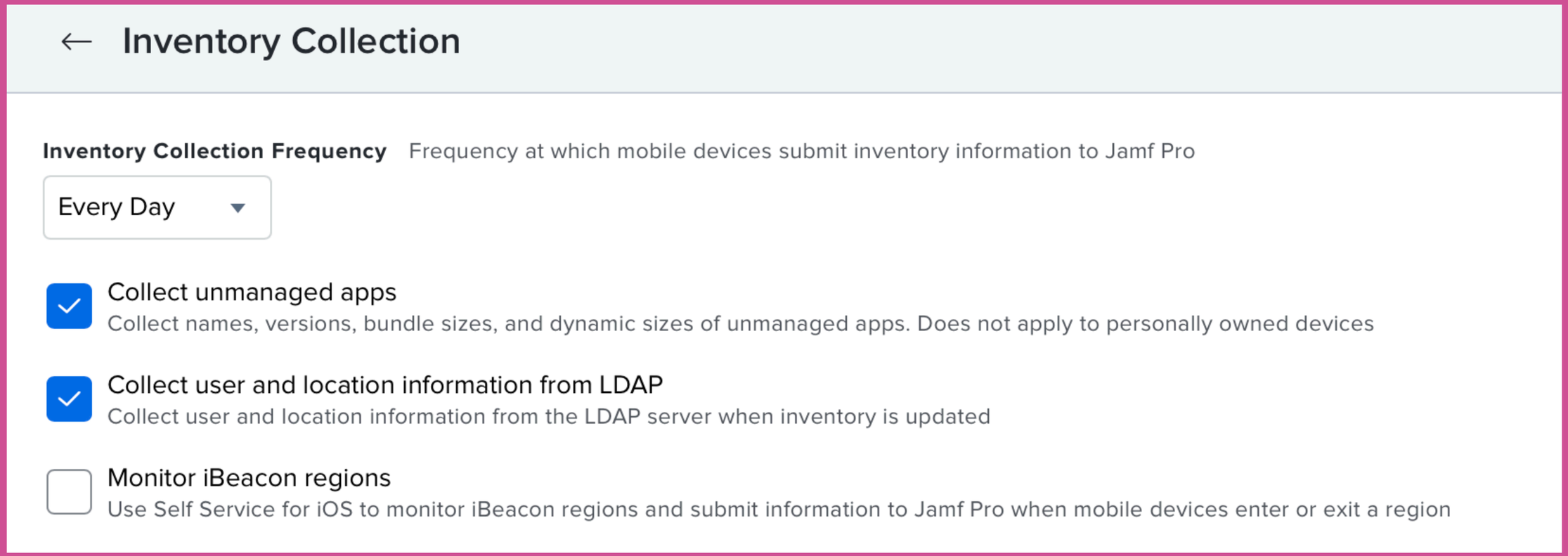


https://docs.jamf.com/jamf-pro/administrator-guide/Re-enrollment_Settings.html

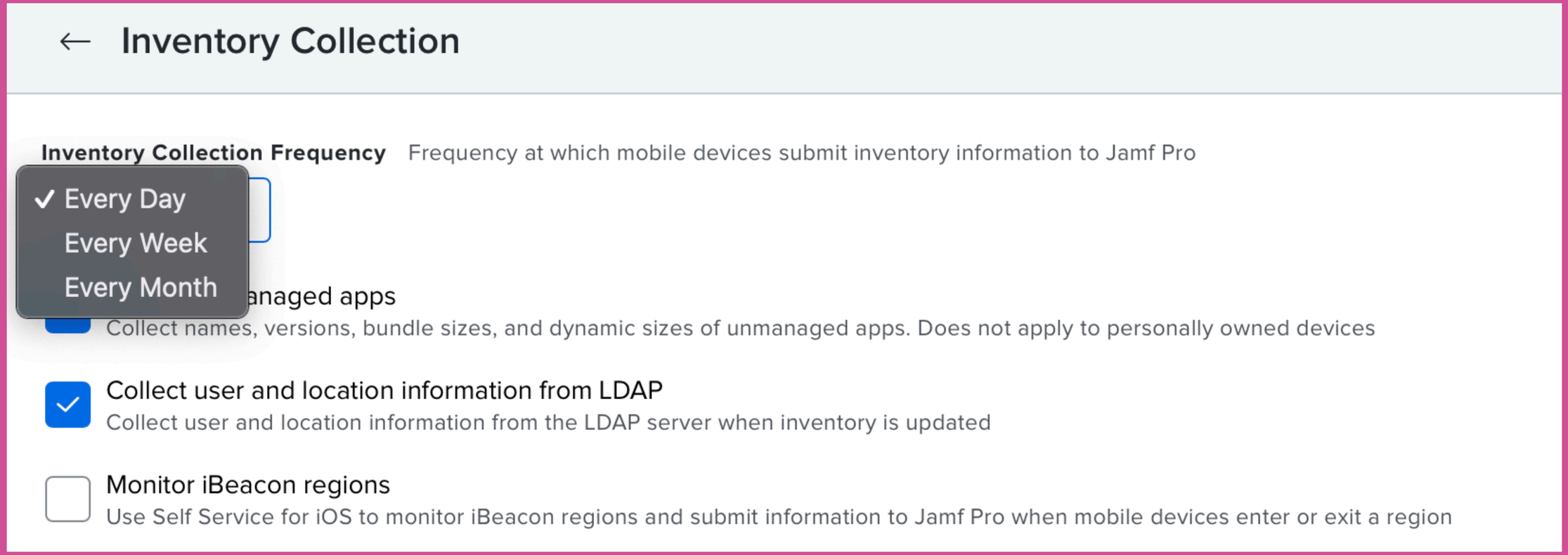


PI-005519

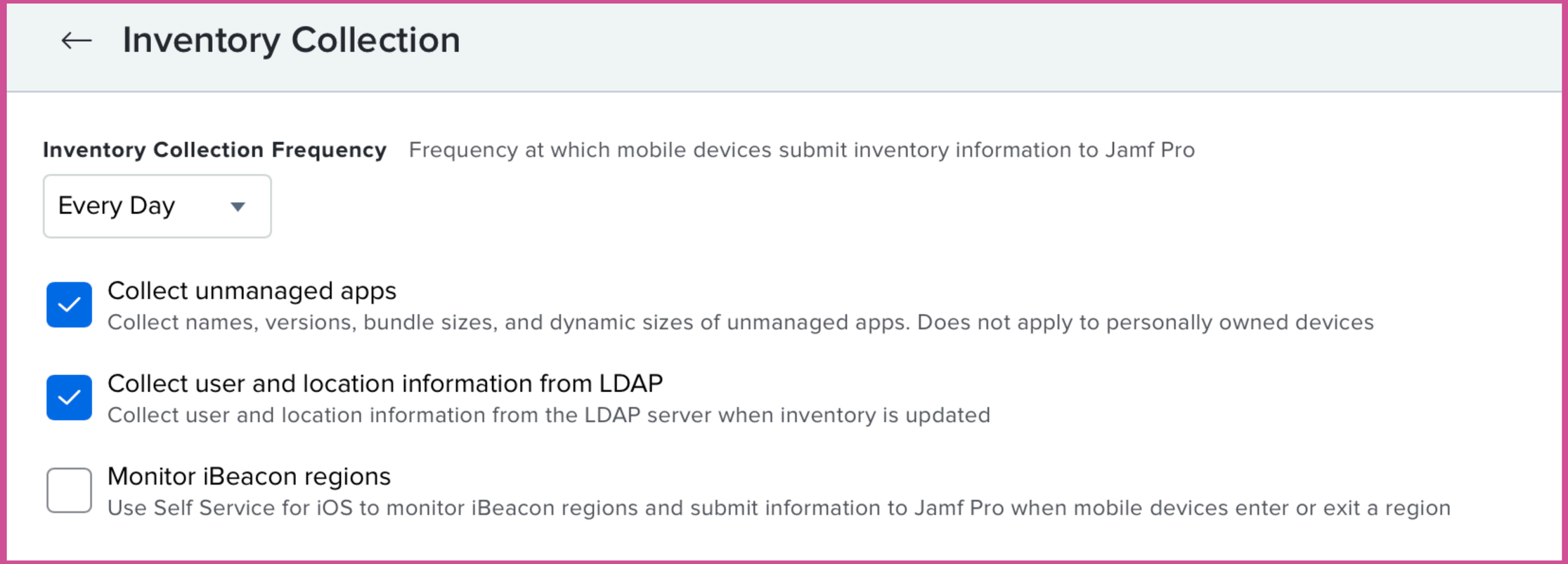




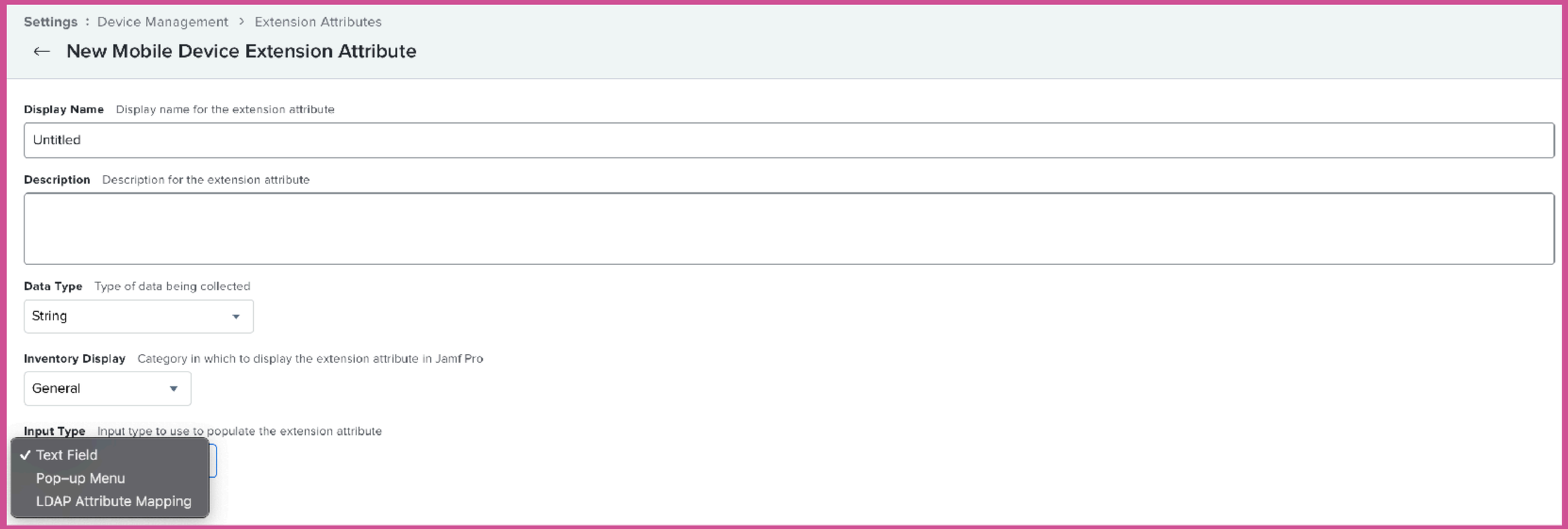
https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Inventory_Collection_Settings.html



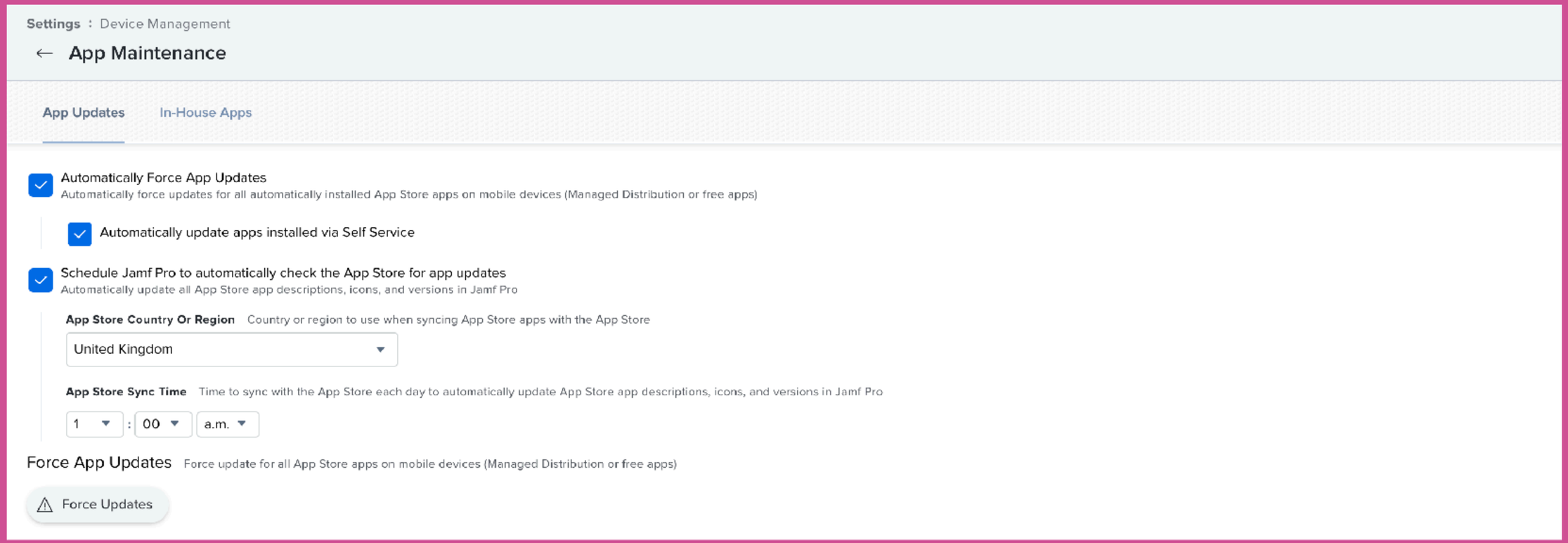
https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Inventory_Collection_Settings.html



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Inventory_Collection_Settings.html



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Extension_Attributes.html

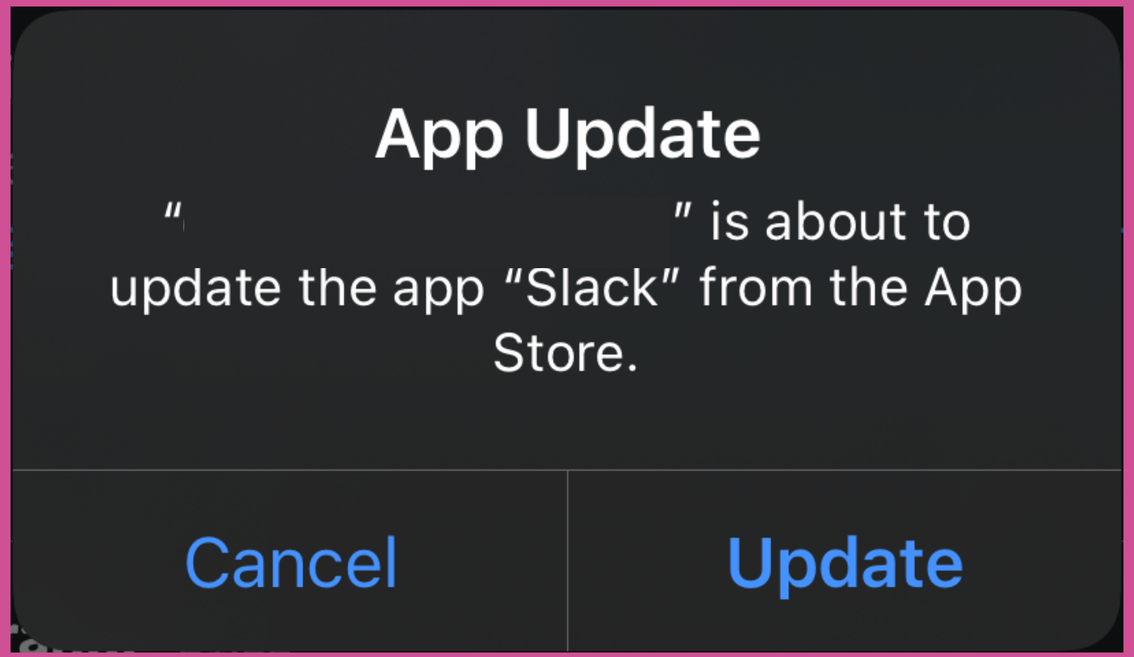


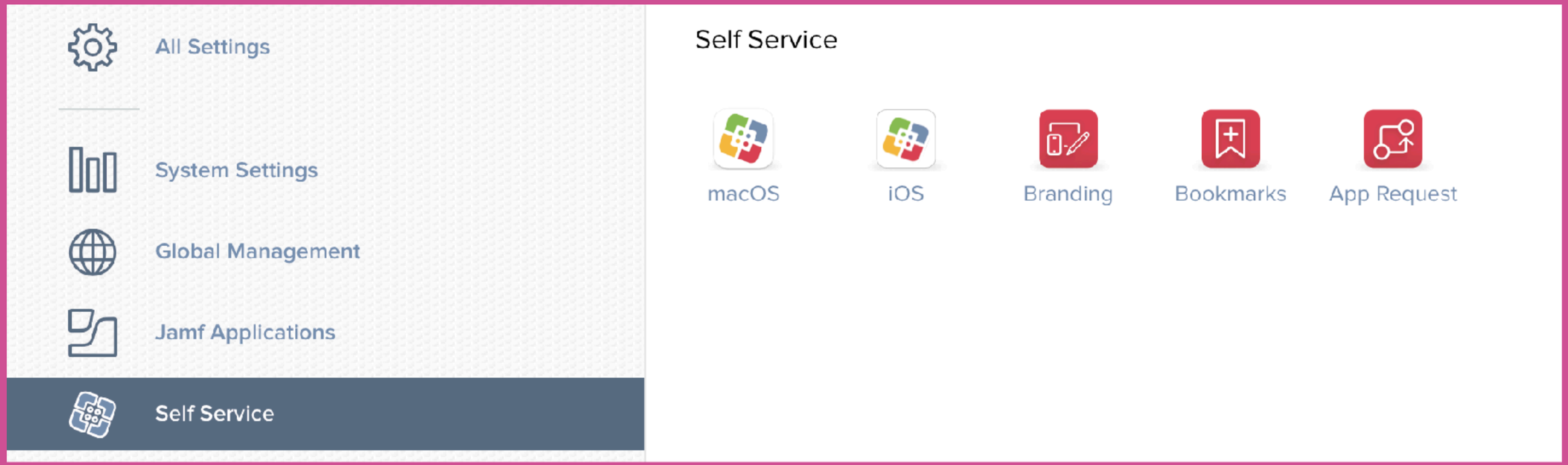
https://docs.jamf.com/jamf-pro/administrator-guide/App_Store_App_Update_Settings.html

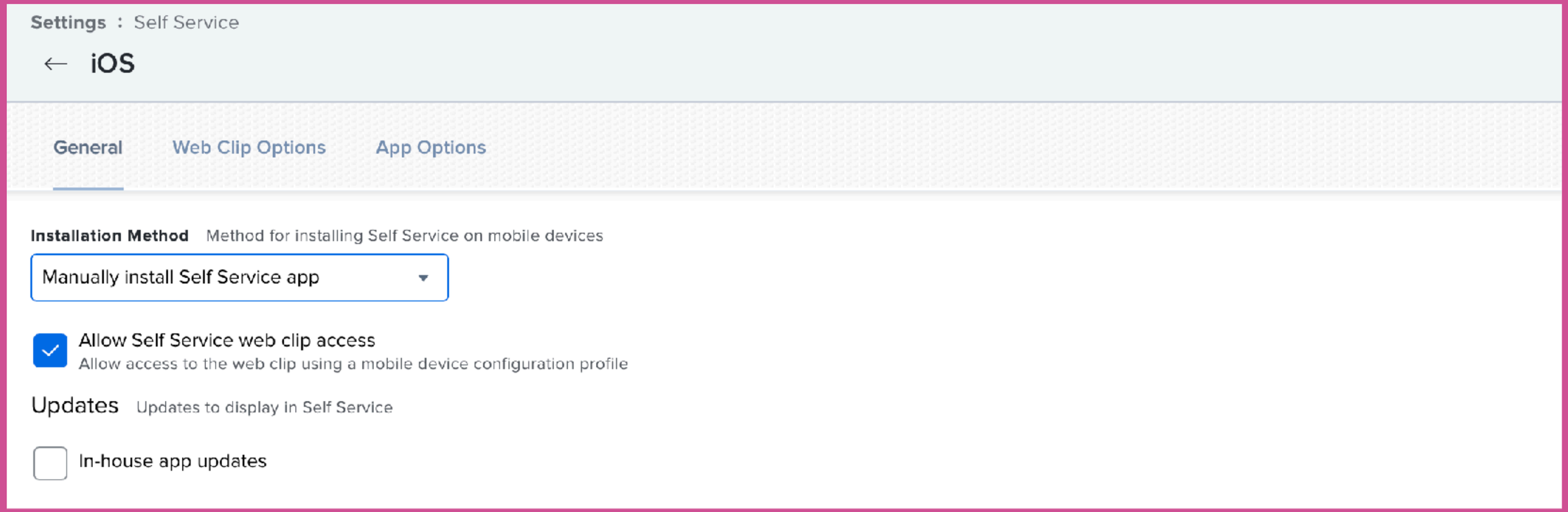
Pending Commands

Cancel All

COMMAND	STATUS	DATE ISSUED	DATE OF LAST PUSH	USERNAME	
Install App - Self Service	Device was busy. Will try again.	15 minutes ago			Cancel



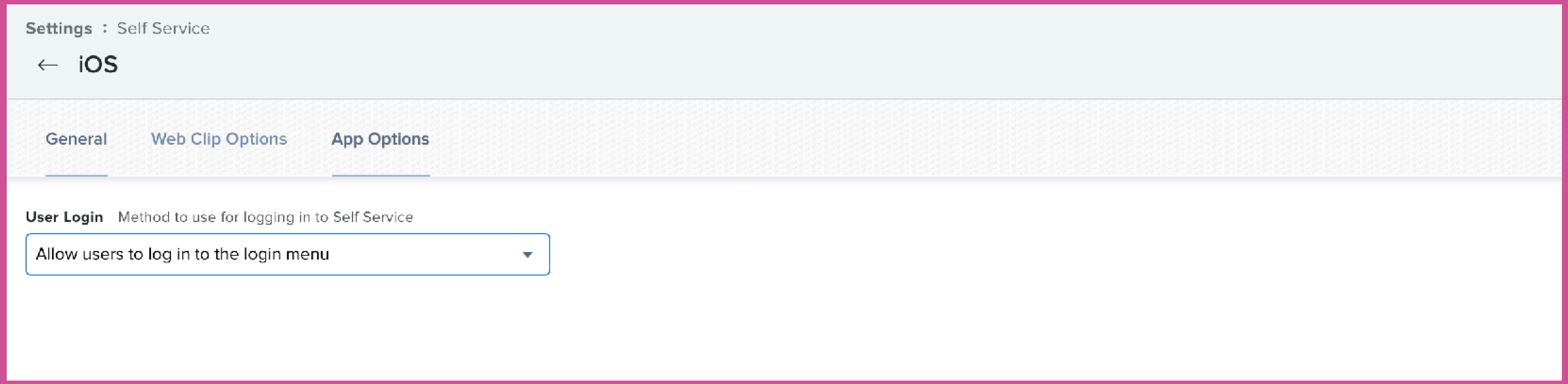




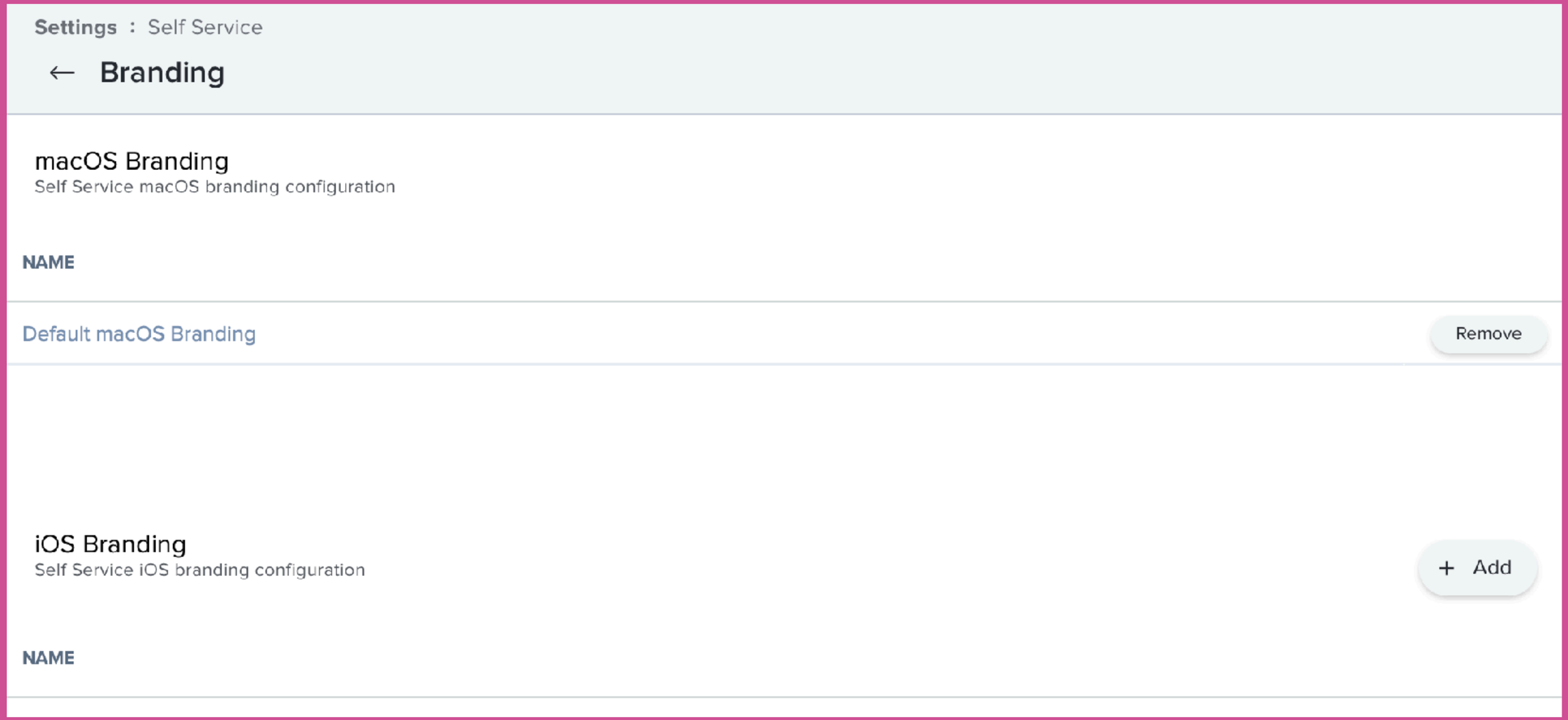
https://docs.jamf.com/jamf-pro/administrator-guide/Jamf_Self_Service_for_iOS.html

dataJAR
Beyond Device Management

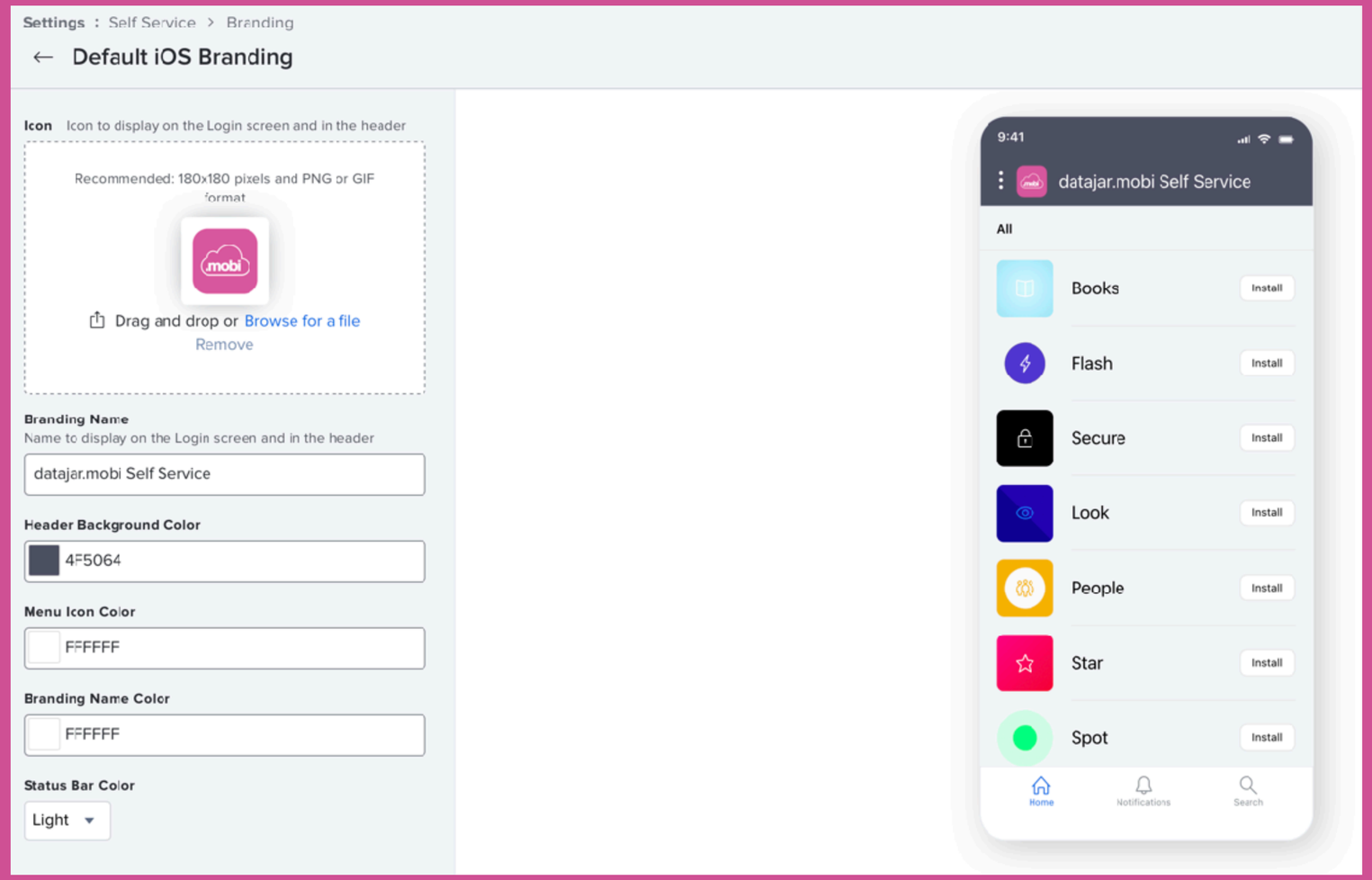
virtual JNUC 2021



https://docs.jamf.com/jamf-pro/administrator-guide/Jamf_Self_Service_for_iOS.html

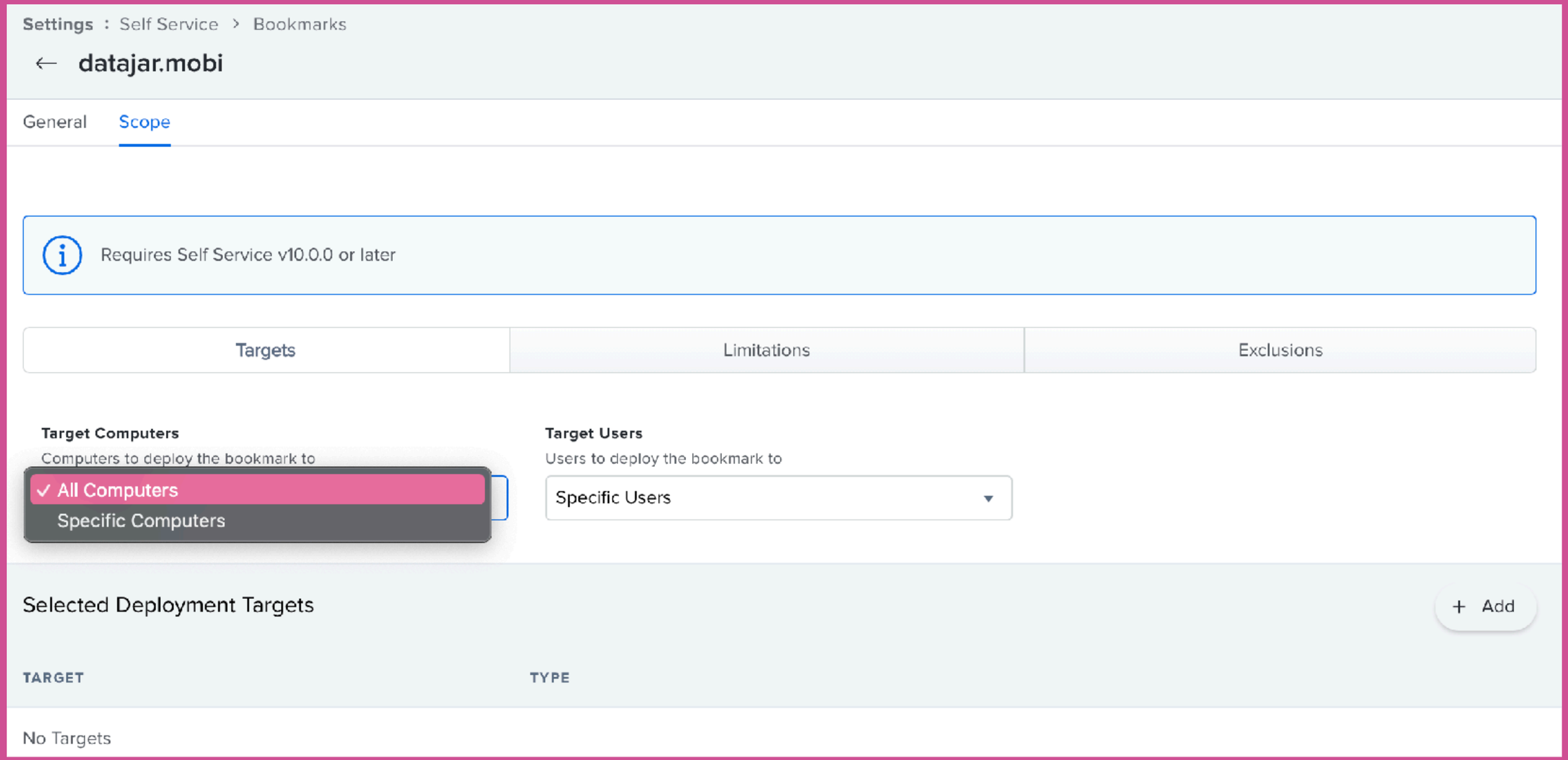


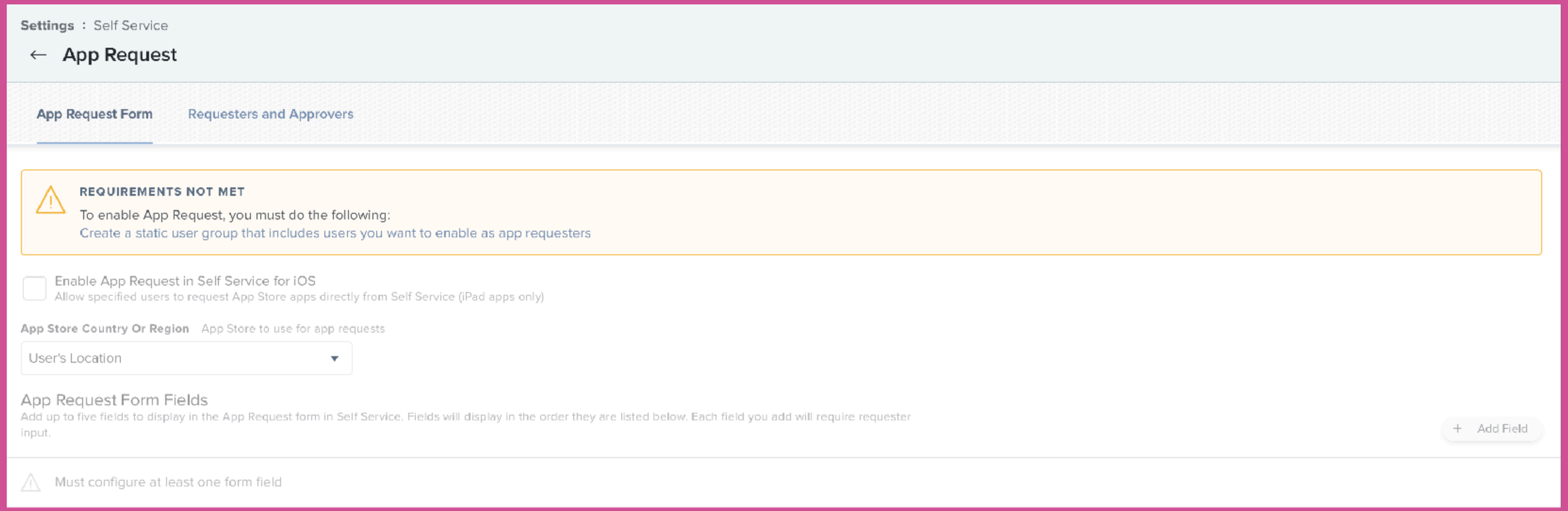
https://docs.jamf.com/jamf-pro/administrator-guide/Jamf_Self_Service_for_iOS_Branding_Settings.html



https://docs.jamf.com/jamf-pro/administrator-guide/Jamf_Self_Service_for_iOS_Branding_Settings.html

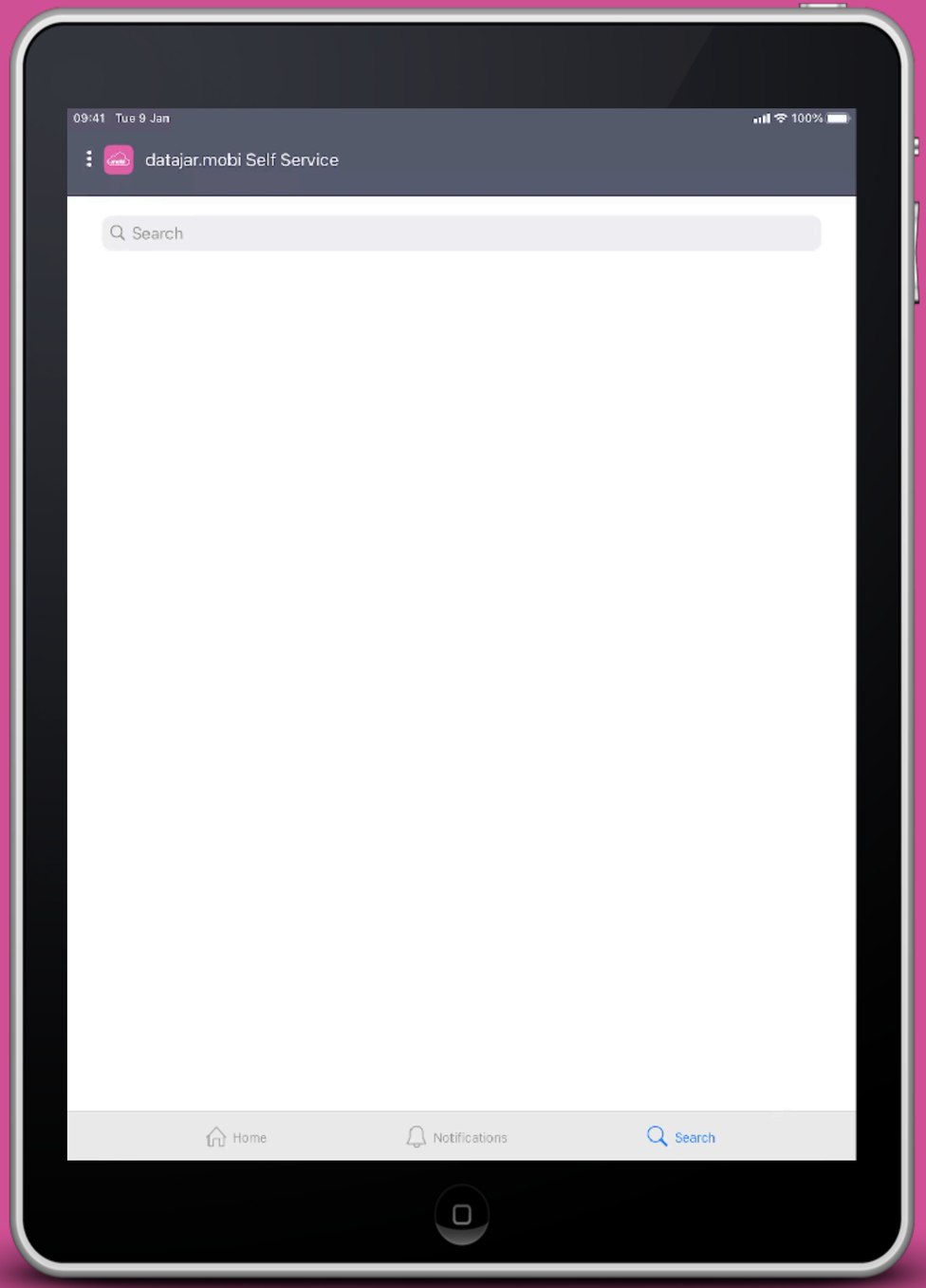
Icon Icon to display on the Login screen and in the header





https://docs.jamf.com/jamf-pro/administrator-guide/App_Request.html

dataJAR
Beyond Device Management



virtual JNUC 2021

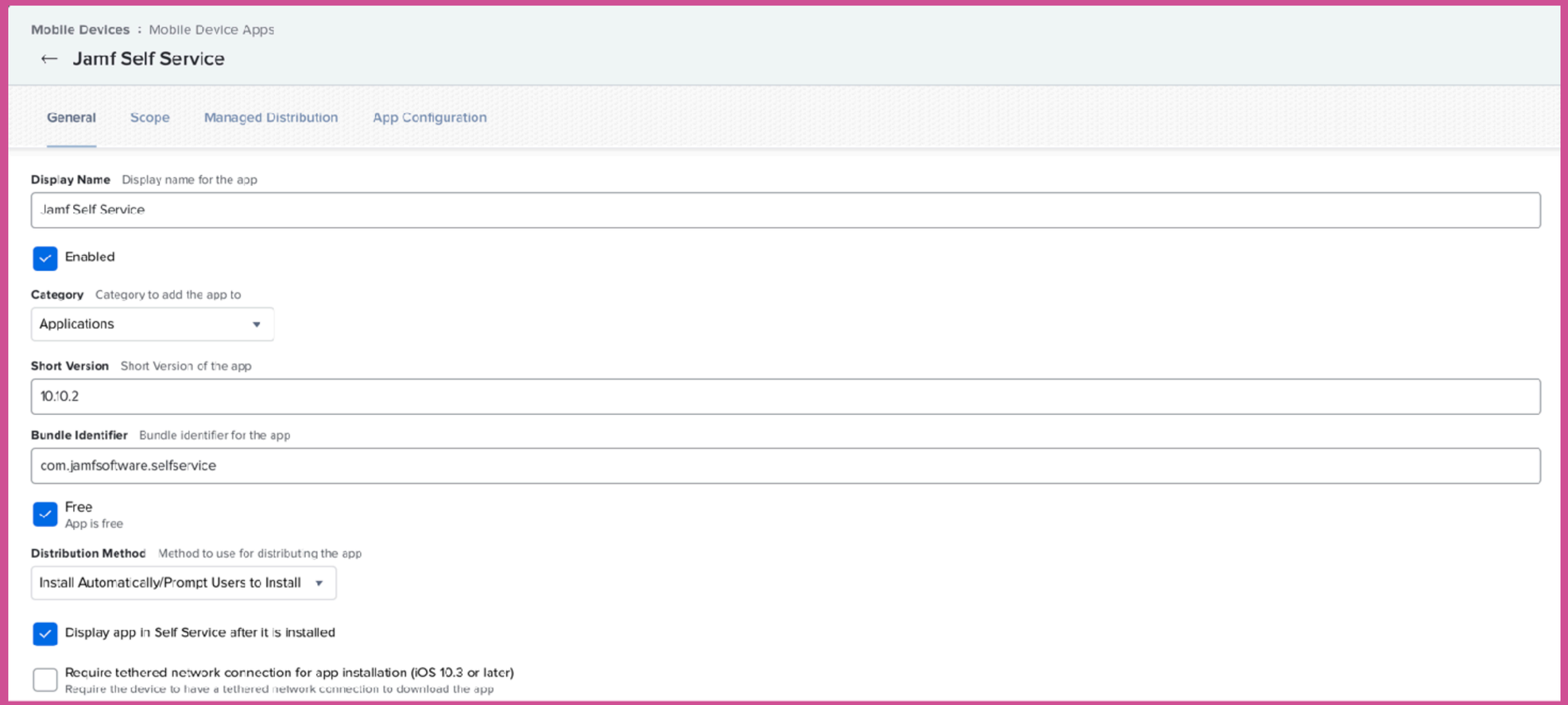
dataJAR
Beyond Device Management

Application Configuration and Deployment

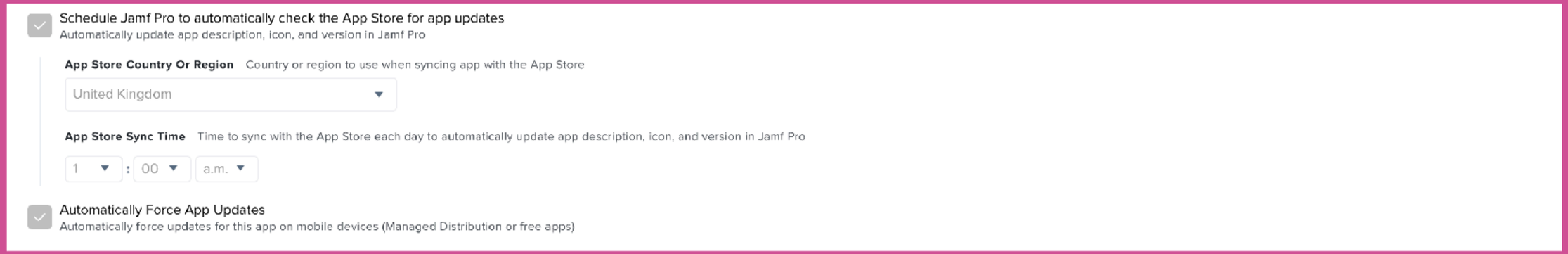
virtual JNUC 2021

dataJAR
Beyond Device Management

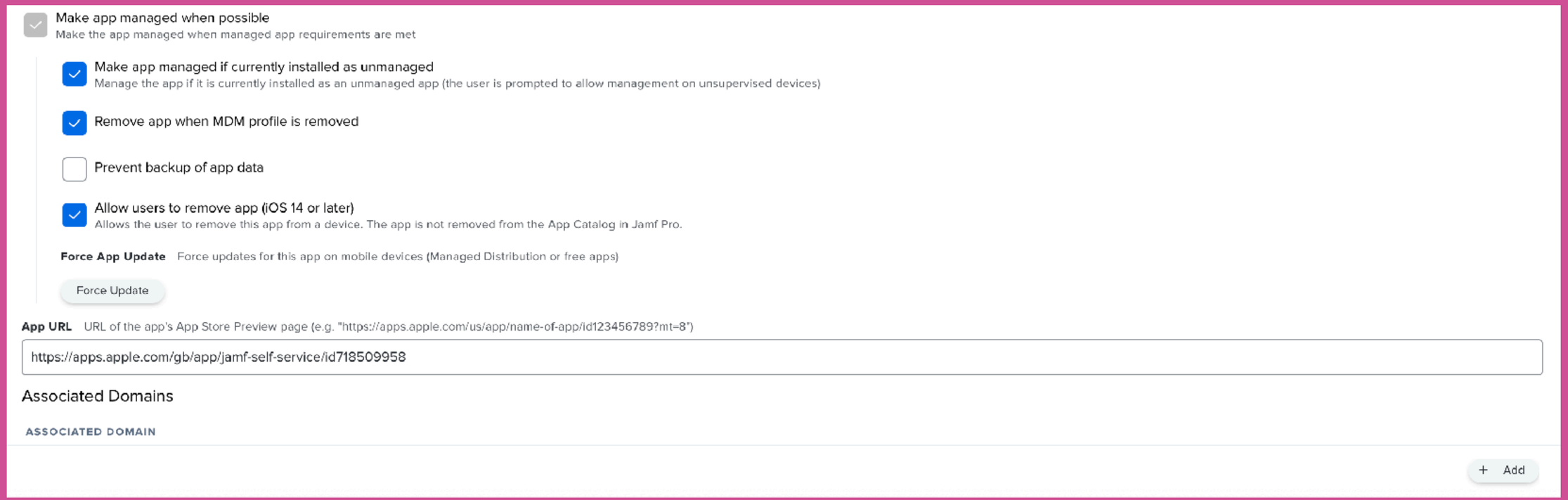
virtual JNUC 2021



https://docs.jamf.com/jamf-pro/administrator-guide/Apps_Purchased_in_Volume.html



https://docs.jamf.com/jamf-pro/administrator-guide/Apps_Purchased_in_Volume.html



https://docs.jamf.com/jamf-pro/administrator-guide/Apps_Purchased_in_Volume.html

Managed app restrictions and capabilities

Managed apps have the following restrictions and capabilities, providing improved security and a better user experience:

- *Managed Open In:* Provides two functions for protecting your organisation's app data:
  - *Allow documents from unmanaged sources in managed destinations*. Enforcing this restriction prevents a user's personal sources and accounts from opening documents in your organisation's managed destinations. For example, this restriction could prevent the user from opening a PDF from a random website in your organisation's PDF app.
  - *Allow documents from managed sources in unmanaged destinations*. Enforcing this restriction prevents an organisation's managed sources and accounts from opening documents in a user's personal destinations. This restriction could prevent a confidential email attachment in your organisation's managed mail account from being opened in any of the user's personal apps.

https://support.apple.com/en-gb/guide/deployment-reference-ios/iorf4d72eded/web

Deploying Pages, Keynote, and Numbers with Volume Purchasing

Apple includes iWork apps for free with the purchase of every new device. When a user sets up a new device, the Apple ID is prompted to redeem these free apps for download.

If your organization is purchasing new devices, you can request that these iWork apps (Pages, Keynote, and Numbers) be added to your Apple Business Manager or Apple School Manager account instead of being redeemed with a user's Apple ID.

Once these apps have been added to your account, you will be able to deploy and manage them with Jamf Now.

Note: For iPad or iPhone with iOS 12.3.x or earlier, users must delete built-in versions of these apps on their devices before Jamf Now can manage the apps. After deletion, deploy apps using volume licenses via Jamf Now.

← Deploying an App to All Devices in a Blueprint

Removing an Application →

https://docs.jamf.com/jamf-now/documentation/Deploying_Pages_Keynote_and_Numbers_with_Volume_Purchasing.html

Back up and restore app documents and data

App documents and data may be included when you back up an iOS or iPadOS device to iCloud, Finder, or iTunes, depending on the options you choose when MDM installs an app:

- If you choose "Prevent backup of the app data," users can't back up or restore documents and data for that app.
- If you choose "Remove app when MDM profile is removed," users can back up data for that app, but they can restore the data only to the same device. If they restore the backup to a new device, the data isn't restored.
- If you choose neither option, users can back up and restore app data to the same device or a new device. Some apps may also choose to exclude data from backups, or prevent their data from being restored to a different device.

For more information, see your MDM solution documentation.

Reinstall managed apps

If the data in a managed app is restored from iCloud, the app will be reinstalled automatically if it was assigned to a user. It also will be reinstalled automatically if it was assigned to a device and the backup was restored to the same device.

The app won't be reinstalled automatically if the backup is restored by Apple Configurator, Finder, or iTunes.

If the app wasn't reinstalled automatically, MDM can reinstall it.

https://support.apple.com/en-us/HT205199

Restoring iOS user data after moving into the Automatic Device Enrolment Program

5 months ago · Updated

When an iCloud backup is restored to the same device, all supervision and profiles come from the backup regardless of how it was configured in the Automatic Device Enrolment Program (previously known as the Device Enrolment Program). For this reason, when restoring backups each user should transition to a new or different device to ensure Automatic Device Enrolment Program supervision and MDM enrolment are enforced and functional.

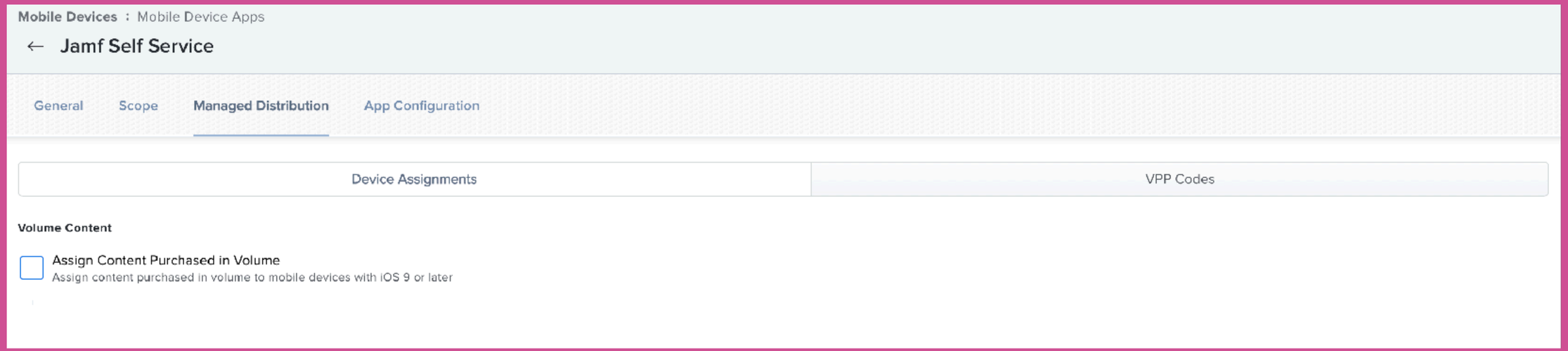
Examples:

- If you configure a device to be supervised and enrolled in MDM using the Automatic Device Enrolment Program, then restore a backup made when the same device was unsupervised, the device will be unsupervised.
- If you configure a device to be supervised and enrolled in MDM using the Automatic Device Enrolment Program, then restore a backup made when the same device was supervised and enrolled, the device will have a broken enrolment and the state will be undefined, and unsupported
- If you restore a backup made when the same device was supervised by Apple Configurator and enrolled in MDM, the device will remain supervised and enrolled, but the MDM profile will be removable, because Apple Configurator cannot lock MDM enrollment.
- If you restore the backup to a different device that is configured for supervision and MDM enrolment via the Automatic Device Enrolment Program, the device will remain supervised and MDM enrolment will not be removable.

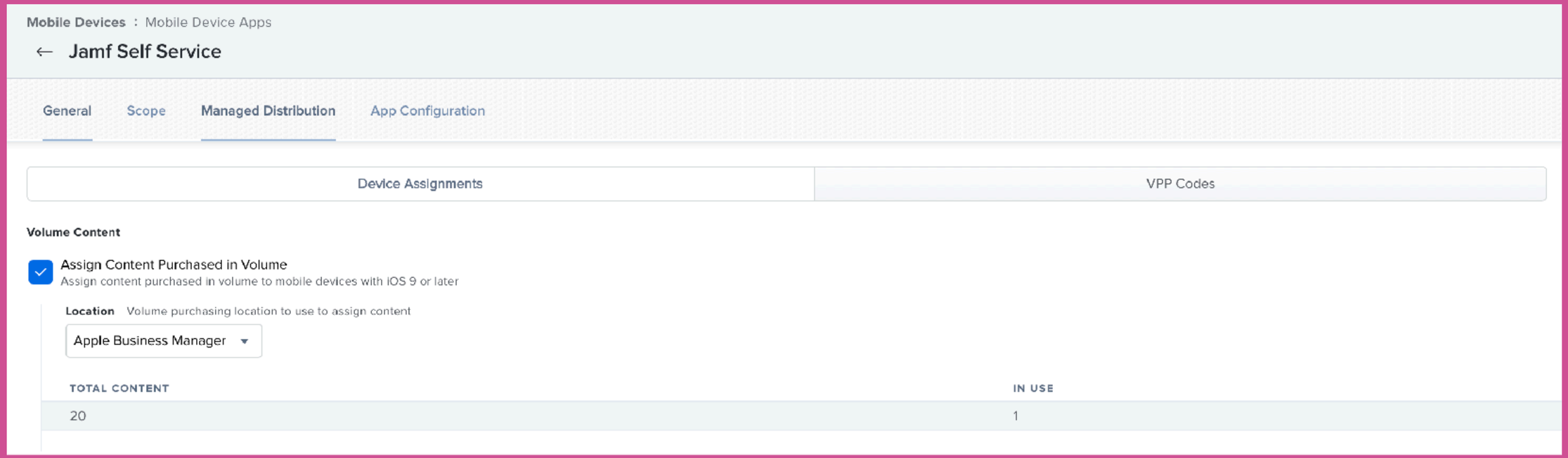
https://support.datajar.co.uk/hc/en-us/articles/206944489

- *Mark apps as non-removable:* In iOS 14 and iPadOS 14, managed apps have the ability to be marked as non-removable. Previously, administrators had to completely lock the Home Screen and prevent the deletion of all apps, which constrained the user's ability to manage their own apps. Users can continue to rearrange their apps, install new apps and delete other apps they've installed. Administrators can mark their mission-critical managed apps as non-removable. When users try to delete or offload a managed app, it prevents it and displays an alert. Non-removable managed apps ensure that an organisation's users always have the apps they need on their devices.

https://support.apple.com/en-gb/guide/deployment-reference-ios/iorf4d72eded/web



https://docs.jamf.com/jamf-pro/administrator-guide/Apps_Purchased_in_Volume.html



https://docs.jamf.com/jamf-pro/administrator-guide/Apps_Purchased_in_Volume.html

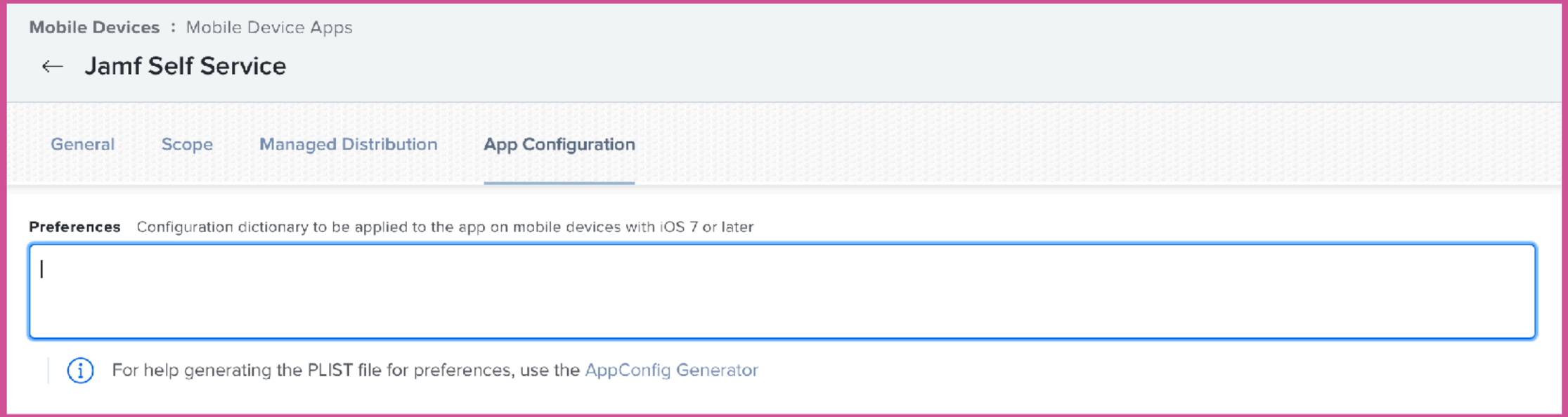
Failed Commands

Cancel All

COMMAND	ERROR	DATE ISSUED	DATE OF LAST PUSH	USERNAME	
Install App - Self Service	Please log in to your iTunes Store account.	Today at 3:04 PM	Today at 3:49 PM		Cancel

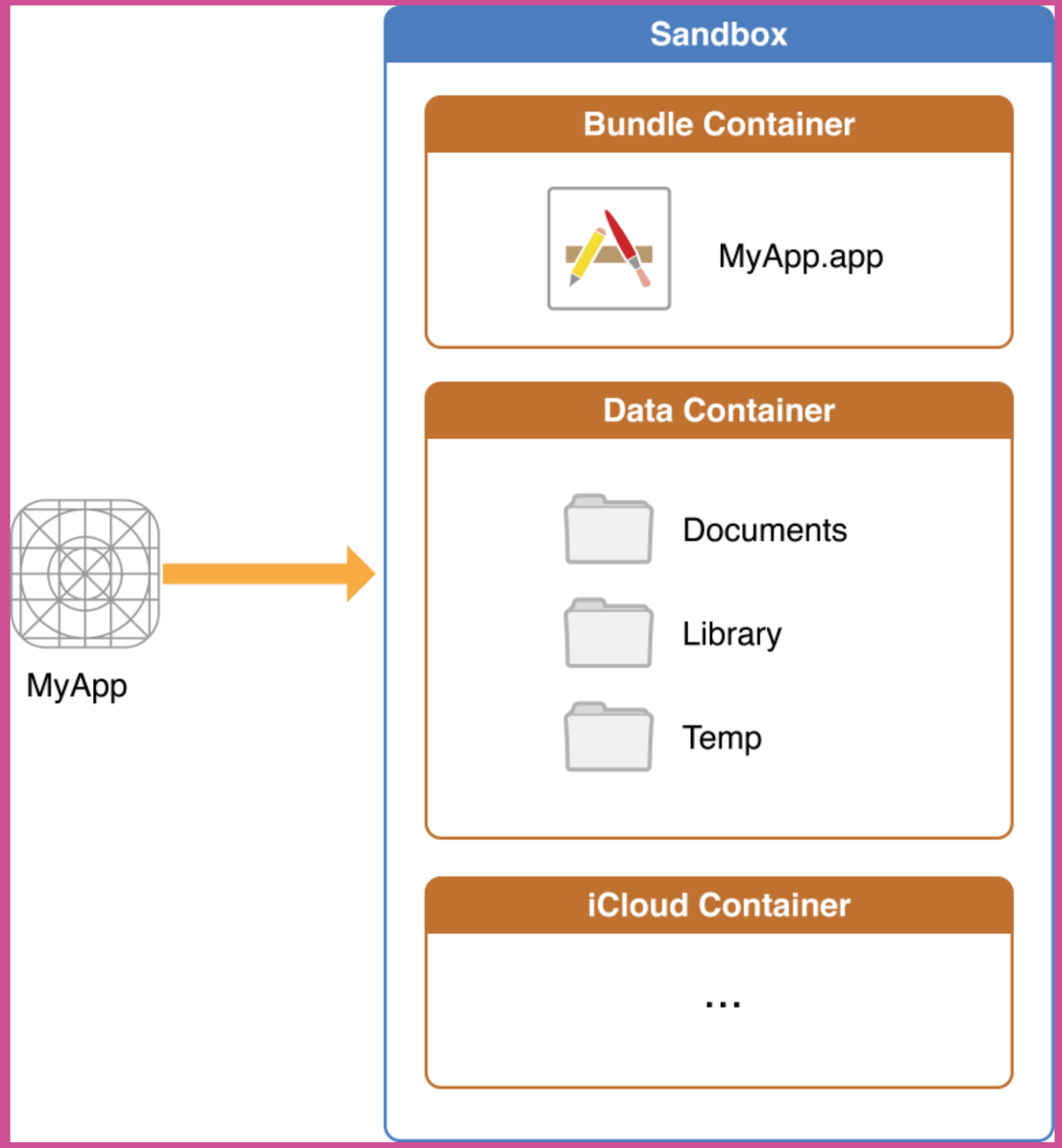
dataJAR
Beyond Device Management

virtual JNUC 2021

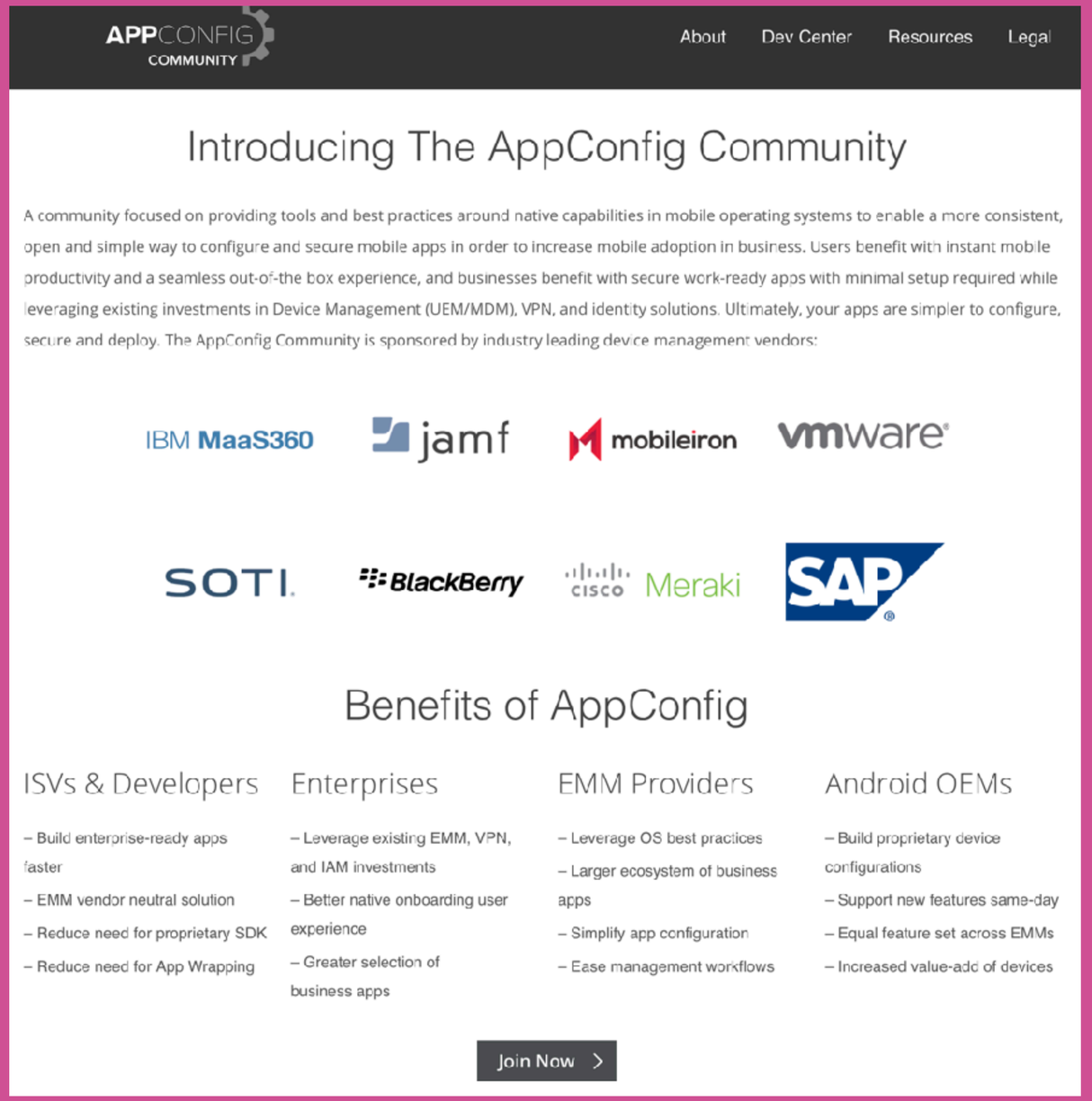


- *App configuration:* App developers can identify configuration settings that can be set before or after the app is installed as a managed app.

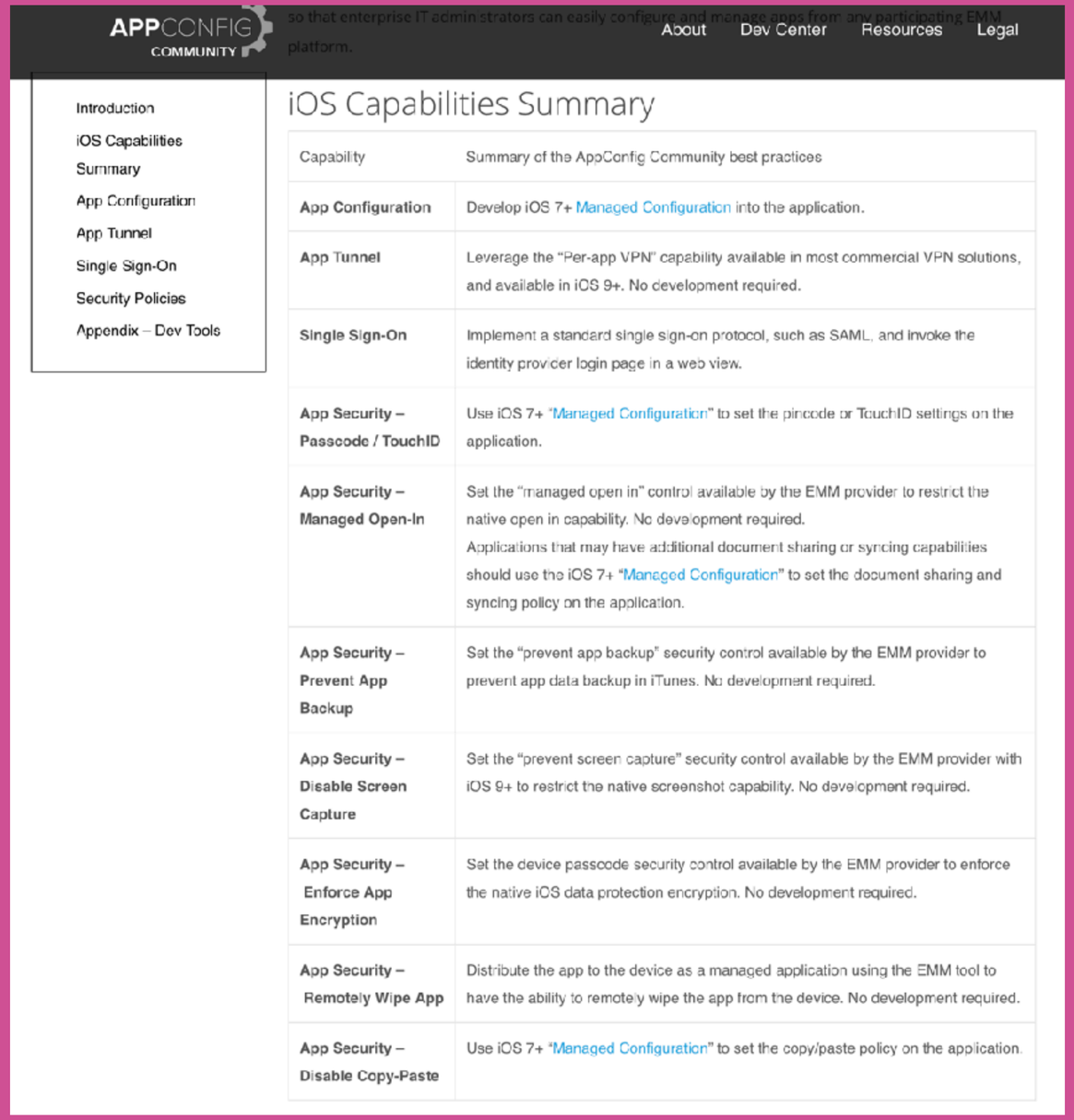
https://support.apple.com/en-gb/guide/deployment-reference-ios/iorf4d72eded/web



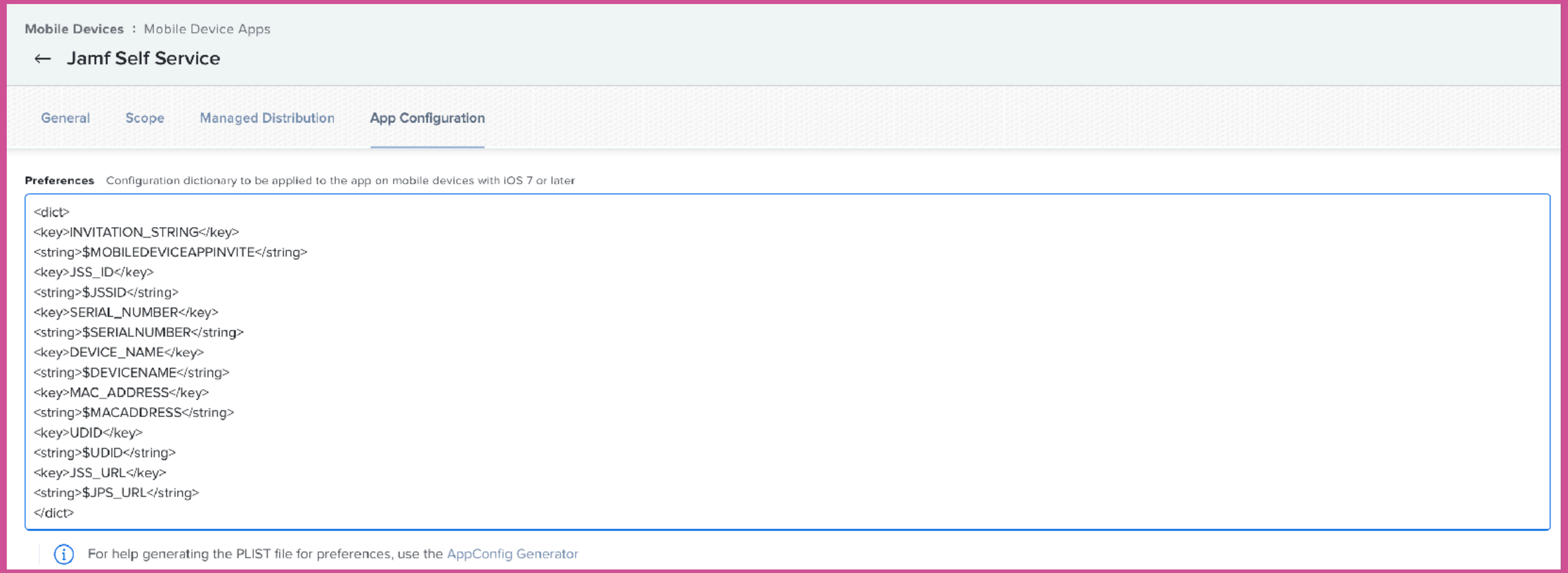
https://macmule.com/2016/12/11/profiles-an-it-admins-best-friend/



https://www.appconfig.org/



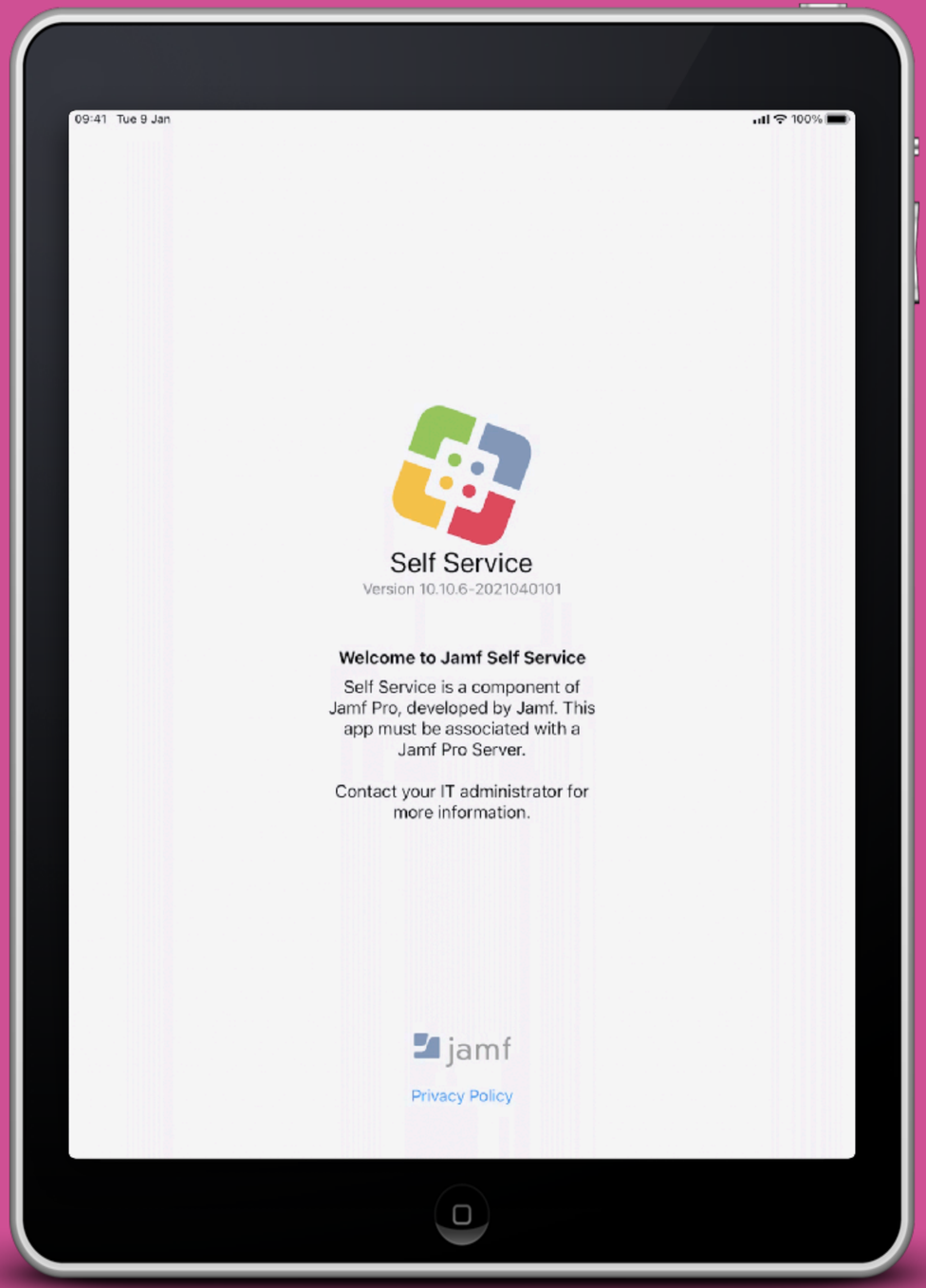
https://www.appconfig.org/ios/



https://docs.jamf.com/jamf-pro/administrator-guide/Jamf_Self_Service_for_iOS.html

dataJAR
Beyond Device Management

virtual JNUC 2021



dataJAR
Beyond Device Management

Automated Device Enrollment

virtual JNUC 2021

Manually add devices to Apple School Manager or Apple Business Manager

You can choose to add iPhone, iPad, and Apple TV devices to Apple School Manager or Apple Business Manager using Apple Configurator 2, even if the devices weren't purchased directly from Apple, an Apple Authorized Reseller, or an authorized cellular carrier. When you set up a device that has been manually enrolled, it behaves like any other enrolled device, with mandatory supervision and mobile device management (MDM) enrollment. For devices that weren't purchased directly, the user has a 30-day provisional period to remove the device from enrollment, supervision, and MDM. The 30-day provisional period begins after the device is activated.

There are two ways to add devices to one of the programs:

- *You don't enable "Activate and complete enrollment":* You have a new or existing device that requires unique user authentication to enroll in MDM. The device is left at the Setup Assistant, and the user completes the enrollment.
- *You enable "Activate and complete enrollment":* You have an existing device that already has a record in, and is managed by, your MDM solution. This can include managing all the Setup Assistant panes so the user gets a device that's ready to use.

https://support.apple.com/en-gb/guide/apple-configurator-2/cad99bc2a859/mac

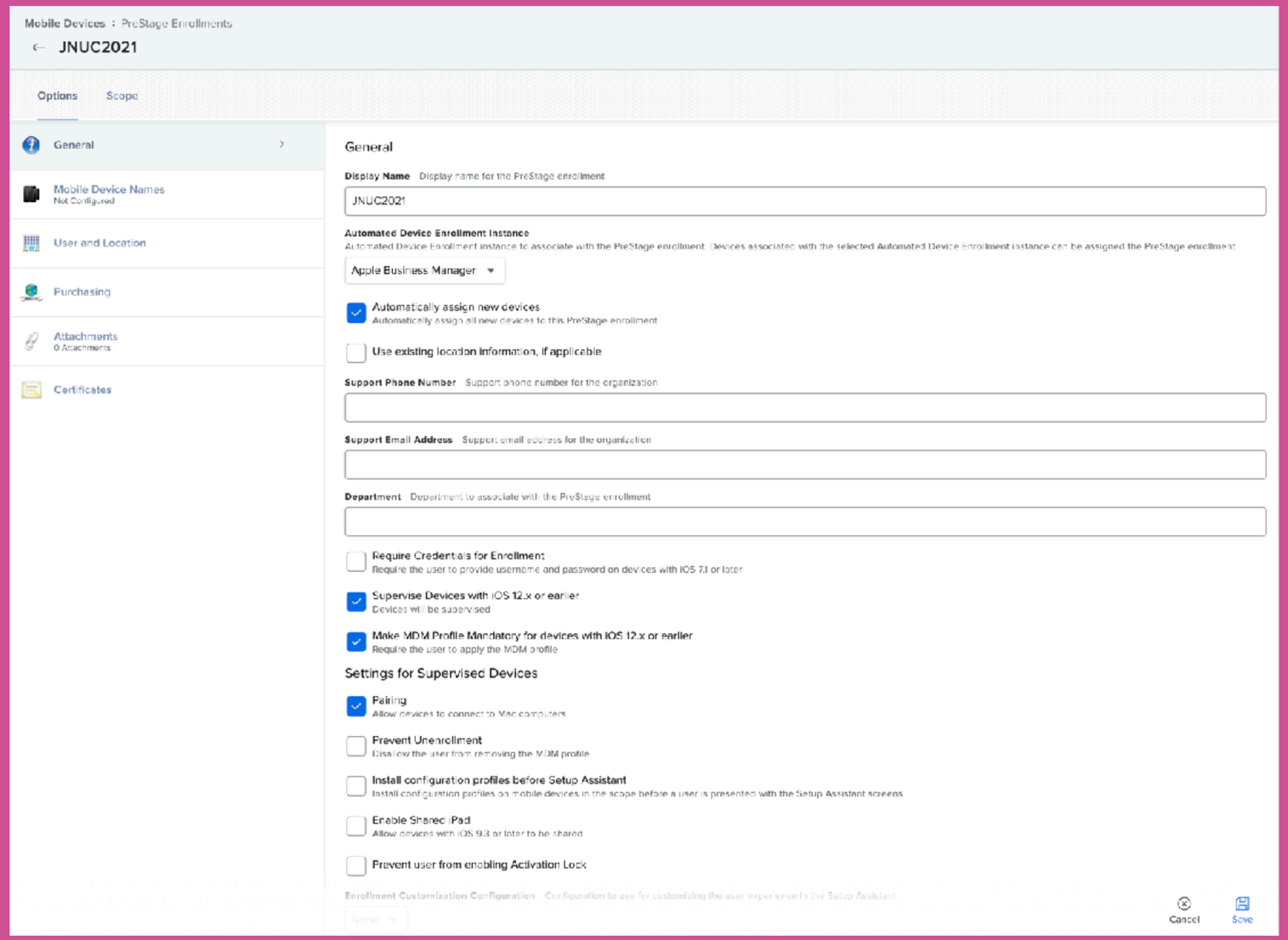
Workflow Two: Use Apple Configurator 2.5 to bring devices into Apple School Manager

This workflow is ideal for devices you purchased through a non-Apple authorized reseller, for donated devices or for re-adding a device that was accidentally released from Apple School Manager.

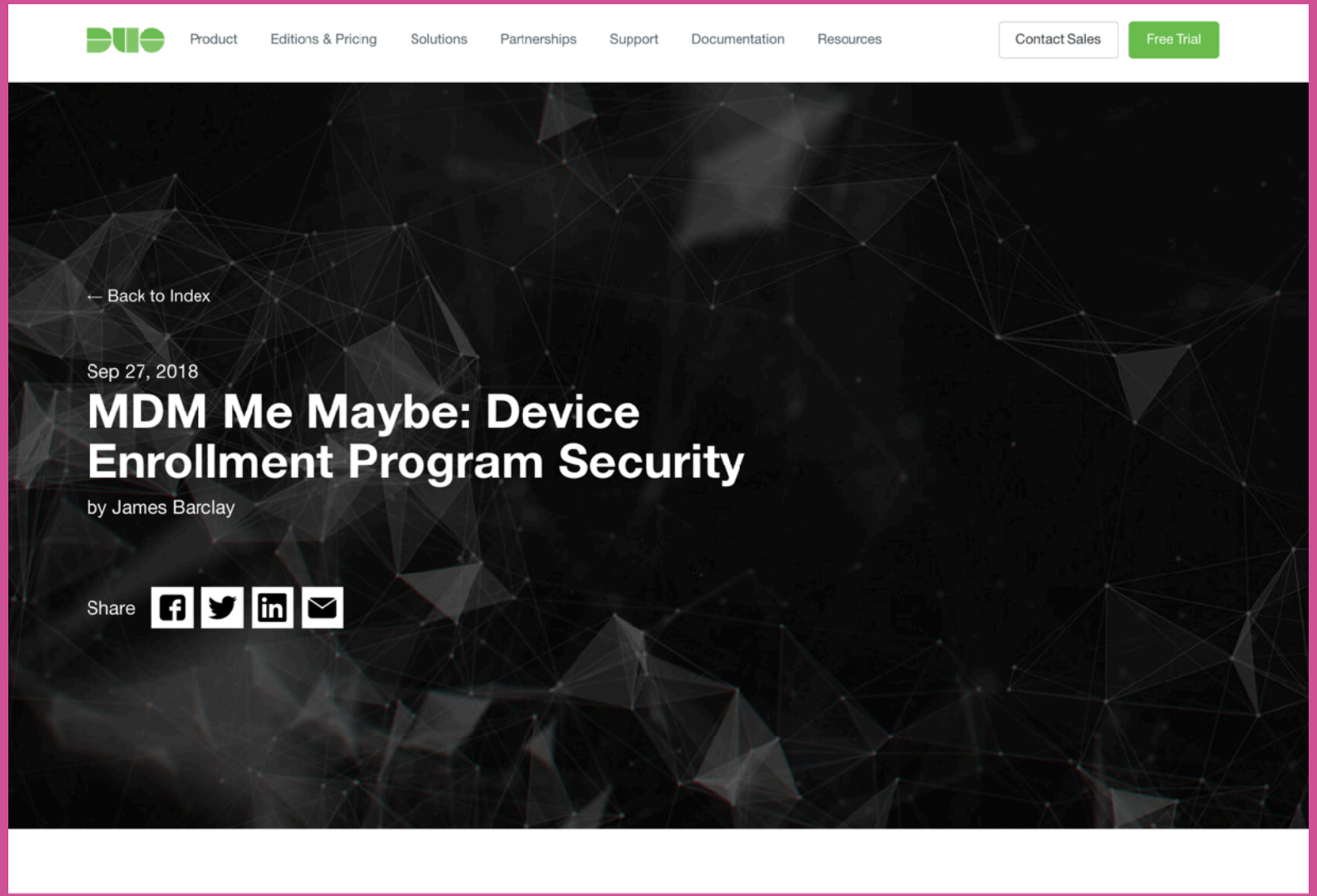
Steps:

1. In Apple Configurator 2.5, go to Preferences > Organizations and add a new organization (use your Apple School Manager Apple ID)
2. Generate a new supervision identity
3. Then select the servers icon and create a new server
4. Enter a display name for your MDM server and the complete URL of your Jamf Pro server
5. Select "Next" when "Unable to verify the server's enrollment URL" page loads
6. Select your iPad and then "Prepare"
7. Select Manual Configuration and "Add to Device Enrollment Program." Then, supervise the device and allow the device to pair with others
8. Select the MDM server that you created in step four
9. Select the organization you created in step two
10. Select the steps you want to show
11. Add a Wi-Fi profile, if wanted, and select "Prepare"
12. This will wipe the device
13. Once device is wiped and displays the setup assistant, you will see a message that the MDM profile can be removed within 30 days. (Be sure to let those devices wait for the 30 days so they cannot be removed from Apple School Manager)
14. In Apple School Manager, go to "Settings" and under the "MDM Servers" section, select "Apple Configurator 2." Then select "Show Devices" and then select one or several devices. Select "Edit Device Management" and move them to your chosen MDM server
15. In Jamf Pro, confirm your devices are available under Global Management > Automated Device Enrollment. Once confirmed, go to your PreStage and make sure your new devices are selected. Then, wipe your devices again to have them enroll into your Jamf Pro server

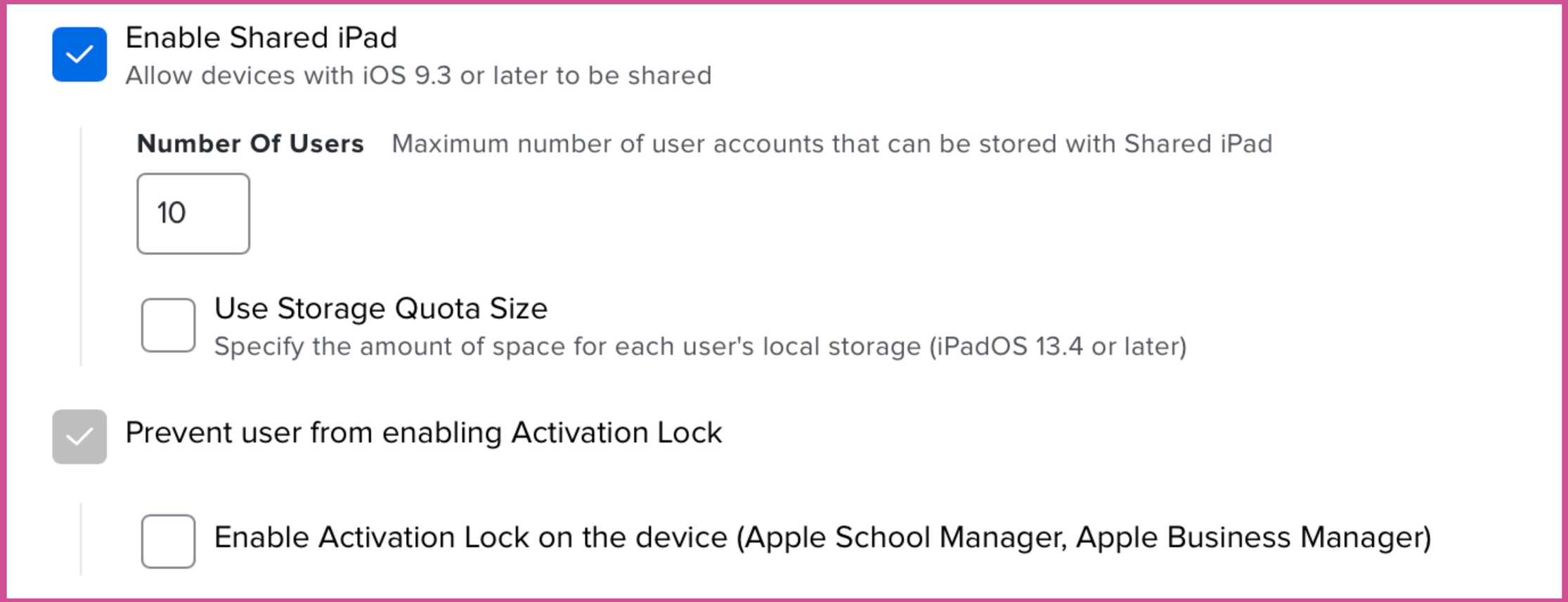
https://www.jamf.com/blog/three-ways-to-get-ios-devices-enrolled-into-management/



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_PreStage_Enrollments.html

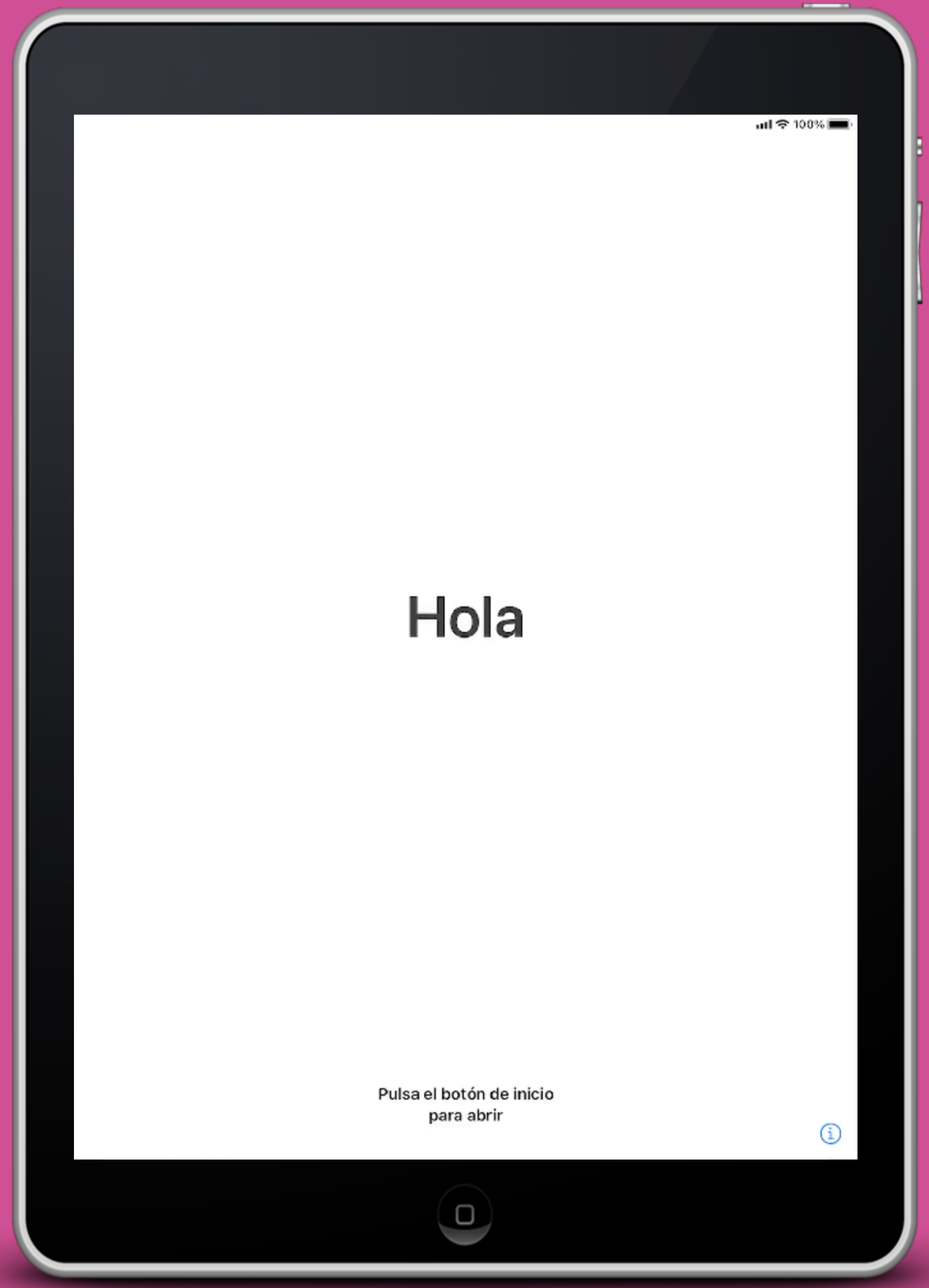


https://duo.com/labs/research/mdm-me-maybe



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_PreStage_Enrollments.html

dataJAR
Beyond Device Management



virtual JNUC 2021

Content caching

Content caching is extremely important for Shared iPad. If you configure content caching to cache iCloud data (including iCloud Photos and CloudKit-enabled apps), Shared iPad saves data to iCloud through the caching service. When a user's data is cached by macOS 10.13 or later, Shared iPad can download the data locally instead of from iCloud.

When a user signs out of an iPad that data is held locally *and* appears automatically in iCloud. When that user signs into a *different* iPad, their data is downloaded from iCloud or by other apps from the App Store that use cloud-based storage.

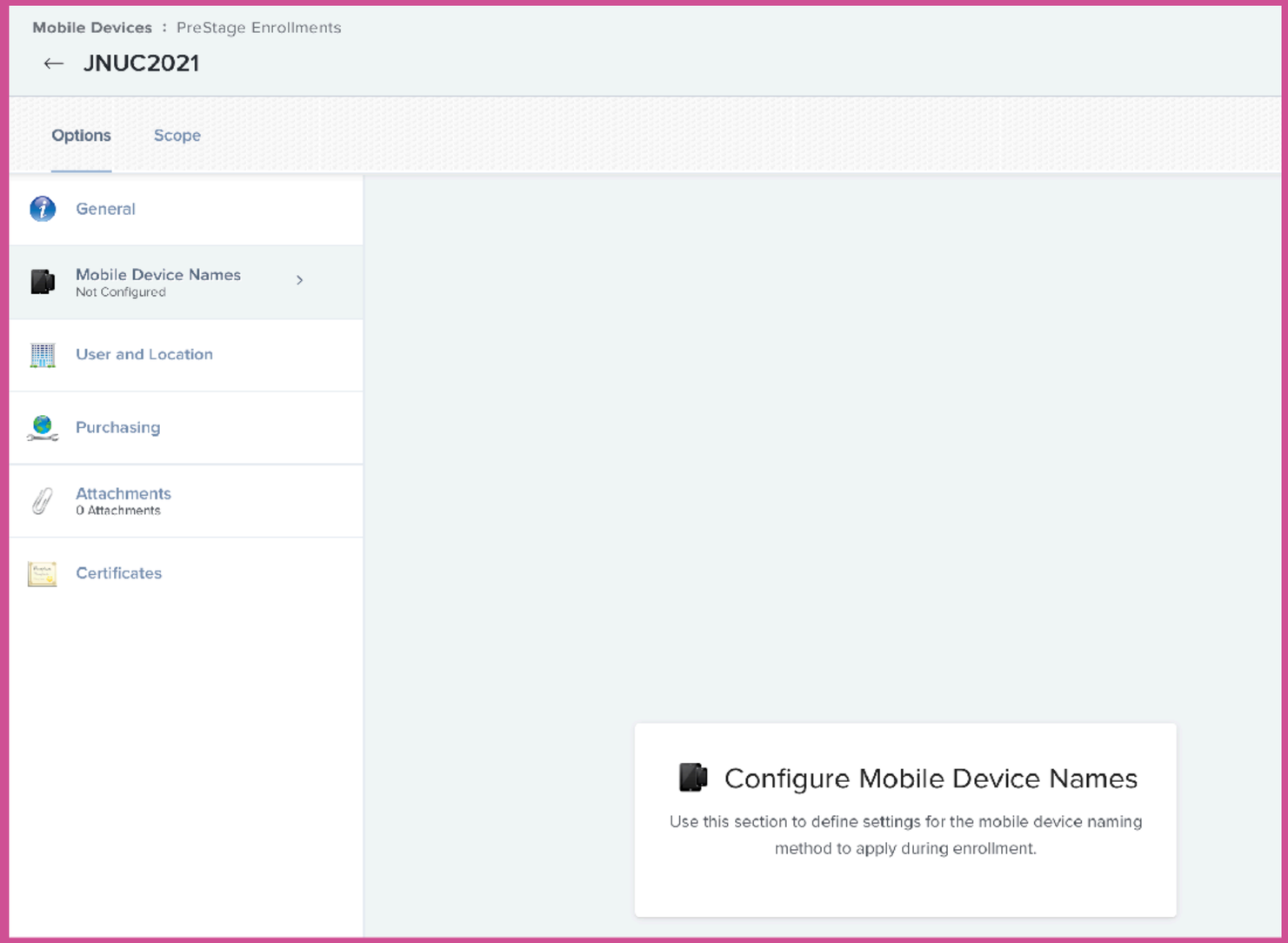
It's recommended that you plan for users to return to the same device each time. With the use of intelligent caching by Shared iPad and the Classroom app, a user can sign out one day and sign back the following day to the same iPad they last used. This lets them quickly pick up where they left off because their data is still on the same iPad.

https://support.apple.com/en-gb/guide/mdm/mdm71124b400/1/web/1

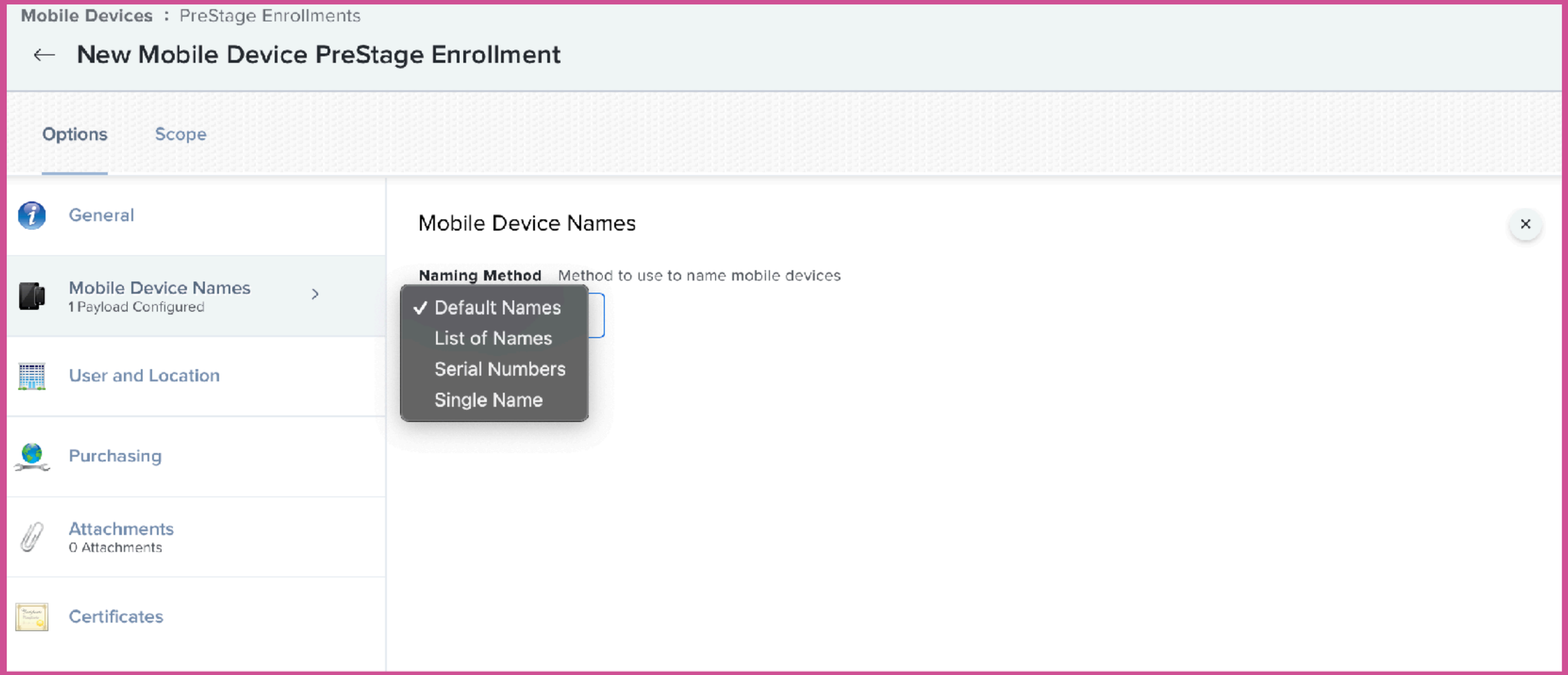
Services	Platform	Description
Apple Pay	iOS iPadOS macOS	The user cannot use it.
Specific iCloud features	iOS iPadOS macOS Web	The user cannot access the following services: • iCloud Mail • iCloud Family Sharing • Allow iMessage in iCloud • iCloud Keychain (although keychain items are saved and restored on Shared iPad devices)
App Store iTunes Store Apple Books	iOS iPadOS macOS	Allows browsing but not purchasing, paid or free.

https://support.apple.com/en-gb/guide/apple-business-manager/tes78b477c81/1/web/1

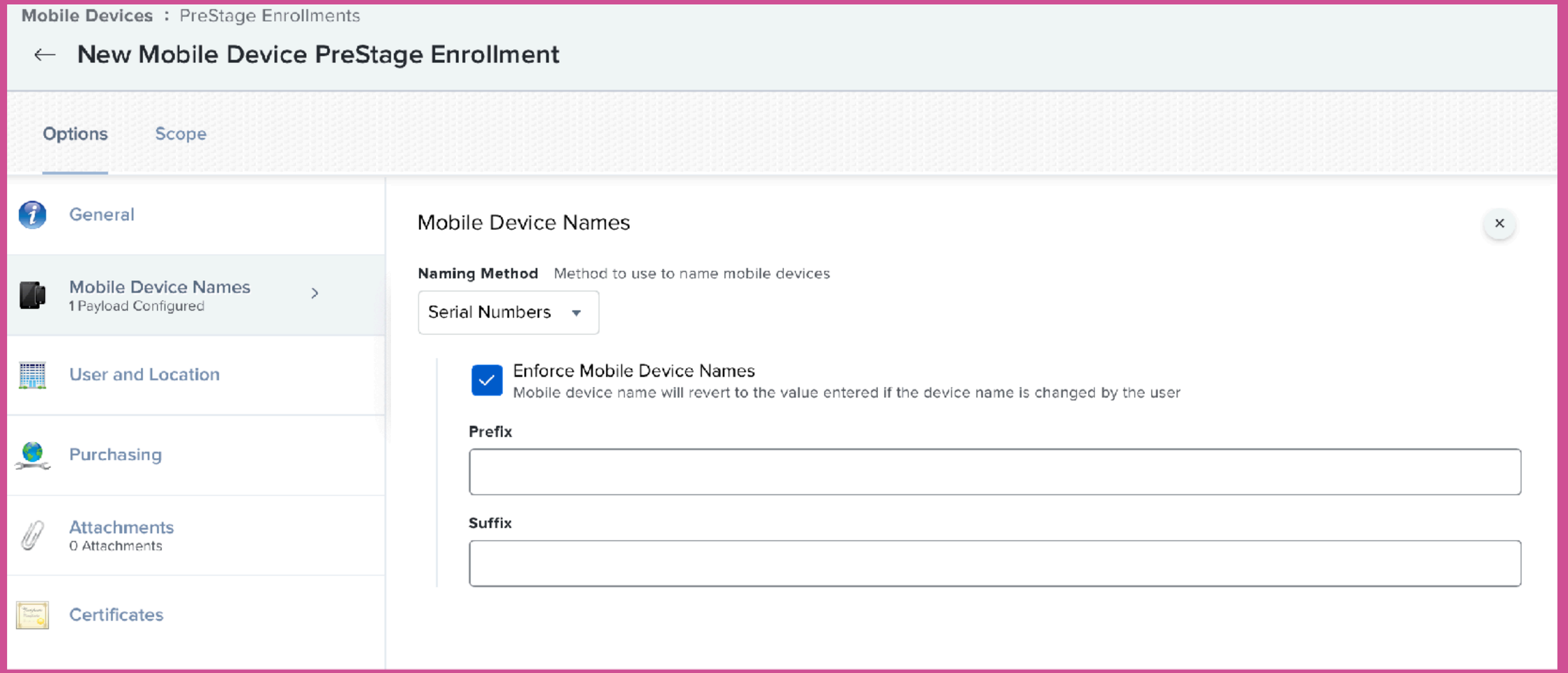
https://support.apple.com/en-gb/guide/apple-school-manager/tes78b477c81/1/web/1



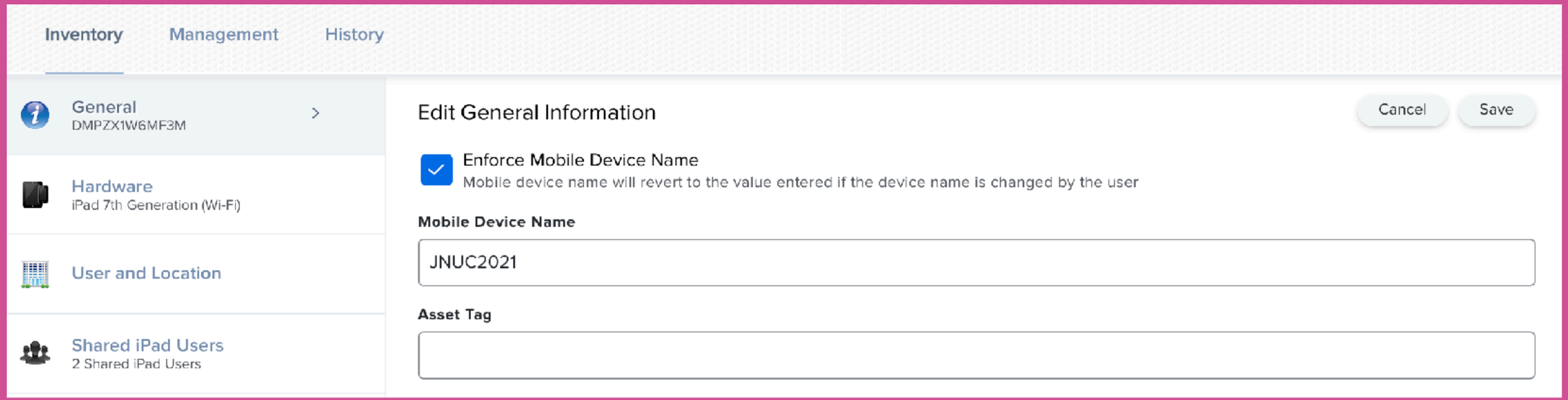
https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_PreStage_Enrollments.html



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_PreStage_Enrollments.html

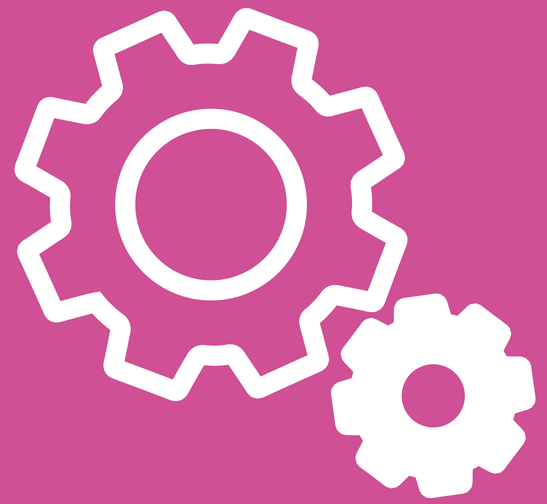


https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_PreStage_Enrollments.html

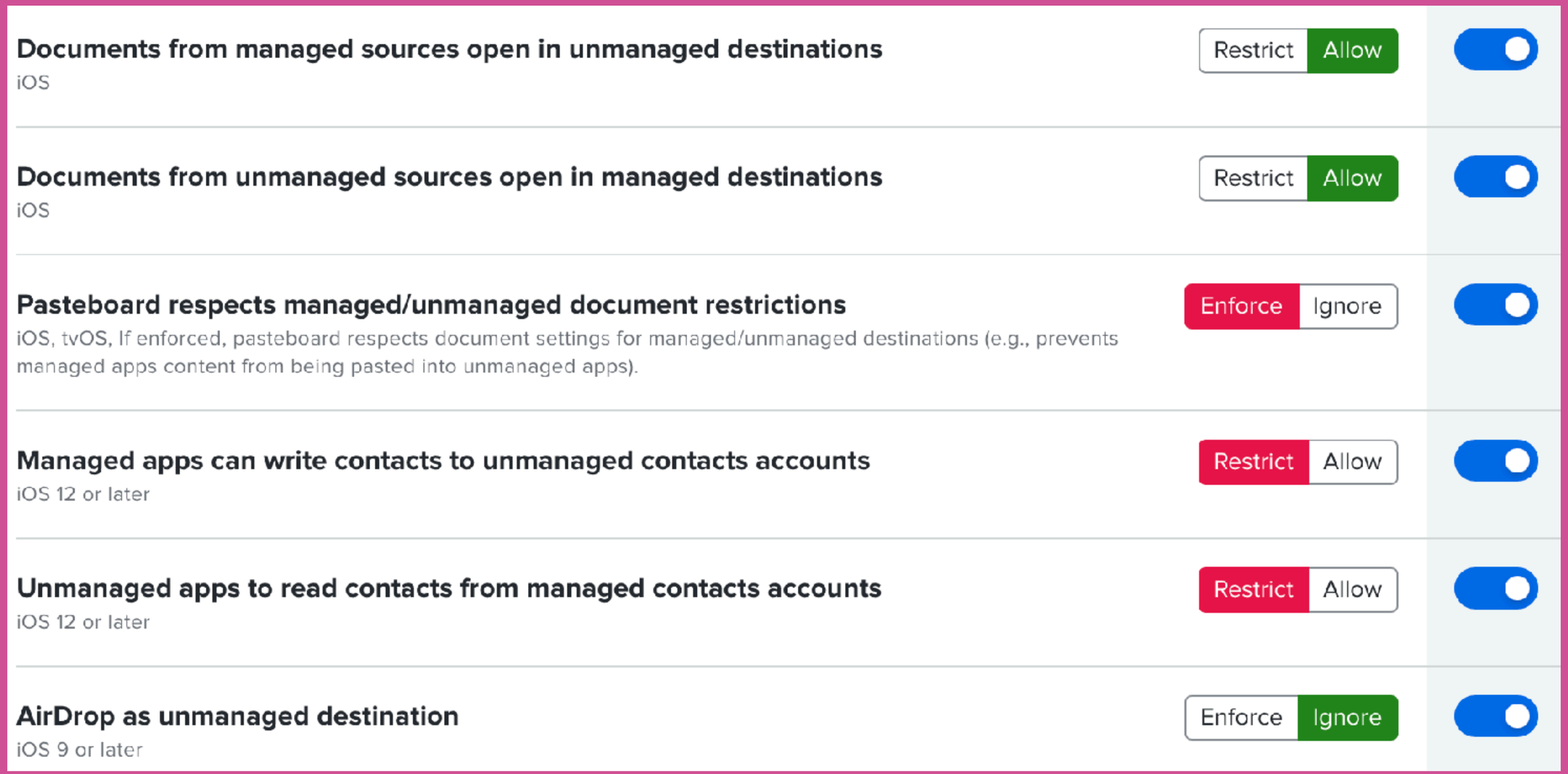


dataJAR
Beyond Device Management

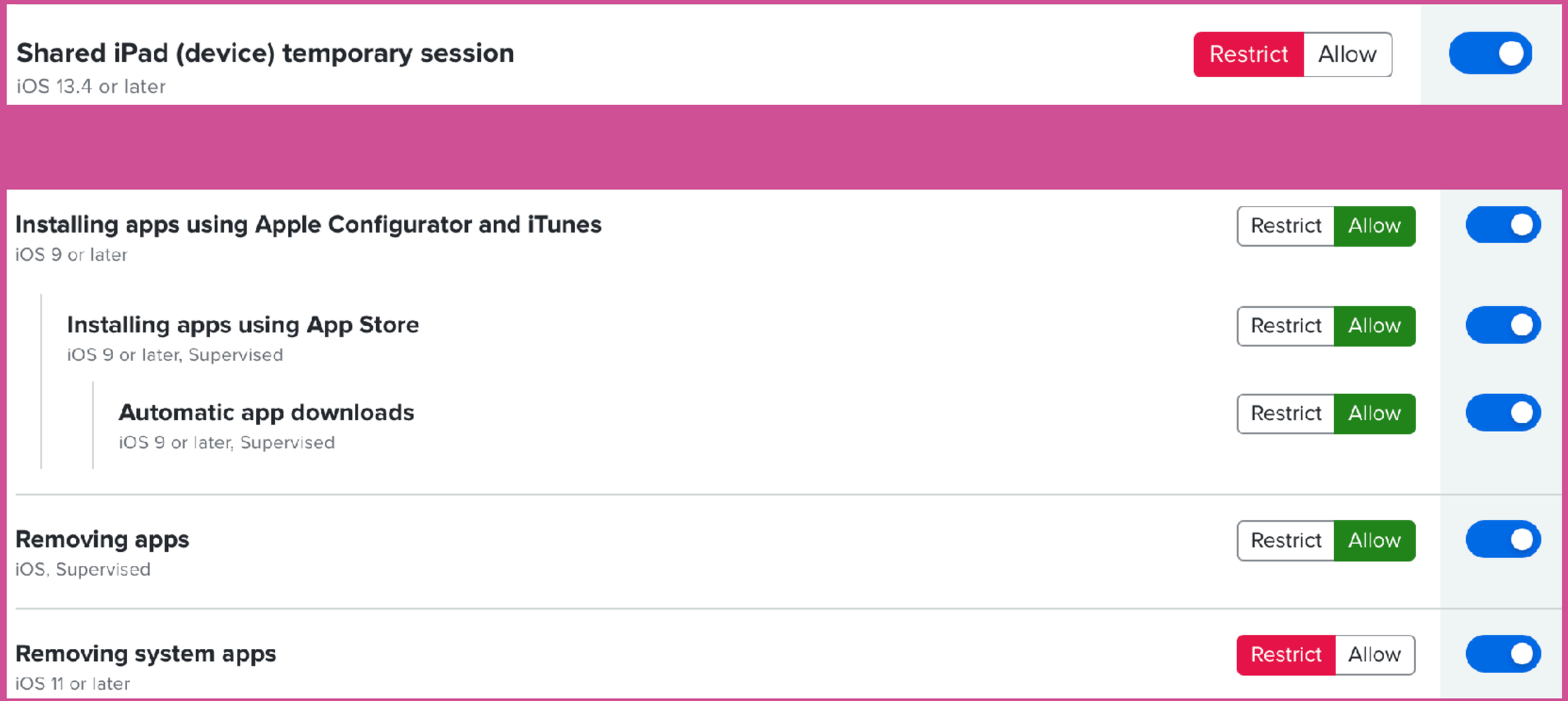
Device Management Settings



virtual JNUC 2021



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

Delete built-in Apple apps on your iOS 12, iOS 13, iPadOS device or Apple Watch

With iOS 12, iOS 13 and iPadOS, you can delete some built-in Apple apps from your iPhone, iPad, iPod touch or Apple Watch.

When you delete a built-in app from your device, you also delete any related user data and configuration files. This can affect things like related system functions or information on your Apple Watch.

Built-in apps that you can delete from your device

If you have iOS 12, iOS 13 or iPadOS 13, you can delete[1] these apps from your device:

- Activity
- Apple Books[4]
- Calculator
- Calendar
- Compass
- Contacts[2]
- FaceTime[3]
- Files
- Find My Friends (iOS 12 only)
- Home
- iTunes Store
- Mail
- Maps[4]
- Measure
- Music[4]
- News (where available)
- Notes
- Podcasts[4]
- Reminders
- Stocks
- Tips
- TV (where available)
- Videos
- Voice Memos
- Watch app[5]
- Weather

https://support.apple.com/en-gb/HT208094

https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

Use parental controls on your child's iPhone, iPad and iPod touch

With Content & Privacy Restrictions in Screen Time, you can block or limit specific apps and features on your child's device. You can also restrict the settings on your iPhone, iPad or iPod touch for explicit content, purchases and downloads, and privacy.

Set Content & Privacy Restrictions	Prevent iTunes & App Store purchases	Allow built-in apps and features
Prevent explicit content and content ratings	Prevent web content	Restrict Siri web search
Restrict Game Center	Allow changes to privacy settings	Allow changes to other settings and features

https://support.apple.com/en-gb/HT201304

https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

Using USB accessories with iOS 11.4.1 and later

You may need to unlock your passcode-protected iPhone, iPad or iPod touch to connect it to a Mac, PC or USB accessory.

Starting with iOS 11.4.1, if you use USB accessories with your iPhone, iPad or iPod touch, or if you connect your device to a Mac or PC, you may need to unlock your device to enable it to recognise and use the accessory. Your accessory will then remain connected, even if your device is subsequently locked.

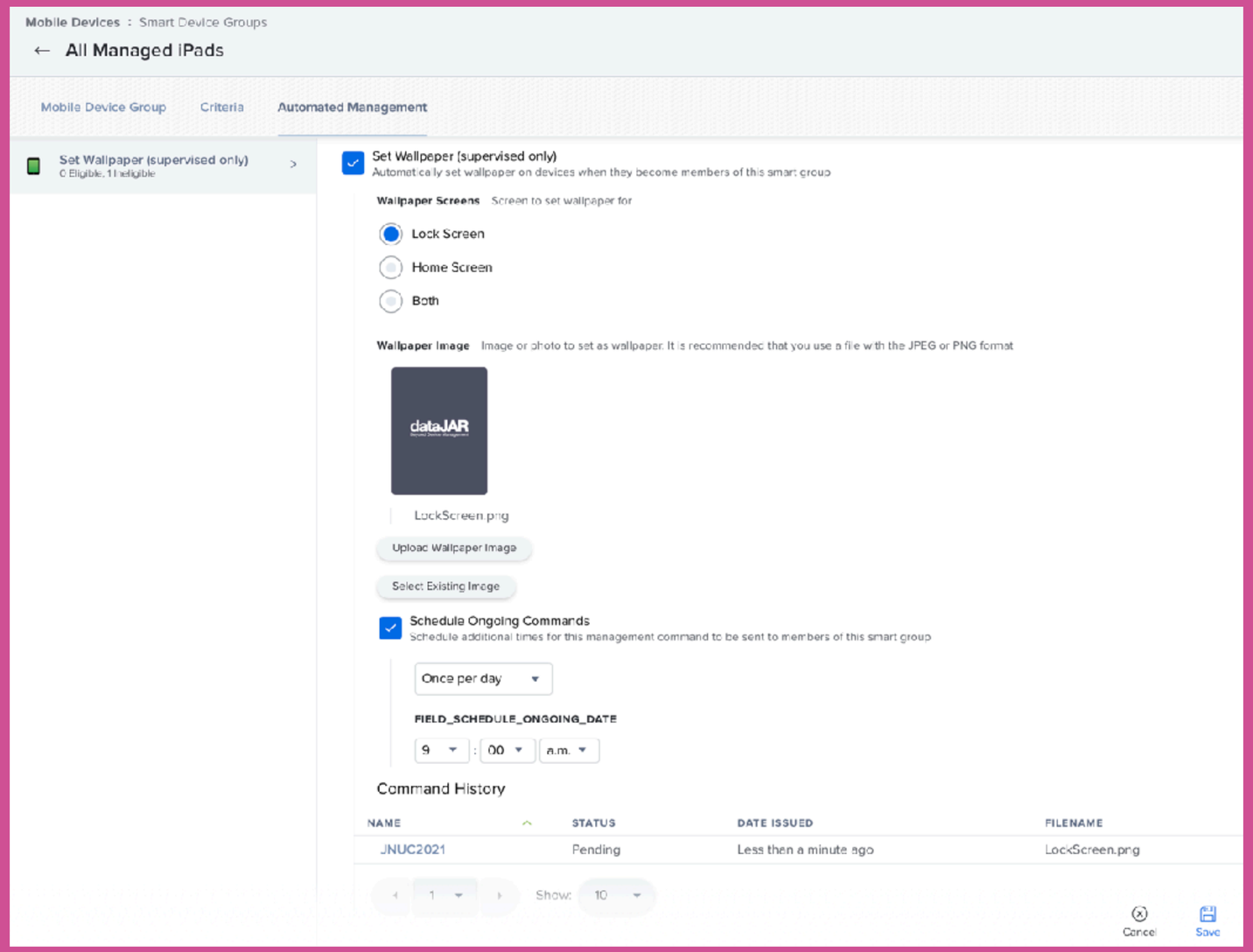
If you don't unlock your password-protected iOS device first – or you haven't unlocked and connected it to a USB accessory within the past hour – your iOS device won't communicate with the accessory or computer, and in some cases it may not charge. You may also see an alert asking you to unlock your device to use accessories.

If the USB accessory is still not recognised after you've unlocked your device, disconnect your device from the accessory, unlock your device and reconnect the accessory.

Your iPhone, iPad or iPod touch charges as usual when it's connected to a USB power adapter.

https://support.apple.com/en-gb/HT208857

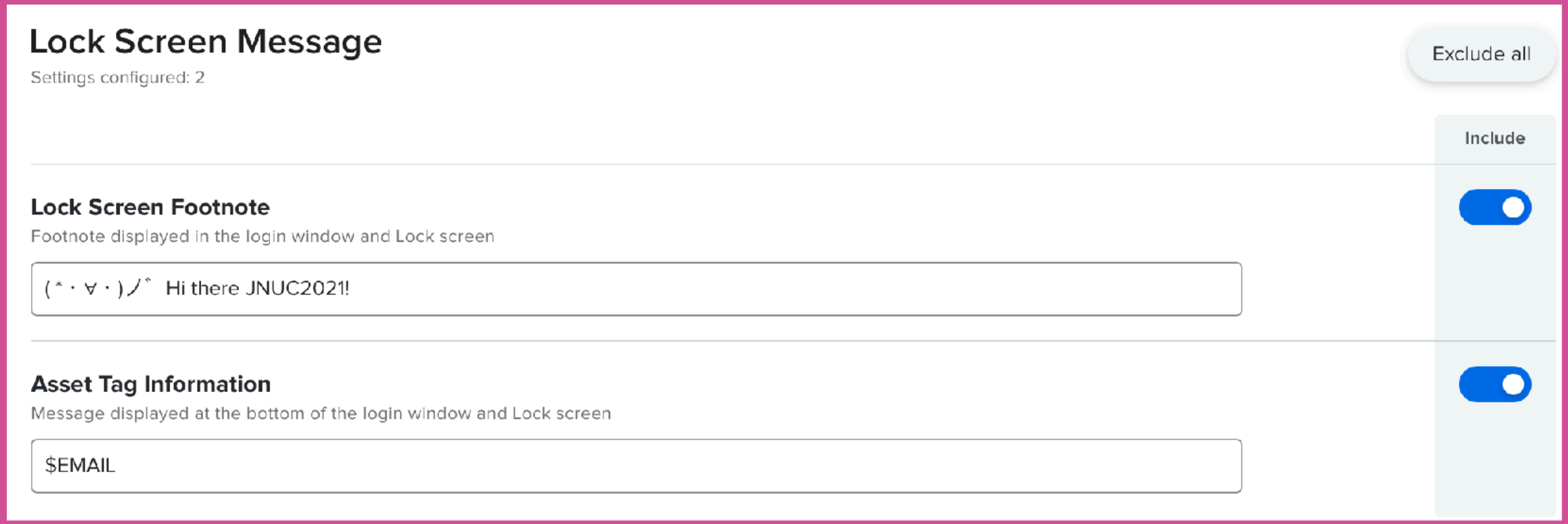
https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html



https://docs.jamf.com/jamf-pro/administrator-guide/Smart_Groups.html

dataJAR
Beyond Device Management

virtual JNUC 2021



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

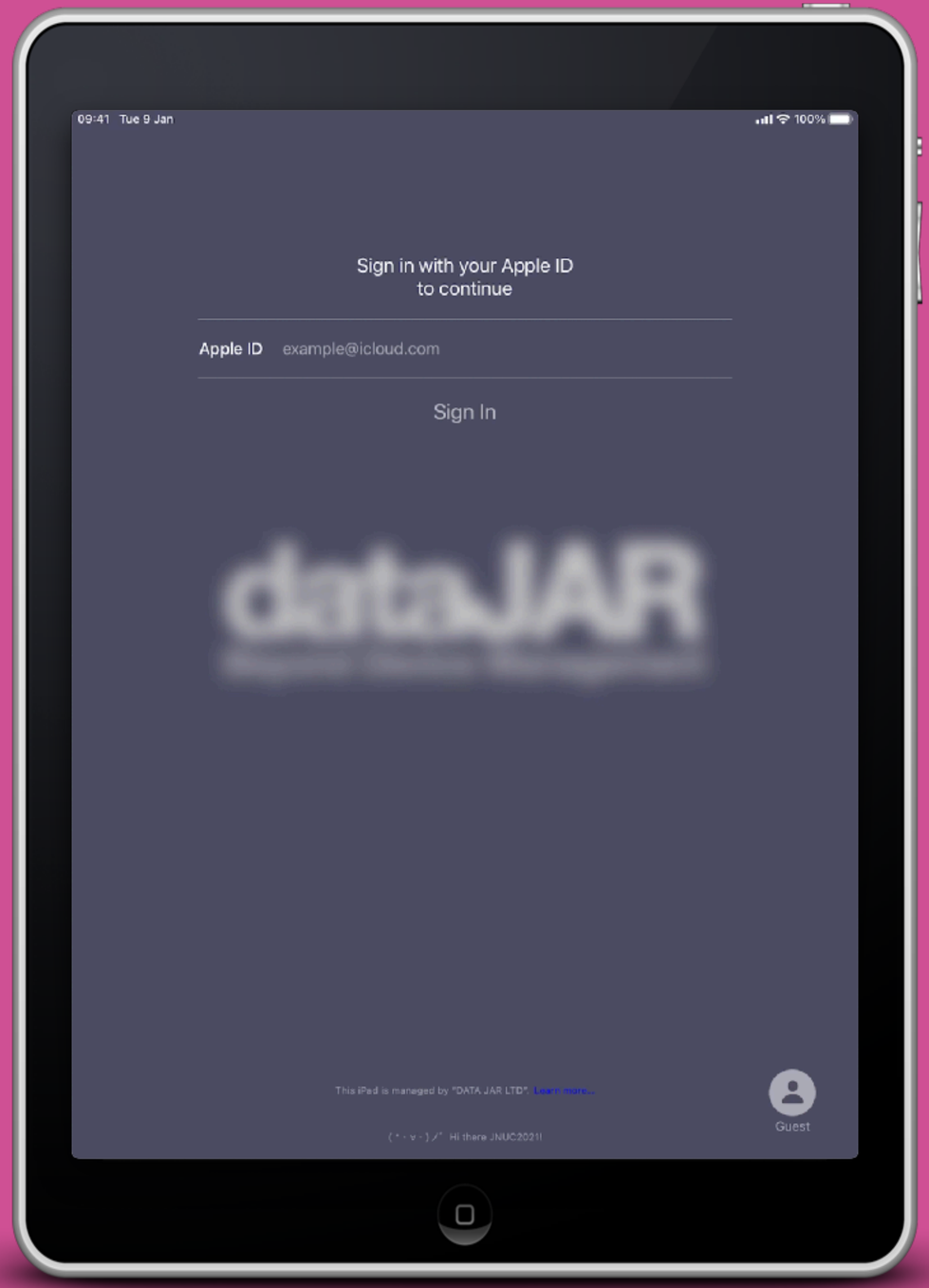
dataJAR
Beyond Device Management

virtual JNUC 2021

dataJAR
Beyond Device Management

virtual JNUC 2021

dataJAR
Beyond Device Management



virtual JNUC 2021

https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

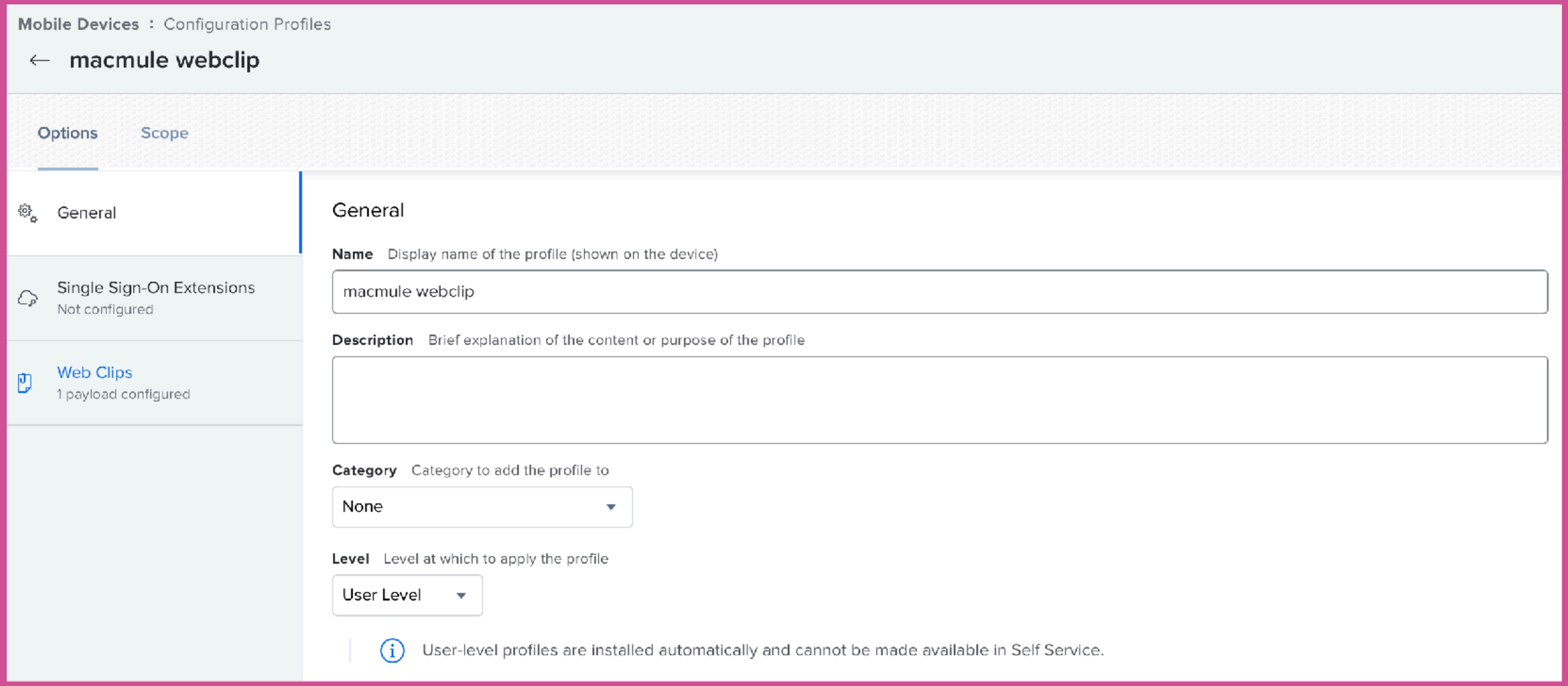
dataJAR
Beyond Device Management

virtual JNUC 2021

Failed Commands

COMMAND	ERROR	DATE ISSUED
Install Configuration Profile macmule webclip	The payload type “com.apple.webClip.managed” is not permitted to be installed for the system in multi-user mode.	About a minute ago

https://docs.jamf.com/jamf-pro/administrator-guide/Smart_Groups.html



https://docs.jamf.com/jamf-pro/administrator-guide/Smart_Groups.html

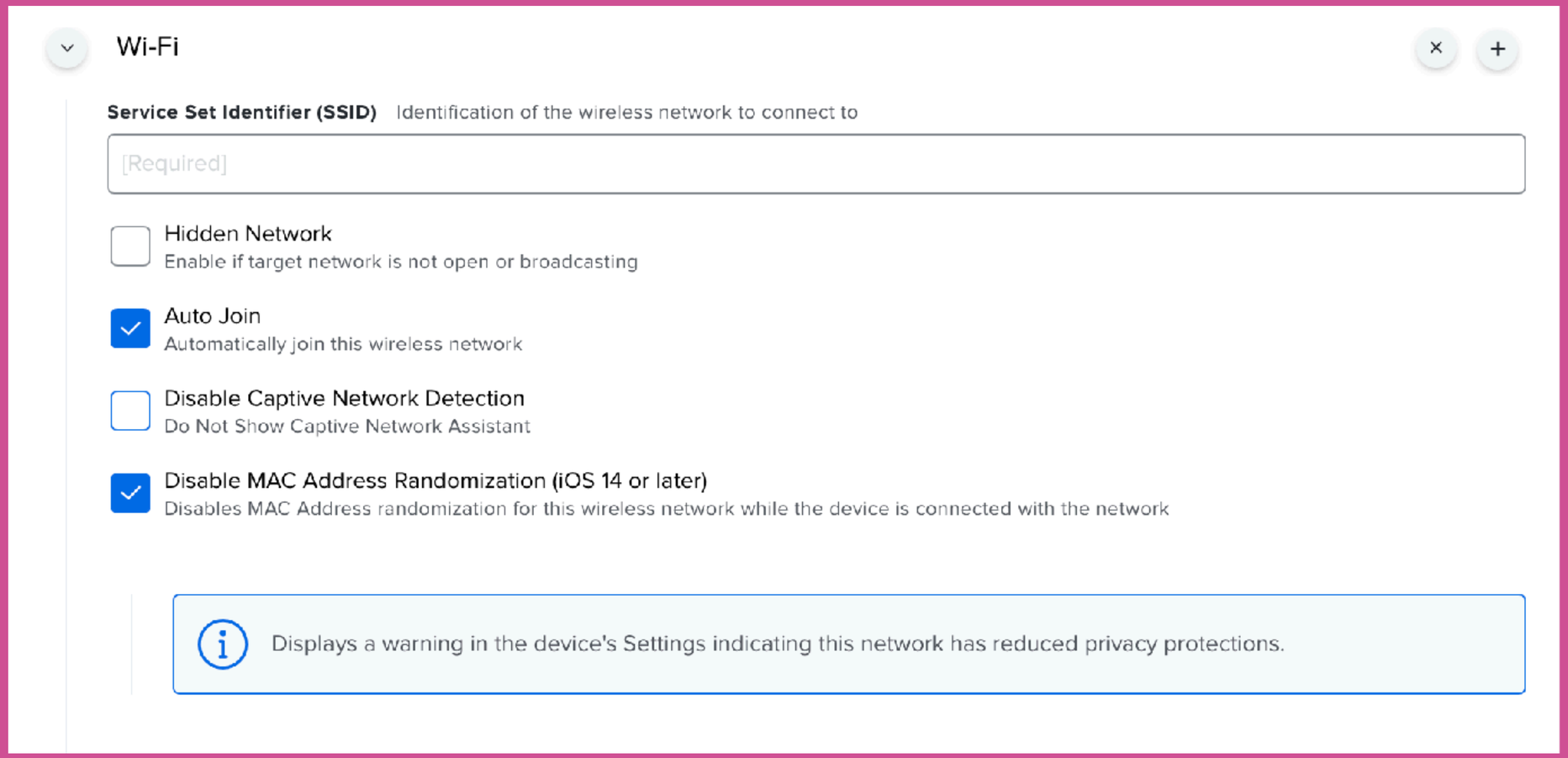
Use private Wi-Fi addresses in iOS 14, iPadOS 14 and watchOS 7

To further protect your privacy, your iPhone, iPad, iPod touch or Apple Watch can use a different MAC address with each Wi-Fi network.

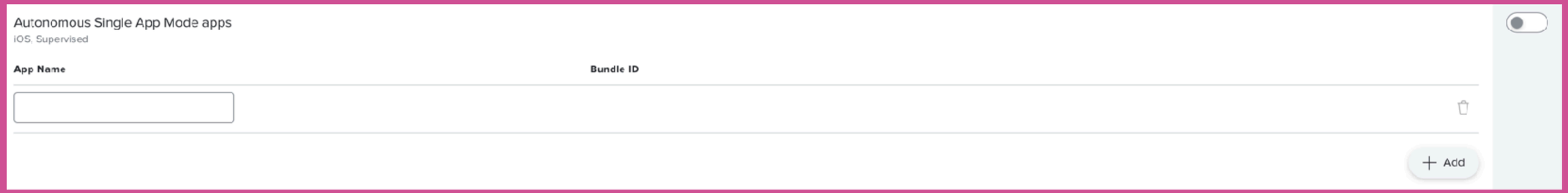
To communicate with a Wi-Fi network, a device must identify itself to the network using a unique network address called a media access control (MAC) address. If the device always uses the same Wi-Fi MAC address across all networks, network providers and other network observers can more easily relate that address to the device's network activity and location over time. This allows a kind of user tracking or profiling, and it applies to all devices on all Wi-Fi networks.

To reduce this privacy risk, iOS 14, iPadOS 14 and watchOS 7 use a different MAC address for each Wi-Fi network. This unique, static MAC address is your device's private Wi-Fi address for that network only.

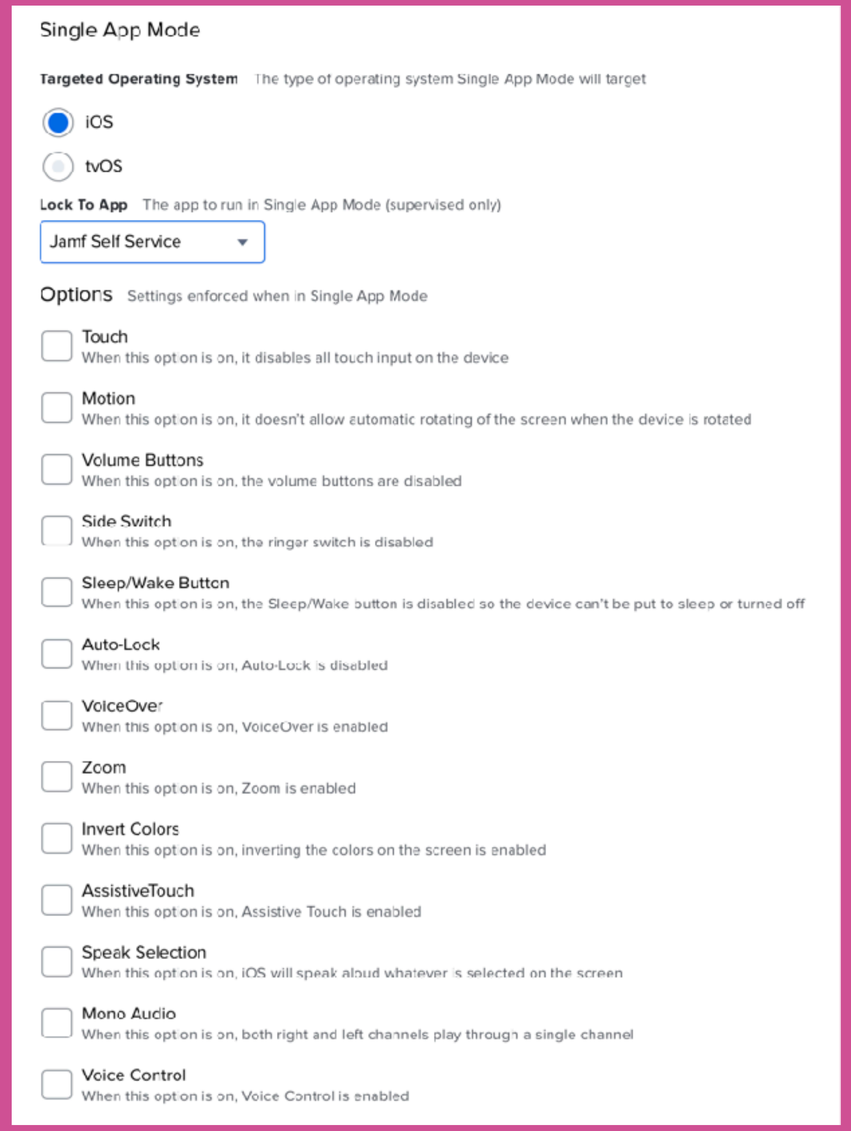
https://support.apple.com/en-gb/HT211227

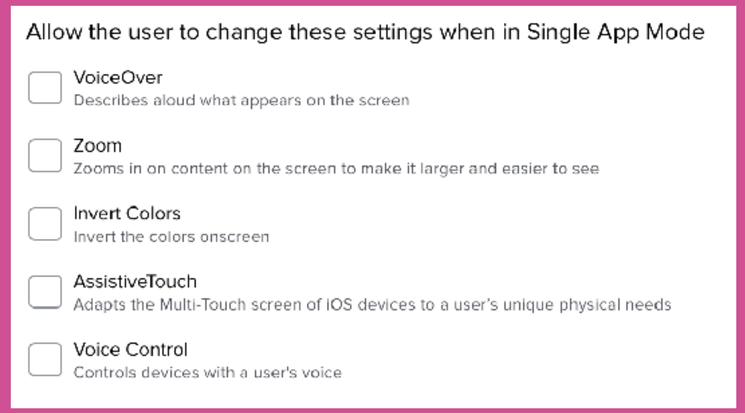


https://support.apple.com/en-gb/HT211227



https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html





https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

dataJAR
Beyond Device Management

Updating iOS on Devices with Single App Mode Enabled

Devices cannot update iOS while single app mode is enabled. You can use the following workflow to disable single app mode on target devices, update iOS, and enable single app mode again.

Updating Devices in Single App Mode

1. Log in to Jamf Pro.
2. Create a smart device group of devices not using the current iOS version following the "Creating a Smart Device Group" section in Updating iOS.
3. Click **Devices** at the top of the page.
4. Click **Configuration Profiles**.
5. Locate the configuration profile scoped to the target devices containing a Single App Mode payload and click it.
6. Click **Edit** at the bottom of the pane.
7. Click the **Scope** tab.
8. Click the **Exclusions** tab.
9. Click **Add** .
10. Click the **Mobile Device Groups** tab.
11. Find the mobile device group you created earlier and click **Add** .
12. Click **Save**.
    Single app mode is disabled on the devices in the target group.
13. Update iOS on devices in the group following the "Updating iOS by Sending a Mass Action Command" section in Updating iOS.
14. After the devices complete the update, click **Configuration Profiles**.
15. Locate the configuration profile scoped to the target devices containing a Single App Mode payload and click it.
16. Click **Edit**.
17. Click the **Scope** tab.
18. Click the **Exclusions** tab.
19. Locate the smart device group you created and click **Remove**.
20. Click **Save**.
    Single app mode is enabled on the devices in the target smart mobile device group.

https://docs.jamf.com/best-practice-workflows/jamf-pro/managing-ios-updates/Updating_iOS_on_Devices_with_Single_App_Mode_Enabled.html

virtual JNUC 2021

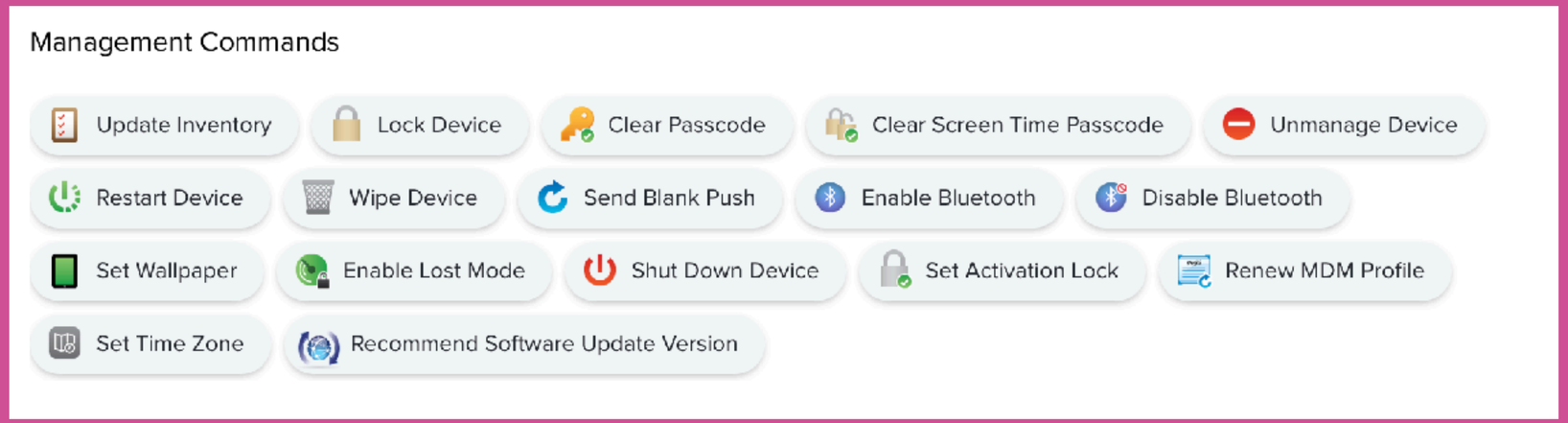
dataJAR
Beyond Device Management

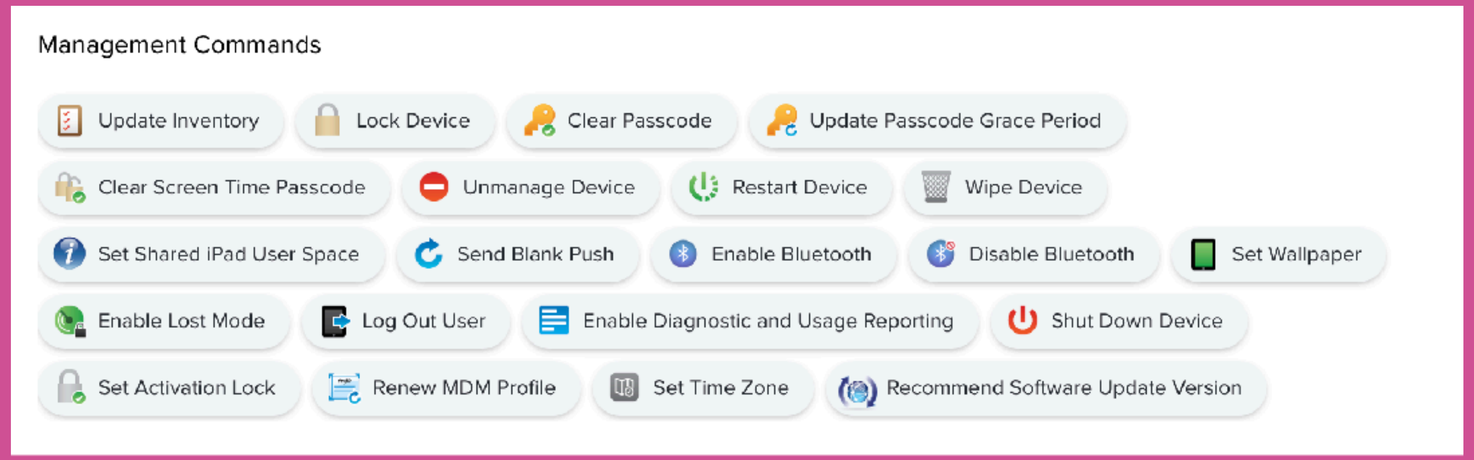
Remote Commands

virtual JNUC 2021

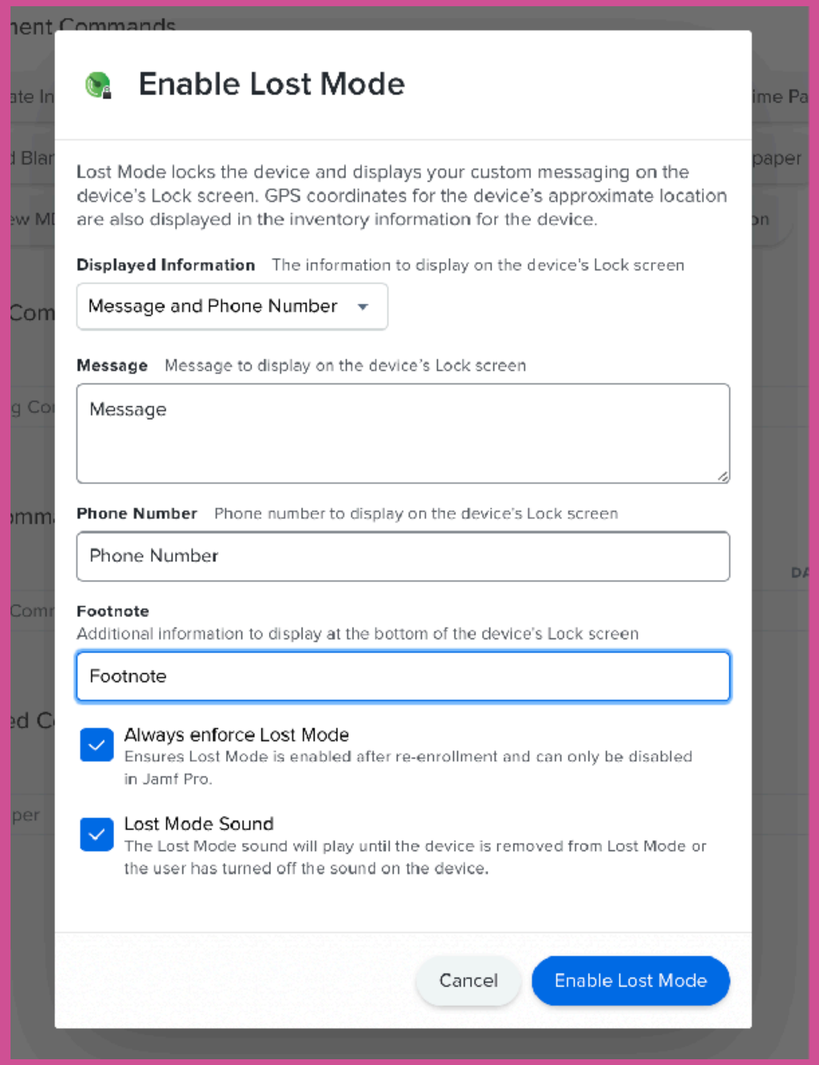
Note: If an iOS device has a passcode enabled, the Update iOS Version mass action command will download the update on the device, but fail to install it. To ensure the update is installed, users must enter their passcode when prompted. You can clear the passcode before sending the mass action to ensure the update installs.

https://docs.jamf.com/best-practice-workflows/jamf-pro/managing-ios-updates/Updating_iOS.html





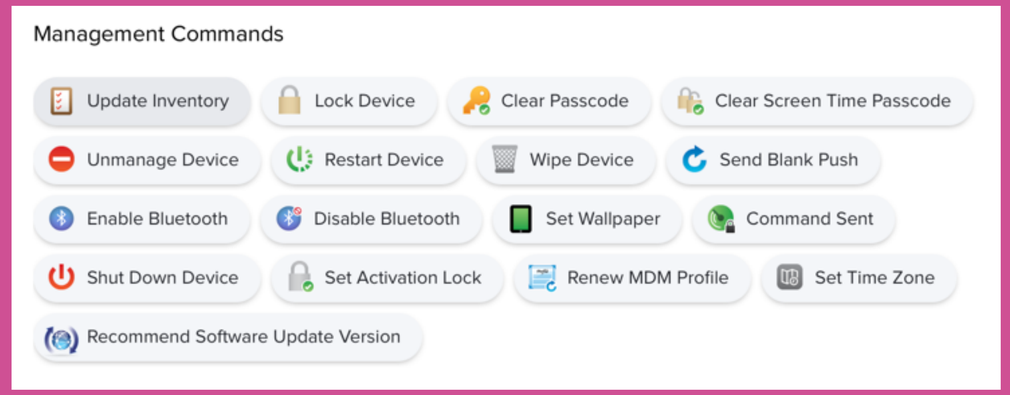
https://docs.jamf.com/jamf-pro/administrator-guide/Remote_Commands_for_Mobile_Devices.html

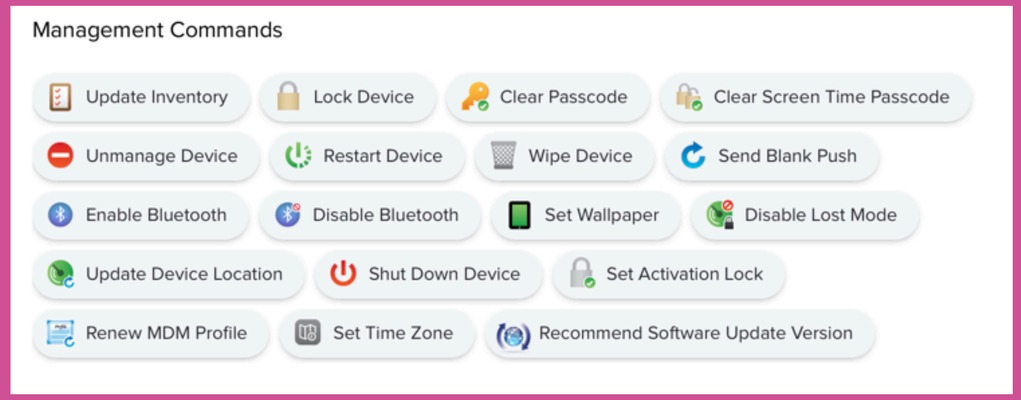


https://docs.jamf.com/jamf-pro/administrator-guide/Remote_Commands_for_Mobile_Devices.html

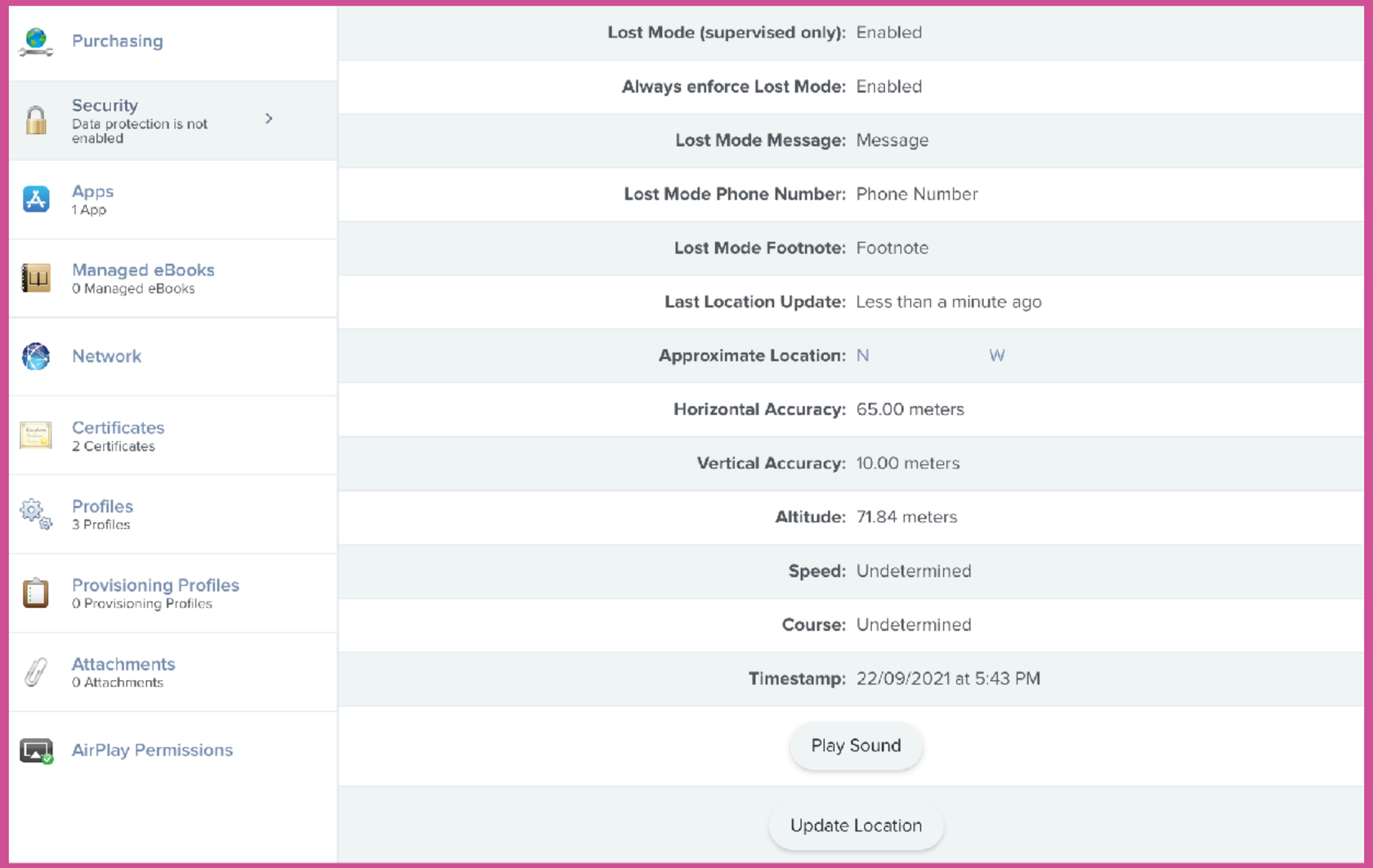
dataJAR
Beyond Device Management

virtual JNUC 2021

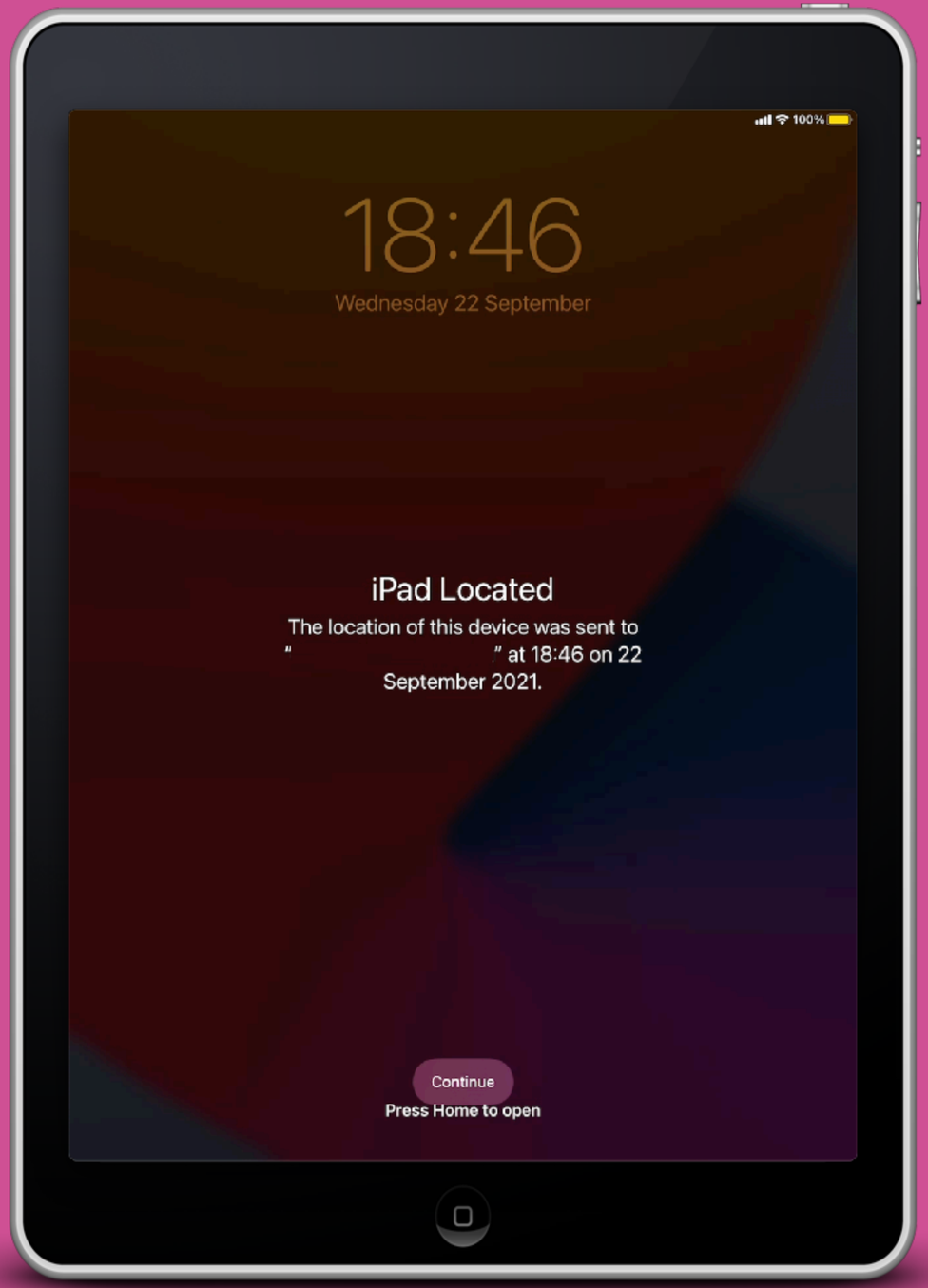




https://docs.jamf.com/jamf-pro/administrator-guide/Remote_Commands_for_Mobile_Devices.html



https://docs.jamf.com/jamf-pro/administrator-guide/Remote_Commands_for_Mobile_Devices.html



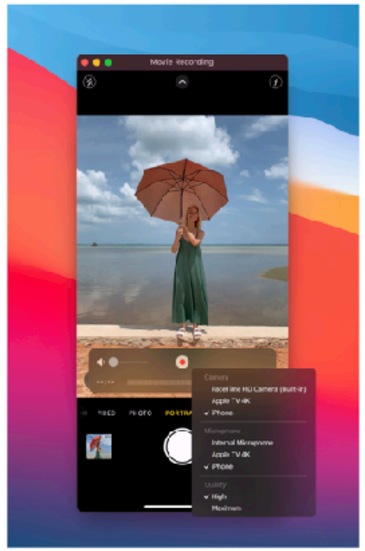
dataJAR
Beyond Device Management

Additional Tips

virtual JNUC 2021

Use an iPhone, iPad or iPod touch connected to your Mac

You can capture what you're seeing on a connected device and save it as a movie file on your Mac.



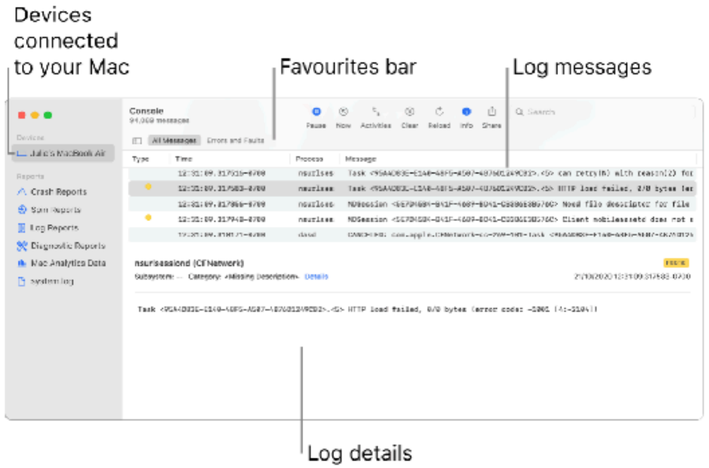
1. Connect your device to your Mac.
2. Open the QuickTime Player app on your Mac.
3. Choose File > New Movie Recording.
4. Click the Options pop-up menu, then choose any of the following recording options:
   - *Camera:* Choose your connected iPhone, iPad or iPod touch.
   - *Microphone:* Choose a microphone (if you have more than one available).
   - *Quality:* Choose the recording quality. Maximum-quality recordings produce uncompressed files, which can use large amounts of storage space.

https://support.apple.com/en-gb/guide/quicktime-player/qtp356b55534/10.5/mac/11.0#apd86177808b0da4

View log messages in Console on Mac

Use Console to view log messages collected by your computer and other connected devices. These log messages may deal with system events, dialogue text, errors, status and other communications. If a problem occurs, you may be able to find information about the cause of the problem by viewing either log messages or activities.

Note: If you're not logged in as an administrator, you need to enter an administrator name and password to view log messages.



1. In the Console app on your Mac, in the Devices list on the left, select the device you want to view log messages for (such as your Mac, iPhone, iPad, Apple Watch or Apple TV). If you don't see the Devices list, click the Sidebar button in the Favourites bar.

https://support.apple.com/en-gb/guide/console/cnsl1012/mac

https://github.com/dataJAR/JNUC2021-Managing-iPads-for-the-Mac-Admin/

virtual JNUC 2021

dataJAR
Beyond Device Management

Thank you for listening!

virtual JNUC 2021