

# Managing iPads, for the Mac Admin





# Ben Toms

Head of Innovation and Platform

dataJAR Ltd | [ben@datajar.co.uk](mailto:ben@datajar.co.uk)



# macmule

macmule.com |  macmule |  @macmuleblog

# Managing iPads, for the Mac Admin

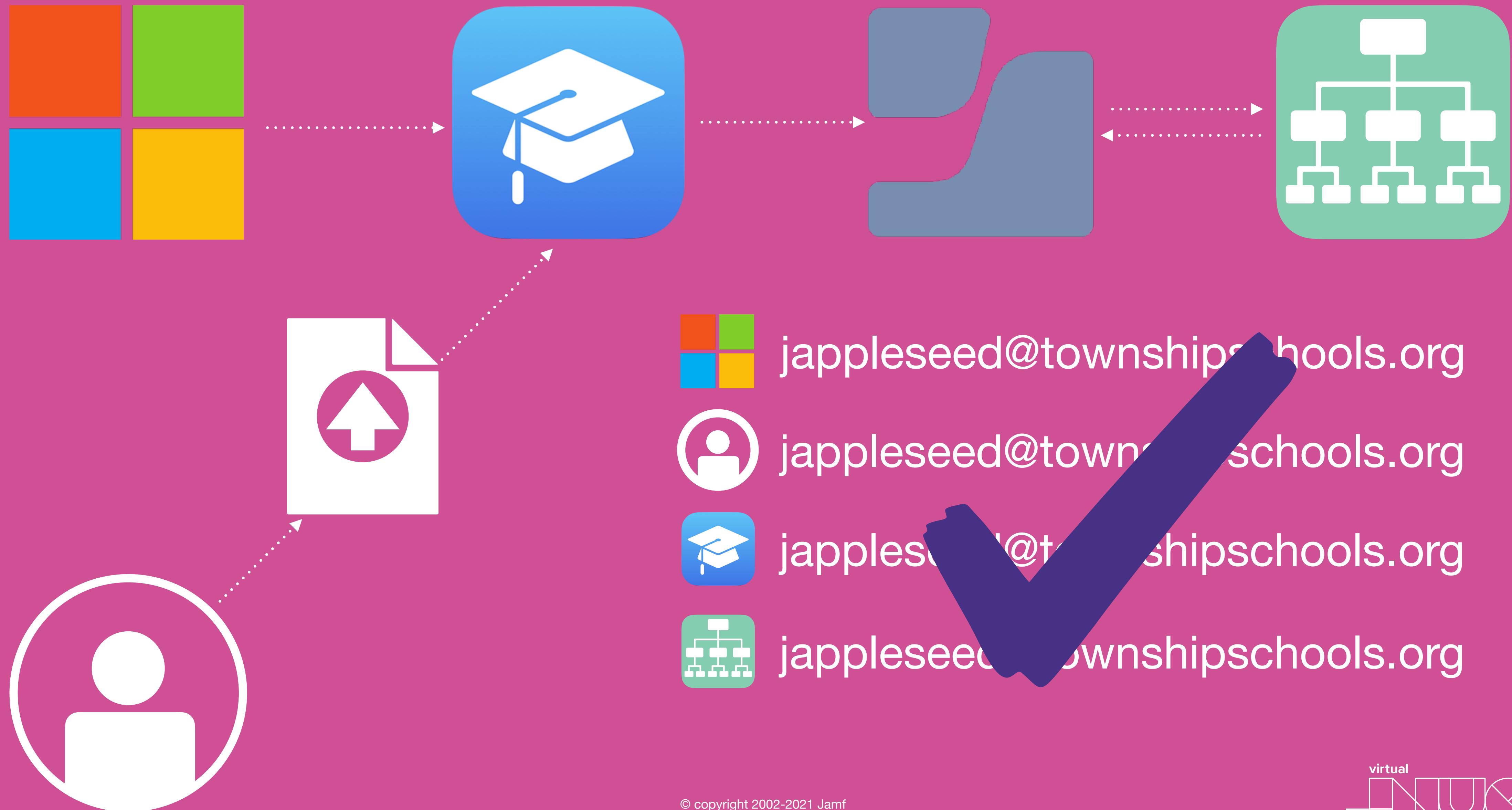
- Apple Deployment Programmes
- Jamf Pro Settings
- Application Deployment and Configuration
- Automated Device Enrollment
- Device Management Settings
- Remote Commands
- Additional Tips

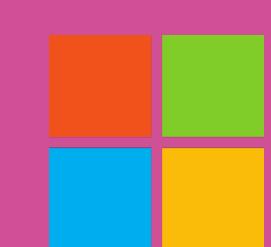
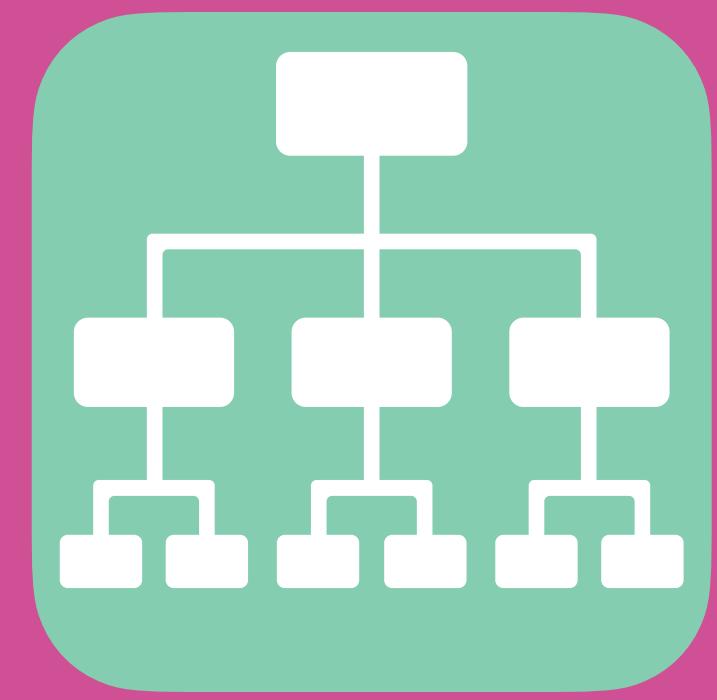
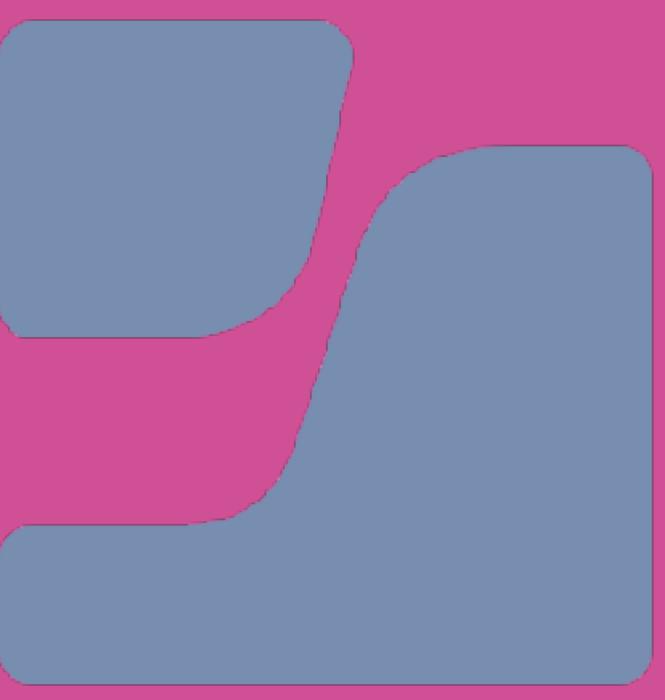
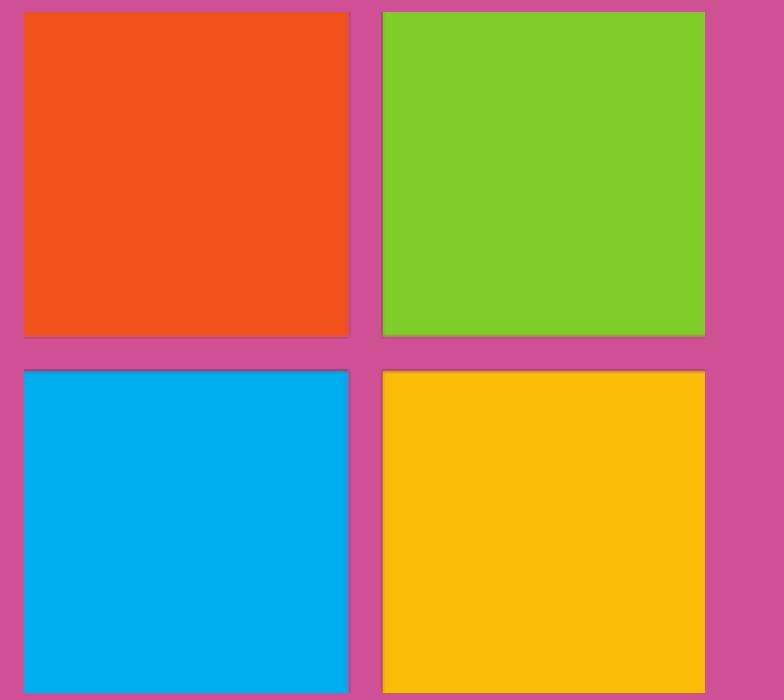


<https://github.com/dataJAR/JNUC2021-Managing-iPads-for-the-Mac-Admin/>

# Apple Deployment Programmes



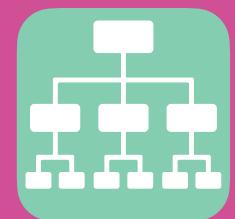




jappleseed@mycompany.com



jappleseed@mycompany.com



jappleseed@mycompany.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-school-manager/apdb19317543/web)**

**[https://support.apple.com/en-gb/guide/apple-business-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/>**



The screenshot shows the Jamf Pro administrative interface. On the left, a sidebar lists navigation options: All Settings, System Settings, Global Management (which is selected and highlighted in dark blue), Jamf Applications, Self Service, Server Infrastructure, and Network Organization. The main content area is titled "Global Management" and contains a grid of 15 icons, each representing a different management setting. The icons are arranged in three rows: Row 1 includes Categories, Push Certificates, GSX Connection, Jamf Pro URL, MDM Profile Settings, PKI Certificates, Volume Purchasing, User-Initiated Enrollment, and Automated Device Enrollment; Row 2 includes Apple Education Support, Re-enrollment, Event Logs, Webhooks, AirPlay Permissions, Conditional Access, Inventory Preload, Enrollment Customization, and Cloud Services Connection; Row 3 includes Remote Administration.

| Categories              | Push Certificates | GSX Connection | Jamf Pro URL | MDM Profile Settings | PKI Certificates   | Volume Purchasing | User-Initiated Enrollment | Automated Device Enrollment |
|-------------------------|-------------------|----------------|--------------|----------------------|--------------------|-------------------|---------------------------|-----------------------------|
| Apple Education Support | Re-enrollment     | Event Logs     | Webhooks     | AirPlay Permissions  | Conditional Access | Inventory Preload | Enrollment Customization  | Cloud Services Connection   |
| Remote Administration   |                   |                |              |                      |                    |                   |                           |                             |

[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)

The screenshot shows the Jamf Pro Global Management interface. On the left, a sidebar lists 'All Settings' with categories: System Settings, Global Management (selected), Jamf Applications, Self Service, Server Infrastructure, and Network Organization. The main area is titled 'Global Management' and contains a grid of icons and labels. A purple arrow points from the 'Apple Education Support' icon to the text 'Apple Education Support' below it. Other visible icons include Categories, Push Certificates, GSX Connection, Jamf Pro URL, MDM Profile Settings, PKI Certificates, Volume Purchasing, User-Initiated Enrollment, Automated Device Enrollment, Enrollment Customization, Cloud Services Connection, and Remote Administration.

| Icon                   | Label                       |
|------------------------|-----------------------------|
| Folder                 | Categories                  |
| Cloud with arrow       | Push Certificates           |
| Globe with wrench      | GSX Connection              |
| Globe                  | Jamf Pro URL                |
| Profile                | MDM Profile Settings        |
| Certificate            | PKI Certificates            |
| Volume icon            | Volume Purchasing           |
| Device with plus       | User-Initiated Enrollment   |
| Device                 | Automated Device Enrollment |
| Cloud with gear        | Cloud Services Connection   |
| Apple icon             | Apple Education Support     |
| Device with checkmark  | Re-enrollment               |
| Calendar               | Event Logs                  |
| Webhook icon           | Webhooks                    |
| Monitor with checkmark | AirPlay Permissions         |
| Lock with key          | Conditional Access          |
| Inventory icon         | Inventory Preload           |
| Checklist              | Enrollment Customization    |
| Cloud                  | Remote Administration       |

[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)

Settings : Global Management

← Apple Education Support

General Apple School Manager Instances

**Enable Apple Education Support**  
Enable support for Shared iPad and Apple's Classroom app for mobile devices (iOS 9.3 or later) and computers (macOS 10.14 or later)

**Enable User Images**  
Enable use of user images

**Distribution Point URL For User Images** URL of the distribution point for user images. The URL should begin with "https://". It is recommended that the images are in PNG format and are 256x256 pixels  
 https:// \$Username.png

**Certificate Download** CA certificate to use for authentication. This certificate is required for user images

 [Download](#)

**Upload Additional Certificate**  
Upload an additional CA certificate to establish trust between Jamf Pro and the distribution point

**[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)**

Settings : Global Management

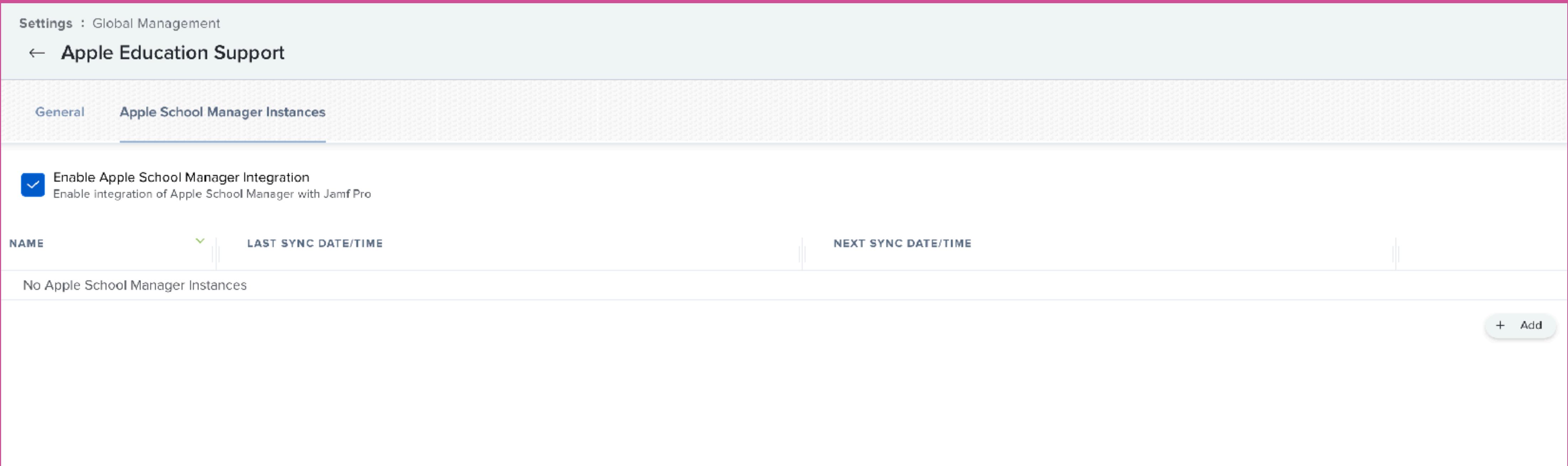
← Apple Education Support

General Apple School Manager Instances

Enable Apple School Manager Integration  
Enable integration of Apple School Manager with Jamf Pro

| NAME                              | LAST SYNC DATE/TIME | NEXT SYNC DATE/TIME |
|-----------------------------------|---------------------|---------------------|
| No Apple School Manager Instances |                     |                     |

+ Add



[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)

Settings : Global Management > Apple Education Support

← Apple School Manager

**Display Name** Display name for the Apple School Manager instance  
Apple School Manager

**Automated Device Enrollment Instance** Automated Device Enrollment instance to associate with the Apple School Manager instance  
Apple School Manager

**Apple School Manager Sync Time** Time to sync with Apple School Manager to update class and student inventory information  
Once a day ▾  
Time Of The Day  
8 : 00 a.m.  
Time Zone  
Europe/London

**Class Naming Format** Sequence of variables to apply to a class name when importing classes from Apple School Manager  
Course Name ▾  

Preview: Course Name

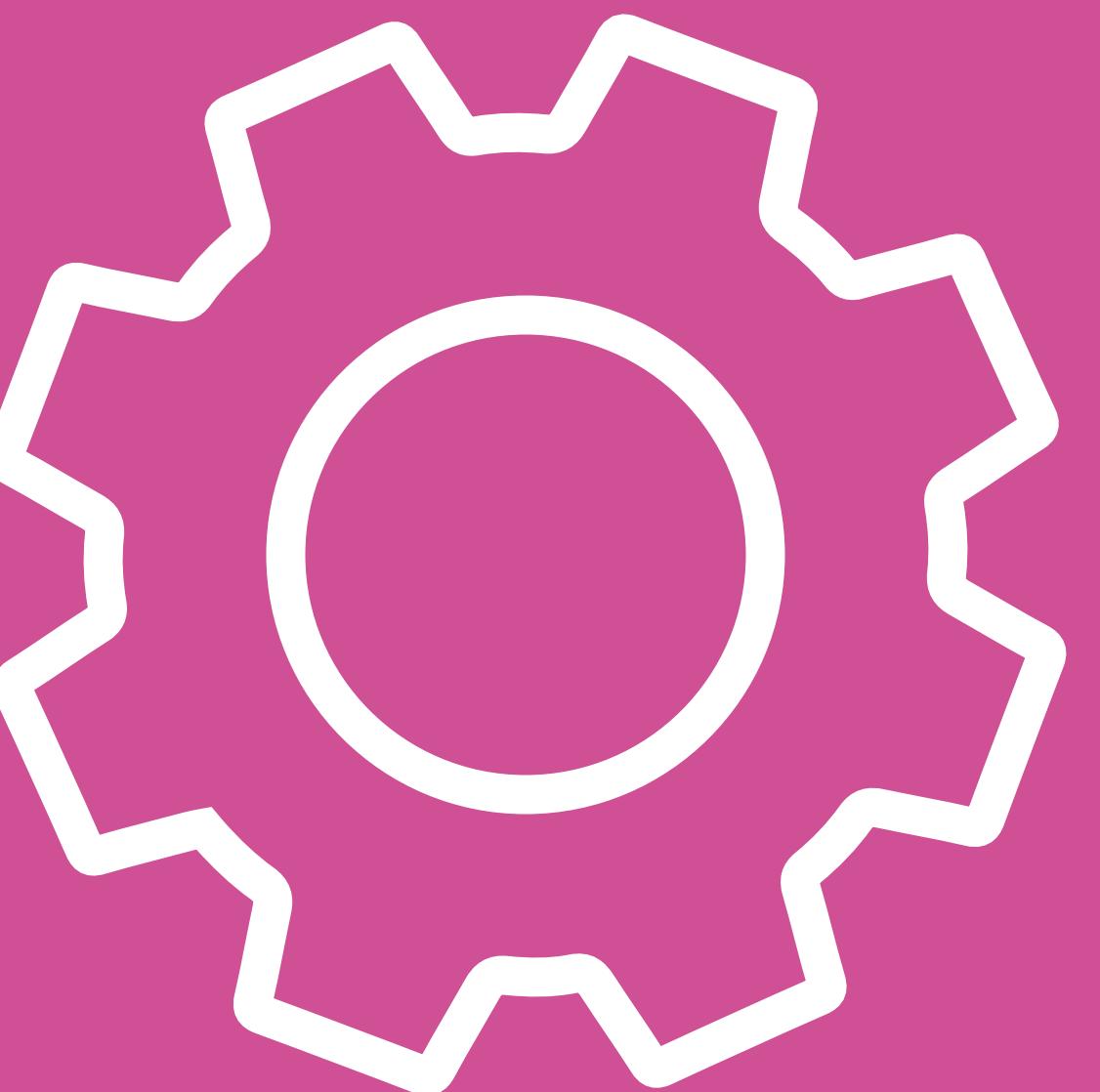
**Class Description Format** Sequence of variables to apply to a class description when importing classes from Apple School Manager

**Matching Criteria for Importing Users** Criteria to use to match Apple School Manager user information with existing user information in Jamf Pro when importing users

| User Criteria           | Operator | User Criteria   |
|-------------------------|----------|-----------------|
| Email (Jamf Pro server) | equals ▾ | Email Address ▾ |

[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)

# Jamf Pro Settings



The screenshot shows the Jamf Pro Global Management settings page. On the left, a sidebar lists 'All Settings' with sub-options: System Settings, Global Management (which is selected and highlighted in dark blue), Jamf Applications, Self Service, Server Infrastructure, and Network Organization. The main content area is titled 'Global Management' and contains a grid of icons and labels. The 'Re-enrollment' icon, which is orange and shows a smartphone and a computer monitor, is highlighted by a large purple arrow pointing from the text below. Other icons include Categories (yellow folder), Push Certificates (cloud with arrow), GSX Connection (globe with wrench), Jamf Pro URL (globe), MDM Profile Settings (blue document), PKI Certificates (golden certificate), Volume Purchasing (blue square with checkmark), User-Initiated Enrollment (smartphone with plus), Automated Device Enrollment (two smartphones), Enrollment Customization (red square with gear), and Cloud Services Connection (cloud with gear). The 'Re-enrollment' icon is located in the second row, third column of the grid.

[https://docs.jamf.com/jamf-pro/administrator-guide/Re-enrollment\\_Settings.html](https://docs.jamf.com/jamf-pro/administrator-guide/Re-enrollment_Settings.html)

Settings : Global Management

← Re-enrollment

**Info** These settings are applied to inventory information for computers and mobile devices when they are re-enrolled with Jamf Pro via user-initiated enrollment, PreStage enrollment, or Apple Configurator 2 (mobile devices only). Use Recon to override these settings for computers.

Clear user and location information on mobile devices and computers  
Clears computer and mobile device information from the User and Location category on the Inventory tab in inventory information during re-enrollment

Clear user and location history information on mobile devices and computers  
Clears computer and mobile device information from the User and Location History category on the History tab in inventory information during re-enrollment

Clear policy logs on computers  
Clears the logs for policies that ran on the computer and clears computer information from the Policy Logs category on the History tab in inventory information during re-enrollment

Clear extension attribute values on computers and mobile devices  
Clears all values for extension attributes from computer and mobile device inventory information during re-enrollment. This does not apply to extension attributes populated by scripts or LDAP Attribute Mapping

**Clear Management History On Mobile Devices And Computers** Clears computer and mobile device information from the Management History category on the History tab in inventory information during re-enrollment

Clear completed, failed and pending commands ▾

[https://docs.jamf.com/jamf-pro/administrator-guide/Re-enrollment\\_Settings.html](https://docs.jamf.com/jamf-pro/administrator-guide/Re-enrollment_Settings.html)

| Failed Commands  |   |                        |                        |          | <a href="#">Cancel All</a> |
|------------------|---|------------------------|------------------------|----------|----------------------------|
| COMMAND          | ERROR   | DATE ISSUED            | DATE OF LAST PUSH      | USERNAME |                            |
| Update Inventory | The connection timed out. Check your network connection and proxy settings. | Less than a minute ago | Less than a minute ago |          | <a href="#">Cancel</a>     |
|                  |   |                        |                        |          |                            |

PI-005519

All Settings

---

System Settings

Global Management

Jamf Applications

Self Service

Server Infrastructure

Network Organization

---

Computer Management

Device Management

### Device Management

Inventory Collection

Inventory Display

Extension Attributes

Apple Configurator Enrollment

App Maintenance

## ← Inventory Collection

**Inventory Collection Frequency** Frequency at which mobile devices submit inventory information to Jamf Pro

Every Day ▾

Collect unmanaged apps

Collect names, versions, bundle sizes, and dynamic sizes of unmanaged apps. Does not apply to personally owned devices

Collect user and location information from LDAP

Collect user and location information from the LDAP server when inventory is updated

Monitor iBeacon regions

Use Self Service for iOS to monitor iBeacon regions and submit information to Jamf Pro when mobile devices enter or exit a region

[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)

## ← Inventory Collection

**Inventory Collection Frequency** Frequency at which mobile devices submit inventory information to Jamf Pro

Every Day

Every Week

Every Month

Managed apps

Collect names, versions, bundle sizes, and dynamic sizes of unmanaged apps. Does not apply to personally owned devices

Collect user and location information from LDAP

Collect user and location information from the LDAP server when inventory is updated



Monitor iBeacon regions

Use Self Service for iOS to monitor iBeacon regions and submit information to Jamf Pro when mobile devices enter or exit a region

[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)

## ← Inventory Collection

**Inventory Collection Frequency** Frequency at which mobile devices submit inventory information to Jamf Pro

Every Day ▾

Collect unmanaged apps

Collect names, versions, bundle sizes, and dynamic sizes of unmanaged apps. Does not apply to personally owned devices

Collect user and location information from LDAP

Collect user and location information from the LDAP server when inventory is updated

Monitor iBeacon regions

Use Self Service for iOS to monitor iBeacon regions and submit information to Jamf Pro when mobile devices enter or exit a region

[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)

Settings : Device Management > Extension Attributes

← New Mobile Device Extension Attribute

**Display Name** Display name for the extension attribute  
Untitled

**Description** Description for the extension attribute

**Data Type** Type of data being collected  
String

**Inventory Display** Category in which to display the extension attribute in Jamf Pro  
General

**Input Type** Input type to use to populate the extension attribute

- Text Field
- Pop-up Menu
- LDAP Attribute Mapping

[https://docs.jamf.com/jamf-pro/administrator-guide/  
Mobile\\_Device.Extension\\_Attributes.html](https://docs.jamf.com/jamf-pro/administrator-guide/Mobile_Device_Extension_Attributes.html)

Settings : Device Management

← App Maintenance

App Updates In-House Apps

Automatically Force App Updates  
Automatically force updates for all automatically installed App Store apps on mobile devices (Managed Distribution or free apps)

Automatically update apps installed via Self Service

Schedule Jamf Pro to automatically check the App Store for app updates  
Automatically update all App Store app descriptions, icons, and versions in Jamf Pro

**App Store Country Or Region** Country or region to use when syncing App Store apps with the App Store  
United Kingdom

**App Store Sync Time** Time to sync with the App Store each day to automatically update App Store app descriptions, icons, and versions in Jamf Pro  
1 : 00 a.m.

**Force App Updates** Force update for all App Store apps on mobile devices (Managed Distribution or free apps)

Force Updates

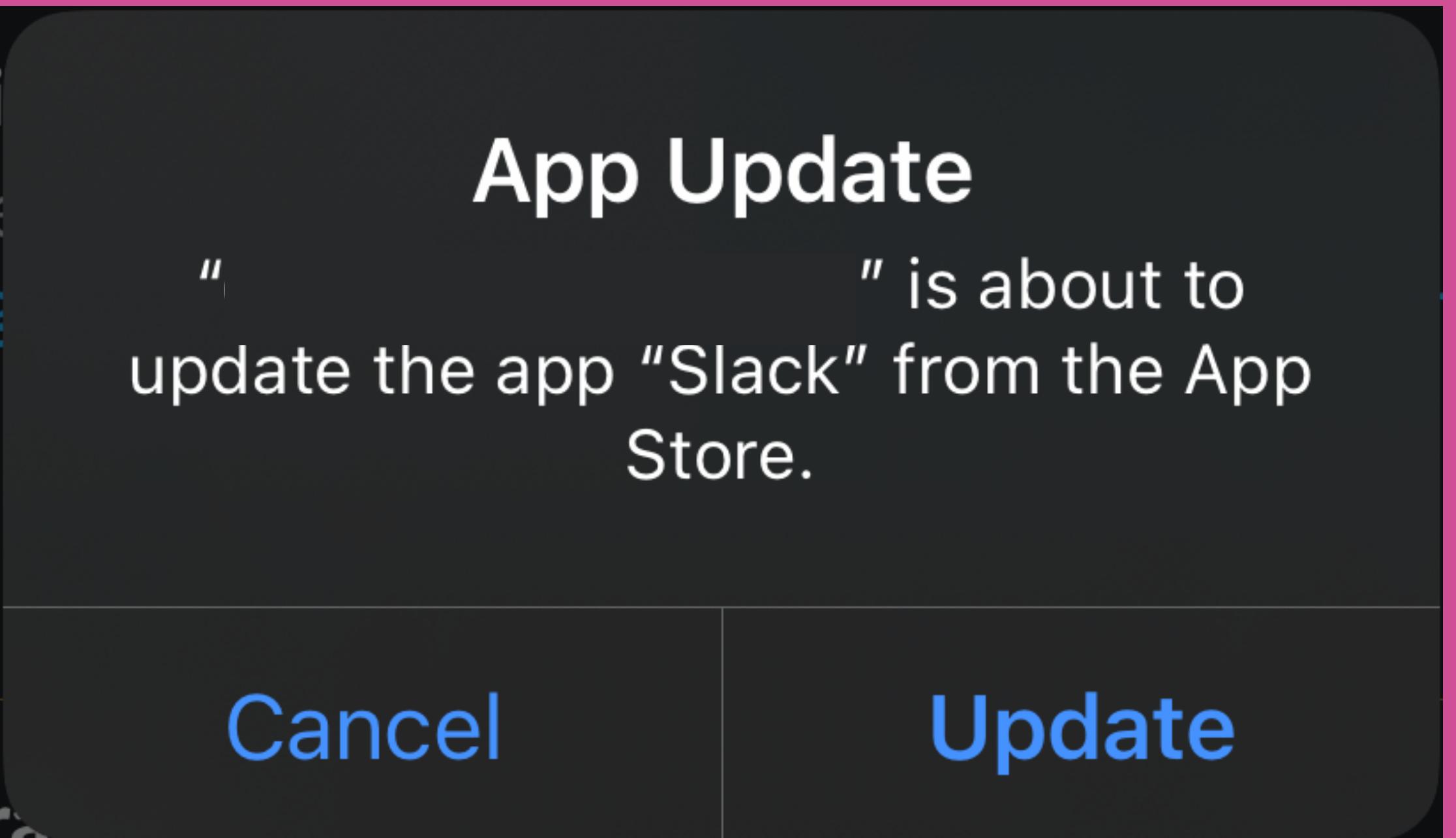
[https://docs.jamf.com/jamf-pro/administrator-guide/  
App\\_Store\\_App\\_Update\\_Settings.html](https://docs.jamf.com/jamf-pro/administrator-guide/App_Store_App_Update_Settings.html)

## 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 |                   | <a href="#">Cancel</a> |





The screenshot shows the Jamf Pro application window. On the left is a sidebar with the following items:

- All Settings (gear icon)
- System Settings (bar chart icon)
- Global Management (globe icon)
- Jamf Applications (document icon)
- Self Service (gear icon)

The "Self Service" item is highlighted with a dark blue bar at the bottom of the sidebar.

## Self Service



macOS



iOS



Branding



Bookmarks



App Request

**Settings : Self Service**

← iOS

General Web Clip Options App Options

**Installation Method** Method for installing Self Service on mobile devices

Manually install Self Service app ▾

Allow Self Service web clip access  
Allow access to the web clip using a mobile device configuration profile

**Updates** Updates to display in Self Service

In-house app updates

[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.html)



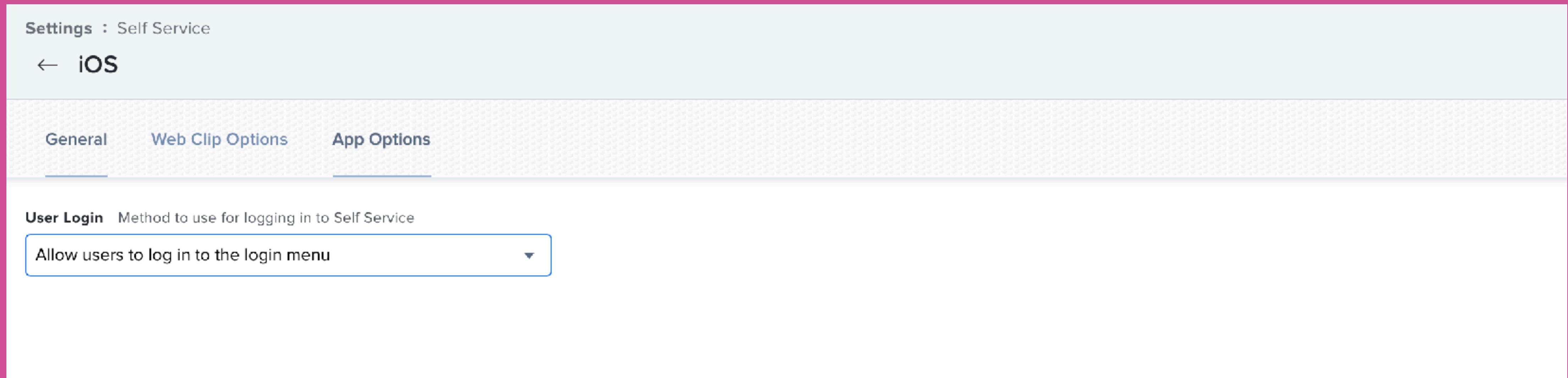
Settings : Self Service

← iOS

General Web Clip Options App Options

User Login Method to use for logging in to Self Service

Allow users to log in to the login menu ▾



[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.html)



Settings : Self Service

← Branding

---

**macOS Branding**  
Self Service macOS branding configuration

**NAME**

|                        |                        |
|------------------------|------------------------|
| Default macOS Branding | <a href="#">Remove</a> |
|------------------------|------------------------|

---

**iOS Branding**  
Self Service iOS branding configuration

**NAME**

|  |                       |
|--|-----------------------|
|  | <a href="#">+ Add</a> |
|--|-----------------------|

[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)



The image shows two side-by-side screenshots. On the left is a web-based configuration interface titled 'Default iOS Branding'. It includes fields for 'Icon' (with a placeholder for a 180x180 pixel PNG or GIF file), 'Branding Name' ('datajar.mobi Self Service'), 'Header Background Color' (#4F5064), 'Menu Icon Color' (FFFFFF), 'Branding Name Color' (FFFFFF), and 'Status Bar Color' (Light). On the right is a screenshot of an iPhone displaying the 'datajar.mobi Self Service' app. The app's header shows the branding name. Below the header is a list of items: Books, Flash, Secure, Look, People, Star, and Spot, each with an 'Install' button. At the bottom of the app screen are 'Home', 'Notifications', and 'Search' icons.

[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



Settings : Self Service > Bookmarks

← **datajar.mobi**

General Scope

**i** Requires Self Service v10.0.0 or later

| Targets | Limitations | Exclusions |
|---------|-------------|------------|
|---------|-------------|------------|

**Target Computers**  
Computers to deploy the bookmark to

All Computers  
Specific Computers

**Target Users**  
Users to deploy the bookmark to

Specific Users

Selected Deployment Targets

+ Add

| TARGET     | TYPE |
|------------|------|
| No Targets |      |

Settings : Self Service

← App Request

App Request Form Requesters and Approvers

**REQUIREMENTS NOT MET**

To enable App Request, you must do the following:  
Create a static user group that includes users you want to enable as app requesters

Enable App Request in Self Service for iOS  
Allow specified users to request App Store apps directly from Self Service (iPad apps only)

App Store Country Or Region App Store to use for app requests

User's Location ▾

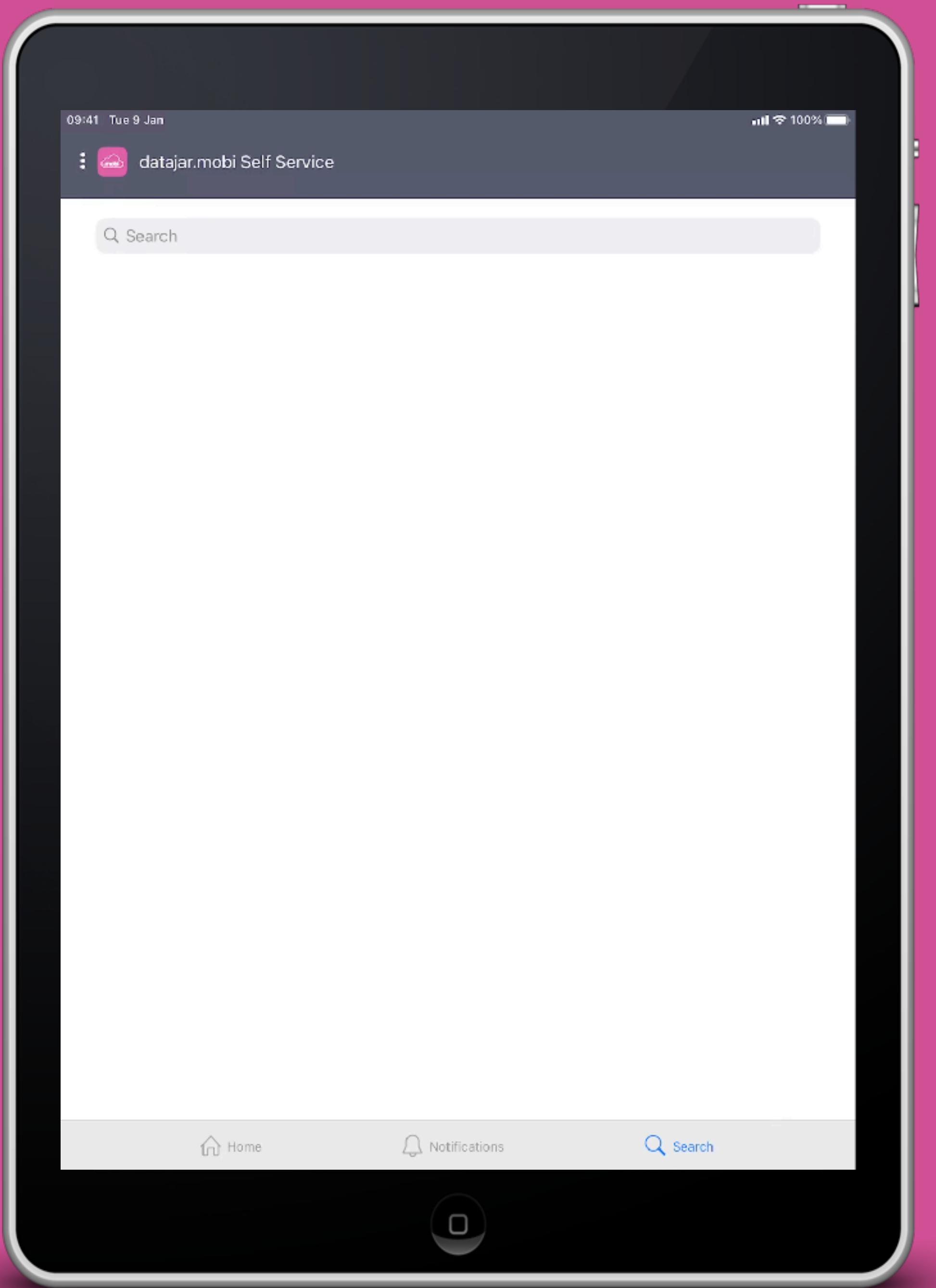
App Request Form Fields

Add up to five fields to display in the App Request form in Self Service. Fields will display in the order they are listed below. Each field you add will require requester input.

+ Add Field

**⚠ Must configure at least one form field**

**[https://docs.jamf.com/jamf-pro/administrator-guide/  
App\\_Request.html](https://docs.jamf.com/jamf-pro/administrator-guide/App_Request.html)**



© copyright 2002-2021 Jamf



# Application Configuration and Deployment





© copyright 2002-2021 Jamf



Mobile Devices : Mobile Device Apps

← Jamf Self Service

General Scope Managed Distribution App Configuration

**Display Name** Display name for the app

Enabled

**Category** Category to add the app to

**Short Version** Short Version of the app

**Bundle Identifier** Bundle identifier for the app

Free  
App is free

**Distribution Method** Method to use for distributing the app

Display app in Self Service after it is installed

Require tethered network connection for app installation (iOS 10.3 or later)  
Require the device to have a tethered network connection to download the app

[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)

Schedule Jamf Pro to automatically check the App Store for app updates  
Automatically update app description, icon, and version in Jamf Pro

**App Store Country Or Region** Country or region to use when syncing app with the App Store

**App Store Sync Time** Time to sync with the App Store each day to automatically update app description, icon, and version in Jamf Pro

Automatically Force App Updates  
Automatically force updates for this app on mobile devices (Managed Distribution or free apps)

[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)

**Make app managed when possible**  
Make the app managed when managed app requirements are met

**Make app managed if currently installed as unmanaged**  
Manage the app if it is currently installed as an unmanaged app (the user is prompted to allow management on unsupervised devices)

Remove app when MDM profile is removed

Prevent backup of app data

**Allow users to remove app (iOS 14 or later)**  
Allows the user to remove this app from a device. The app is not removed from the App Catalog in Jamf Pro.

**Force App Update** Force updates for this app on mobile devices (Managed Distribution or free apps)

**App URL** URL of the app's App Store Preview page (e.g. "https://apps.apple.com/us/app/name-of-app/id123456789?mt=8")

**Associated Domains**

**ASSOCIATED DOMAIN**

**[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/iorf4d72edeb/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](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/  
iorf4d72edeb/web](https://support.apple.com/en-gb/guide/deployment-reference-ios/iorf4d72edeb/web)

Mobile Devices : Mobile Device Apps  
← Jamf Self Service

General Scope Managed Distribution App Configuration

Device Assignments VPP Codes

Volume Content

Assign Content Purchased in Volume  
Assign content purchased in volume to mobile devices with iOS 9 or later

[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)



Mobile Devices : Mobile Device Apps

← Jamf Self Service

General Scope Managed Distribution App Configuration

Device Assignments VPP Codes

**Volume Content**

Assign Content Purchased in Volume  
Assign content purchased in volume to mobile devices with iOS 9 or later

**Location** Volume purchasing location to use to assign content  
Apple Business Manager

| TOTAL CONTENT | IN USE |
|---------------|--------|
| 20            | 1      |

[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            |   |                  |                   |          | <a href="#">Cancel All</a> |
|----------------------------|---|------------------|-------------------|----------|----------------------------|
| 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  |          | <a href="#">Cancel</a>     |





Mobile Devices : Mobile Device Apps

← Jamf Self Service

General Scope Managed Distribution **App Configuration**

**Preferences** Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later

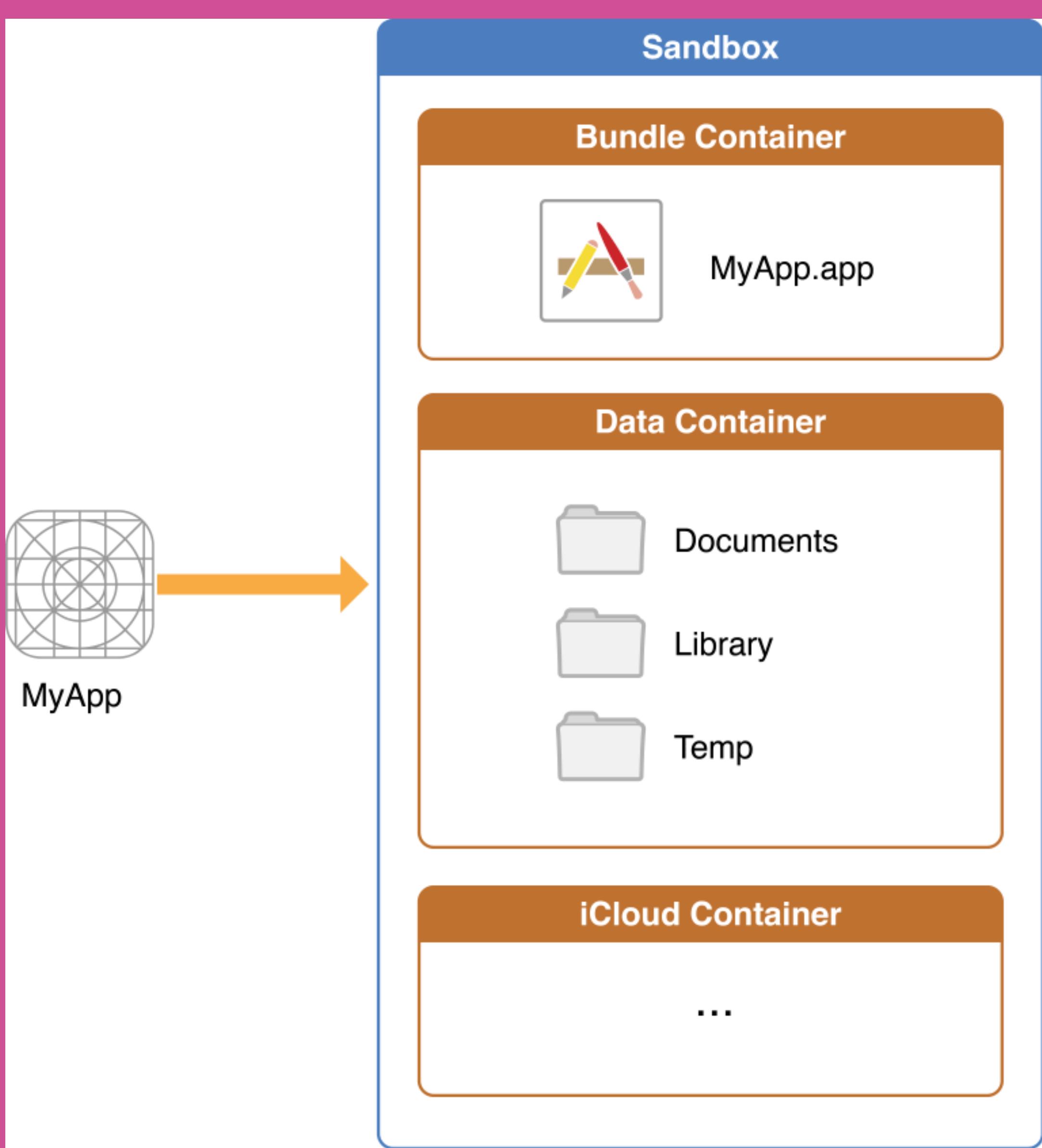
|

| **i** For help generating the PLIST file for preferences, use the [AppConfig Generator](#)

- *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/  
iorf4d72edeb/web](https://support.apple.com/en-gb/guide/deployment-reference-ios/iorf4d72edeb/web)**



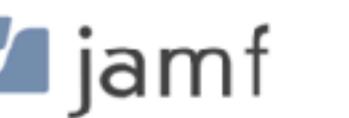


<https://macmule.com/2016/12/11/profiles-an-it-admins-best-friend/>

# Introducing The AppConfig Community

A community focused on providing tools and best practices around native capabilities in mobile operating systems to enable a more consistent, open and simple way to configure and secure mobile apps in order to increase mobile adoption in business. Users benefit with instant mobile productivity and a seamless out-of-the box experience, and businesses benefit with secure work-ready apps with minimal setup required while leveraging existing investments in Device Management (UEM/MDM), VPN, and identity solutions. Ultimately, your apps are simpler to configure, secure and deploy. The AppConfig Community is sponsored by industry leading device management vendors:

IBM MaaS360



mobileiron

vmware®

SOTI

BlackBerry

cisco Meraki



## Benefits of AppConfig

### ISVs & Developers

- Build enterprise-ready apps faster
- EMM vendor neutral solution
- Reduce need for proprietary SDK
- Reduce need for App Wrapping

### Enterprises

- Leverage existing EMM, VPN, and IAM investments
- Better native onboarding user experience
- Greater selection of business apps

### EMM Providers

- Leverage OS best practices
- Larger ecosystem of business apps
- Simplify app configuration
- Ease management workflows

### Android OEMs

- Build proprietary device configurations
- Support new features same-day
- Equal feature set across EMMs
- Increased value-add of devices

[Join Now >](#)

**<https://www.appconfig.org/>**



| iOS Capabilities Summary                     |  |
|--|--|
| Capability                                   | Summary of the AppConfig Community best practices  |
| <b>App Configuration</b>                     | Develop iOS 7+ <a href="#">Managed Configuration</a> into the application.   |
| <b>App Tunnel</b>                            | Leverage the “Per-app VPN” capability available in most commercial VPN solutions, and available in iOS 9+. No development required.  |
| <b>Single Sign-On</b>                        | Implement a standard single sign-on protocol, such as SAML, and invoke the identity provider login page in a web view.   |
| <b>Security Policies</b>                     |  |
| <b>Appendix – Dev Tools</b>                  |  |
| <b>App Security – Passcode / TouchID</b>     | Use iOS 7+ <a href="#">“Managed Configuration”</a> to set the pincode or TouchID settings on the application.  |
| <b>App Security – Managed Open-In</b>        | Set the “managed open in” control available by the EMM provider to restrict the native open in capability. No development required.<br>Applications that may have additional document sharing or syncing capabilities should use the iOS 7+ <a href="#">“Managed Configuration”</a> to set the document sharing and syncing policy on the application. |
| <b>App Security – Prevent App Backup</b>     | Set the “prevent app backup” security control available by the EMM provider to prevent app data backup in iTunes. No development required.   |
| <b>App Security – Disable Screen Capture</b> | Set the “prevent screen capture” security control available by the EMM provider with iOS 9+ to restrict the native screenshot capability. No development required.   |
| <b>App Security – Enforce App Encryption</b> | Set the device passcode security control available by the EMM provider to enforce the native iOS data protection encryption. No development required.  |
| <b>App Security – Remotely Wipe App</b>      | Distribute the app to the device as a managed application using the EMM tool to have the ability to remotely wipe the app from the device. No development required.  |
| <b>App Security – Disable Copy-Paste</b>     | Use iOS 7+ <a href="#">“Managed Configuration”</a> to set the copy/paste policy on the application.  |

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

Mobile Devices : Mobile Device Apps

← Jamf Self Service

General Scope Managed Distribution App Configuration

**Preferences** Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later

```
<dict>
<key>INVITATION_STRING</key>
<string>$MOBILEDEVICEAPPINVITE</string>
<key>JSS_ID</key>
<string>$JSSID</string>
<key>SERIAL_NUMBER</key>
<string>$SERIALNUMBER</string>
<key>DEVICE_NAME</key>
<string>$DEVICENAME</string>
<key>MAC_ADDRESS</key>
<string>$MACADDRESS</string>
<key>UDID</key>
<string>$UDID</string>
<key>JSS_URL</key>
<string>$JPS_URL</string>
</dict>
```

|  For help generating the PLIST file for preferences, use the [AppConfig Generator](#)

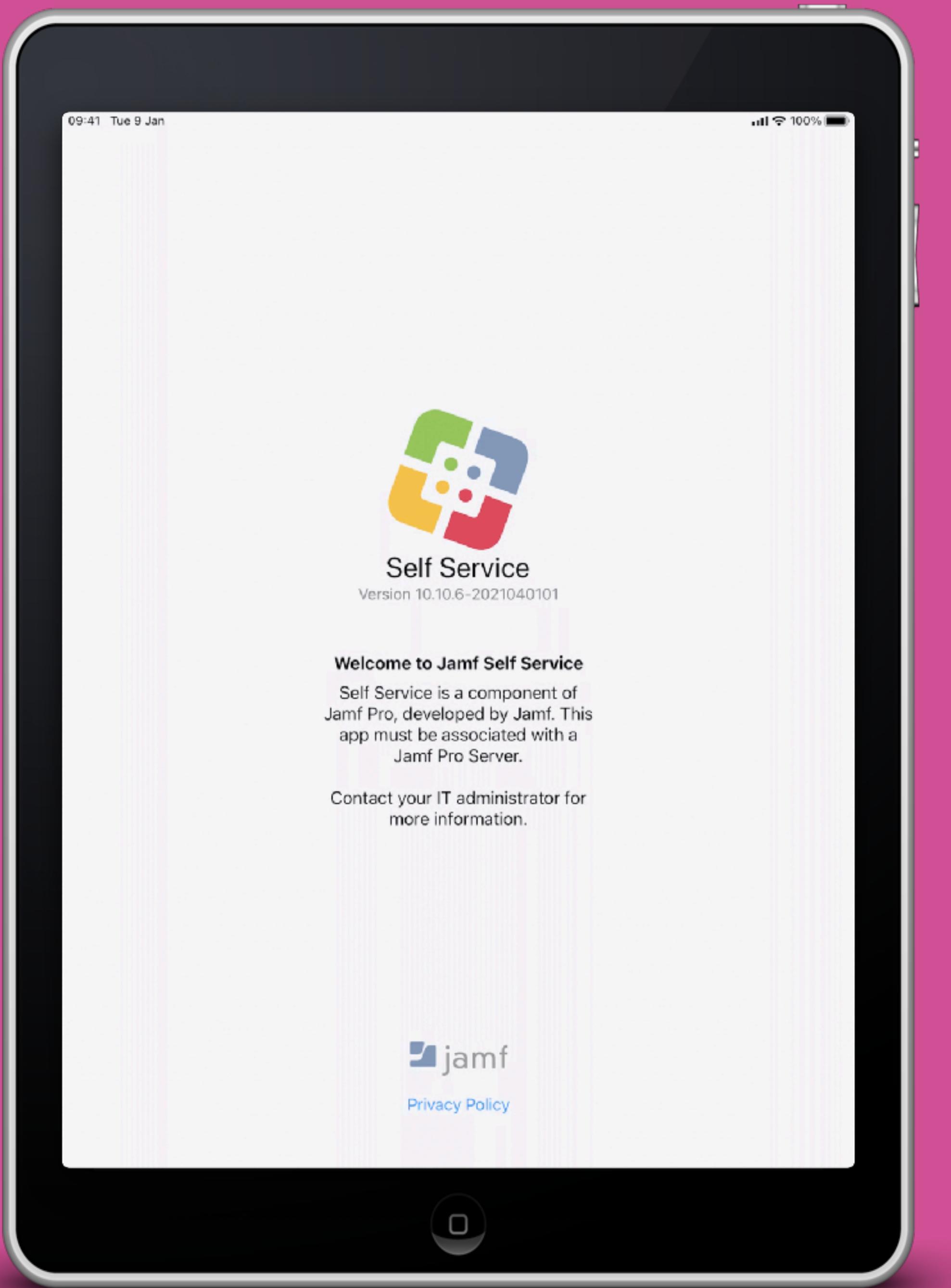
**[https://docs.jamf.com/jamf-pro/administrator-guide/  
Jamf\\_Self\\_Service\\_for\\_iOS.html](https://docs.jamf.com/jamf-pro/administrator-guide/Jamf_Self_Service_for_iOS.html)**





© copyright 2002-2021 Jamf





© copyright 2002-2021 Jamf



# Automated Device Enrollment



# 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/>

Mobile Devices : PreStage Enrollments  
← JNUC2021

Options Scope

- General
- Mobile Device Names Not Configured
- User and Location
- Purchasing
- Attachments 0 Attachments
- Certificates

**General**

**Display Name:** Display name for the PreStage enrollment  
JNUC2021

**Automated Device Enrollment Instance:** Automated Device Enrollment instance to associate with the PreStage enrollment. Devices associated with the selected Automated Device Enrollment instance can be assigned the PreStage enrollment.  
Apple Business Manager

Automatically assign new devices  
Automatically assign all new devices to this PreStage enrollment

Use existing location information, if applicable

**Support Phone Number:** Support phone number for the organization

**Support Email Address:** Support email address for the organization

**Department:** Department to associate with the PreStage enrollment

Require Credentials for Enrollment  
Require the user to provide username and password on devices with iOS 7.0 or later

Supervise Devices with iOS 12.x or earlier  
Devices will be supervised

Make MDM Profile Mandatory for devices with iOS 12.x or earlier  
Require the user to apply the MDM profile

**Settings for Supervised Devices**

Pairing  
Allow devices to connect to Mac computers

Prevent Unenrollment  
Disallow the user from removing the MDM profile

Install configuration profiles before Setup Assistant  
Install configuration profiles on mobile devices in the scope before a user is presented with the Setup Assistant screens

Enable Shared iPad  
Allow devices with iOS 9.3 or later to be shared

Prevent user from enabling Activation Lock

**Enrollment Customization Configuration:** Configuration to use for customizing the user experience in the Setup Assistant  
None

[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)



Product

Editions & Pricing

Solutions

Partnerships

Support

Documentation

Resources

Contact Sales

Free Trial

**dataJAR**  
Beyond Device Management

← Back to Index

Sep 27, 2018

# MDM Me Maybe: Device Enrollment Program Security

by James Barclay

Share



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

© copyright 2002-2021 Jamf

virtual  
**JNUK**  
2021



### Enable Shared iPad

Allow devices with iOS 9.3 or later to be shared

**Number Of Users** Maximum number of user accounts that can be stored with Shared iPad

10



### Use Storage Quota Size

Specify the amount of space for each user's local storage (iPadOS 13.4 or later)



### Prevent user from enabling Activation Lock



Enable Activation Lock on the device (Apple School Manager, Apple Business Manager)

[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)



© copyright 2002-2021 Jamf



# 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      | The user cannot use it.   |
|  | iPadOS   |   |
|  | macOS    |   |
| Specific iCloud features                 | iOS      | The user cannot access the following services:  |
|  | iPadOS   |   |
|  | macOS    |   |
|  | Web      | <ul style="list-style-type: none"> <li>• iCloud Mail</li> <li>• iCloud Family Sharing</li> <li>• Allow iMessage in iCloud</li> <li>• iCloud Keychain (although keychain items are saved and restored on Shared iPad devices)</li> </ul> |
| App Store<br>iTunes Store<br>Apple Books | iOS      | Allows browsing but not purchasing, paid or free.   |
|  | iPadOS   |   |
|  | macOS    |   |

<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>

Mobile Devices : PreStage Enrollments

← JNUC2021

Options Scope

**i General**

**Mobile Device Names** >  
Not Configured

User and Location

Purchasing

Attachments  
0 Attachments

Certificates

**Configure Mobile Device Names**

Use this section to define settings for the mobile device naming method to apply during enrollment.

[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)

Mobile Devices : PreStage Enrollments

← New Mobile Device PreStage Enrollment

Options Scope

**i General**

- Mobile Device Names** > 1 Payload Configured
- User and Location
- Purchasing
- Attachments 0 Attachments
- Certificates

Mobile Device Names

**Naming Method** Method to use to name mobile devices

- Default Names
- List of Names
- Serial Numbers
- Single Name

[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)

Mobile Devices : PreStage Enrollments

← New Mobile Device PreStage Enrollment

Options Scope

**i General**

**Mobile Device Names** >  
1 Payload Configured

User and Location

Purchasing

Attachments 0 Attachments

Certificates

Mobile Device Names

**Naming Method** Method to use to name mobile devices

Serial Numbers ▾

**Enforce Mobile Device Names**  
Mobile device name will revert to the value entered if the device name is changed by the user

Prefix

Suffix

[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)

Inventory   Management   History

**i General**  
DMPZX1W6MF3M >

**Hardware**  
iPad 7th Generation (Wi-Fi)

**User and Location**

**Shared iPad Users**  
2 Shared iPad Users

**Edit General Information**

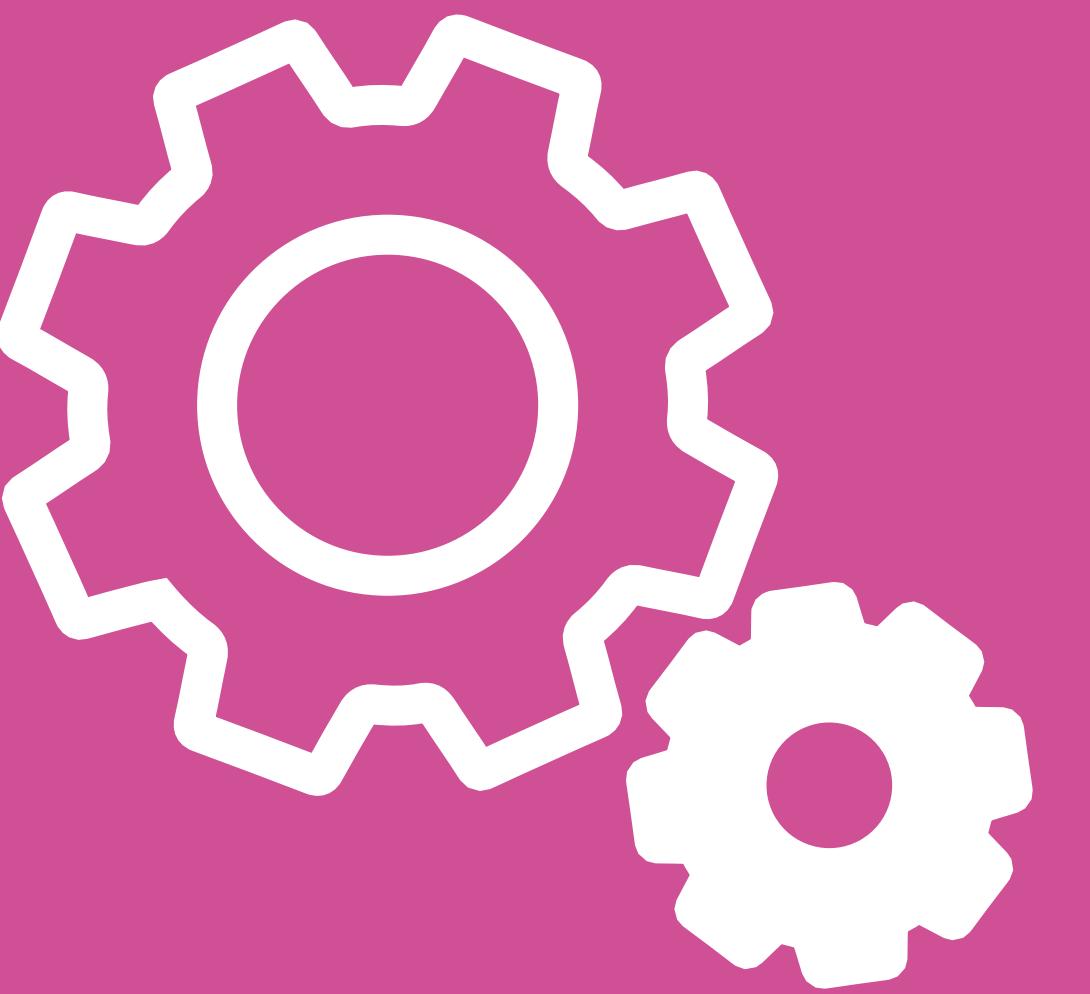
**Enforce Mobile Device Name**  
Mobile device name will revert to the value entered if the device name is changed by the user

**Mobile Device Name**  
JNUC2021

**Asset Tag**

Cancel   Save

# Device Management Settings



|   |   |                                     |
|---|---|-------------------------------------|
| <b>Documents from managed sources open in unmanaged destinations</b><br>iOS   | <input type="button" value="Restrict"/> <input checked="" type="button" value="Allow"/> | <input checked="" type="checkbox"/> |
| <b>Documents from unmanaged sources open in managed destinations</b><br>iOS   | <input type="button" value="Restrict"/> <input checked="" type="button" value="Allow"/> | <input checked="" type="checkbox"/> |
| <b>Pasteboard respects managed/unmanaged document restrictions</b><br>iOS, tvOS, If enforced, pasteboard respects document settings for managed/unmanaged destinations (e.g., prevents managed apps content from being pasted into unmanaged apps). | <input type="button" value="Enforce"/> <input checked="" type="button" value="Ignore"/> | <input checked="" type="checkbox"/> |
| <b>Managed apps can write contacts to unmanaged contacts accounts</b><br>iOS 12 or later  | <input type="button" value="Restrict"/> <input checked="" type="button" value="Allow"/> | <input checked="" type="checkbox"/> |
| <b>Unmanaged apps to read contacts from managed contacts accounts</b><br>iOS 12 or later  | <input type="button" value="Restrict"/> <input checked="" type="button" value="Allow"/> | <input checked="" type="checkbox"/> |
| <b>AirDrop as unmanaged destination</b><br>iOS 9 or later   | <input type="button" value="Enforce"/> <input checked="" type="button" value="Ignore"/> | <input checked="" type="checkbox"/> |

[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)

## Shared iPad (device) temporary session

iOS 13.4 or later

Restrict   Allow



## Installing apps using Apple Configurator and iTunes

iOS 9 or later

Restrict   Allow



### Installing apps using App Store

iOS 9 or later, Supervised

Restrict   Allow



### Automatic app downloads

iOS 9 or later, Supervised

Restrict   Allow



## Removing apps

iOS, Supervised

Restrict   Allow



## Removing system apps

iOS 11 or later

Restrict   Allow



[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<sup>1</sup> these apps from your device:

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

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



[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)

# 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

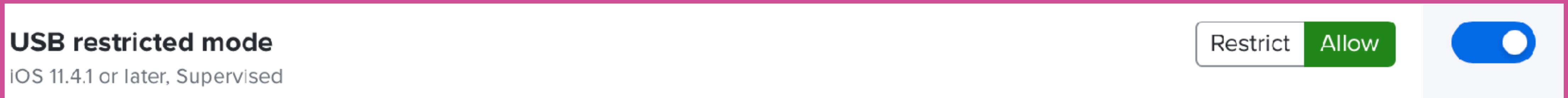
Restrict Siri  
web search

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](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>**

**Modifying device name**

iOS 9 or later, tvOS 11 or later, Supervised

Restrict    Allow



**Modifying wallpaper**

iOS 9 or later, Supervised

Restrict    Allow



[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)

Mobile Devices : Smart Device Groups  
← All Managed iPads

Mobile Device Group Criteria Automated Management

Set Wallpaper (supervised only)  
0 Eligible, 1 Ineligible

Set Wallpaper (supervised only)  
Automatically set wallpaper on devices when they become members of this smart group

Wallpaper Screens Screen to set wallpaper for  
 Lock Screen  
 Home Screen  
 Both

Wallpaper Image Image or photo to set as wallpaper. It is recommended that you use a file with the JPEG or PNG format



LockScreen.png

Schedule Ongoing Commands  
Schedule additional times for this management command to be sent to members of this smart group

Once per day  
  
 9 : 00 a.m.

Command History

| NAME     | STATUS  | DATE ISSUED            | FILENAME       |
|----------|---------|------------------------|----------------|
| JNUC2021 | Pending | Less than a minute ago | LockScreen.png |

Show: 10

[https://docs.jamf.com/jamf-pro/administrator-guide/  
Smart\\_Groups.html](https://docs.jamf.com/jamf-pro/administrator-guide/Smart_Groups.html)



© copyright 2002-2021 Jamf



## Lock Screen Message

Settings configured: 2

Exclude all

Include



### Lock Screen Footnote

Footnote displayed in the login window and Lock screen

(\*・∀・)ノ^ Hi there JNUC2021!



### Asset Tag Information

Message displayed at the bottom of the login window and Lock screen

\$EMAIL

[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)



© copyright 2002-2021 Jamf







© copyright 2002-2021 Jamf



Web Clips

**Label** The name to display for the Web Clip

**URL** The URL to be displayed when opening the Web Clip

**Removable**  
Enable removal of the Web Clip

**Icon** The icon to use for the Web Clip. It is recommended that you use a file with the GIF, ICO, or PNG format



**Upload Icon**

**Precomposed Icon**  
The icon will be displayed with no added visual effects

**Full Screen**  
Displays the Web Clip as a full screen app

[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)



© copyright 2002-2021 Jamf



## 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)



Mobile Devices : Configuration Profiles

← macmule webclip

Options Scope



General



Single Sign-On Extensions  
Not configured



Web Clips  
1 payload configured

General

**Name** Display name of the profile (shown on the device)

macmule webclip

**Description** Brief explanation of the content or purpose of the profile

**Category** Category to add the profile to

None

**Level** Level at which to apply the profile

User Level



User-level profiles are installed automatically and cannot be made available in Self Service.

[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>**

Wi-Fi

**Service Set Identifier (SSID)** Identification of the wireless network to connect to

[Required]

**Hidden Network**  
Enable if target network is not open or broadcasting

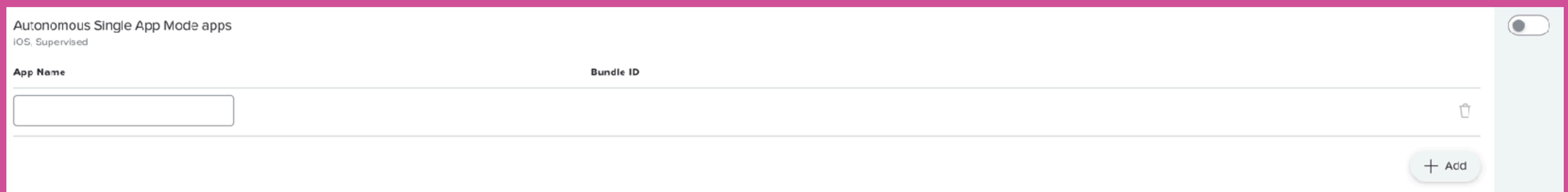
**Auto Join**  
Automatically join this wireless network

**Disable Captive Network Detection**  
Do Not Show Captive Network Assistant

**Disable MAC Address Randomization (iOS 14 or later)**  
Disables MAC Address randomization for this wireless network while the device is connected with the network

**i** Displays a warning in the device's Settings indicating this network has reduced privacy protections.

<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)

## Single App Mode

**Targeted Operating System** The type of operating system Single App Mode will target

- iOS
- tvOS

**Lock To App** The app to run in Single App Mode (supervised only)

Jamf Self Service ▾

**Options** Settings enforced when in Single App Mode

- Touch  
When this option is on, it disables all touch input on the device
- Motion  
When this option is on, it doesn't allow automatic rotating of the screen when the device is rotated
- Volume Buttons  
When this option is on, the volume buttons are disabled
- Side Switch  
When this option is on, the ringer switch is disabled
- Sleep/Wake Button  
When this option is on, the Sleep/Wake button is disabled so the device can't be put to sleep or turned off
- Auto-Lock  
When this option is on, Auto-Lock is disabled
- VoiceOver  
When this option is on, VoiceOver is enabled
- Zoom  
When this option is on, Zoom is enabled
- Invert Colors  
When this option is on, inverting the colors on the screen is enabled
- AssistiveTouch  
When this option is on, Assistive Touch is enabled
- Speak Selection  
When this option is on, iOS will speak aloud whatever is selected on the screen
- Mono Audio  
When this option is on, both right and left channels play through a single channel
- Voice Control  
When this option is on, Voice Control is enabled

Allow the user to change these settings when in Single App Mode

- VoiceOver  
Describes aloud what appears on the screen
- Zoom  
Zooms in on content on the screen to make it larger and easier to see
- Invert Colors  
Inverts the colors onscreen
- AssistiveTouch  
Adapts the Multi-Touch screen of iOS devices to a user's unique physical needs
- Voice Control  
Controls devices with a user's voice

[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)

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

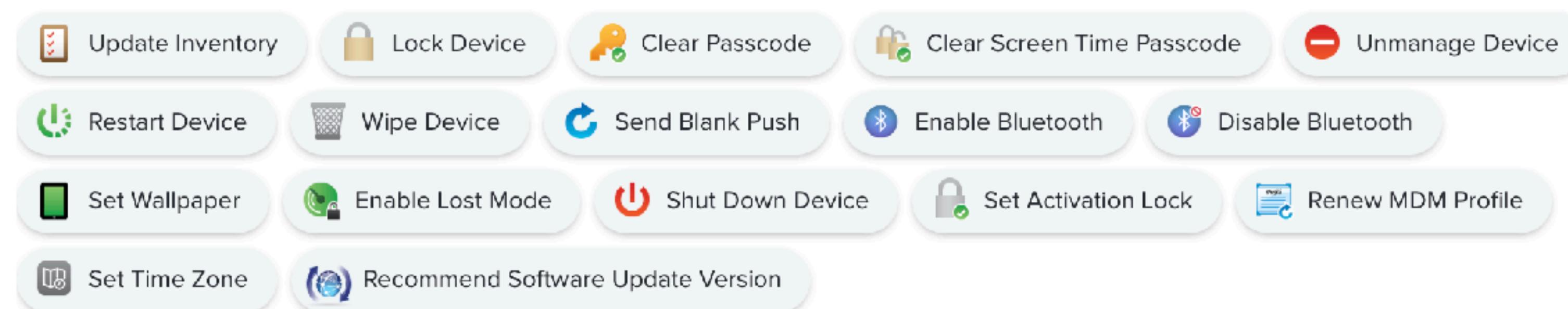
# Remote Commands



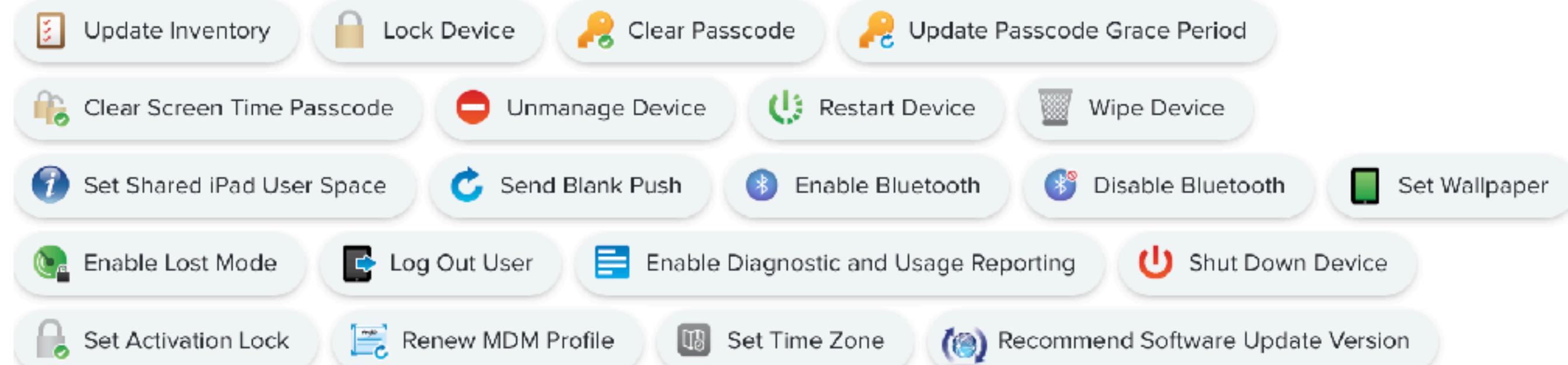
**Note:** If an iOS device has a passcode enabled, the Update iOS Version mass action command will download the update on the device, but fail to install it. To ensure the update is installed, users must enter their passcode when prompted. You can clear the passcode before sending the mass action to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

[https://docs.jamf.com/best-practice-workflows/jamf-pro/managing-ios-updates/Updating\\_iOS.html](https://docs.jamf.com/best-practice-workflows/jamf-pro/managing-ios-updates/Updating_iOS.html)

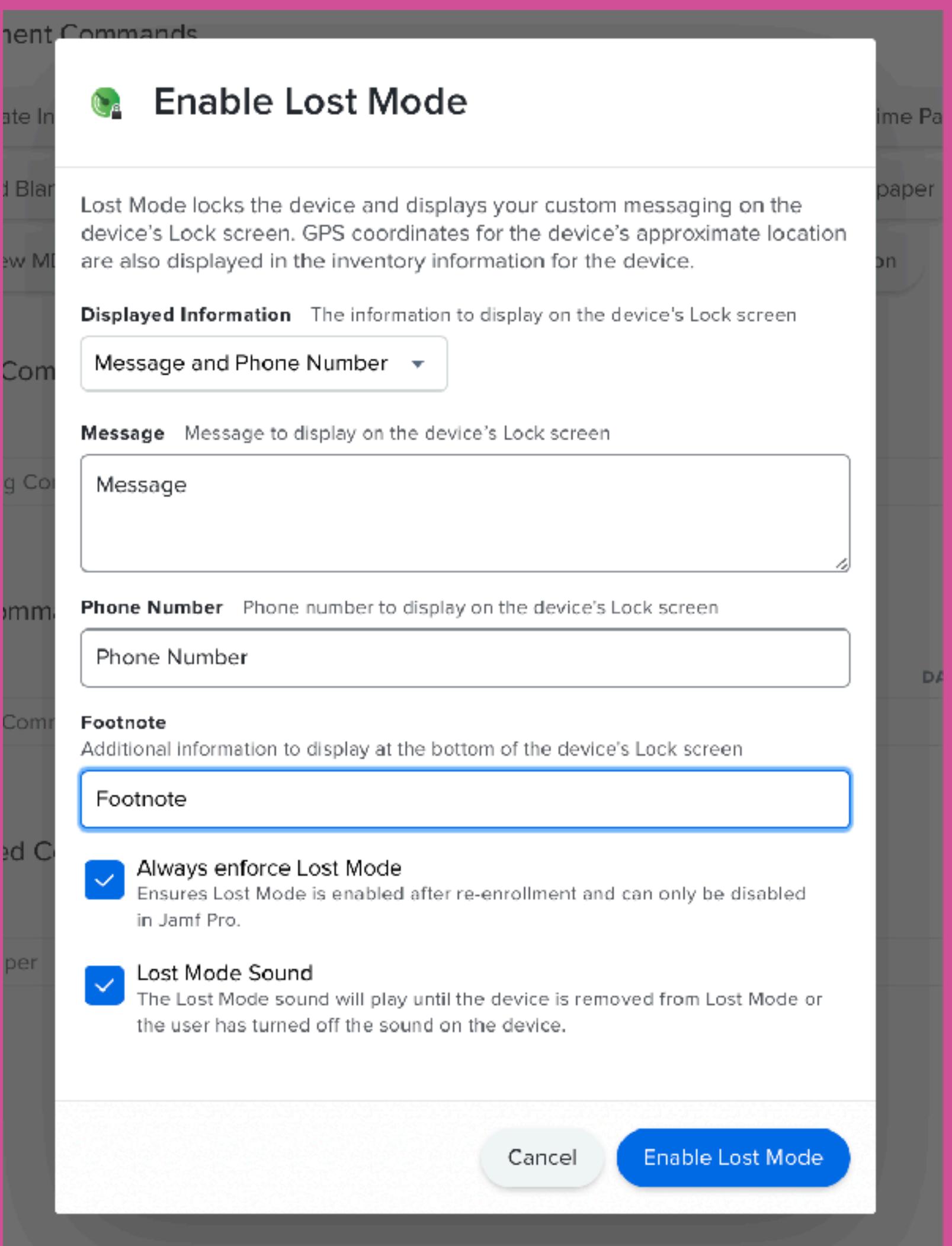
## Management Commands



## Management Commands



[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)

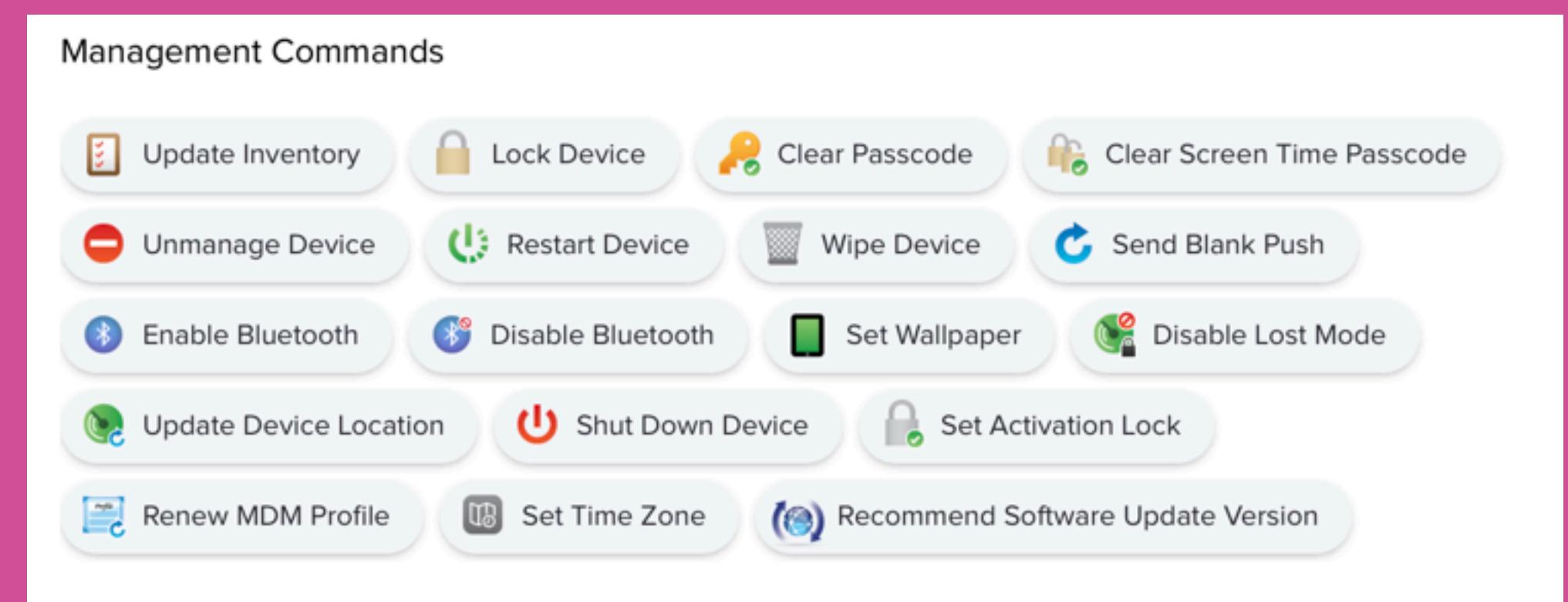
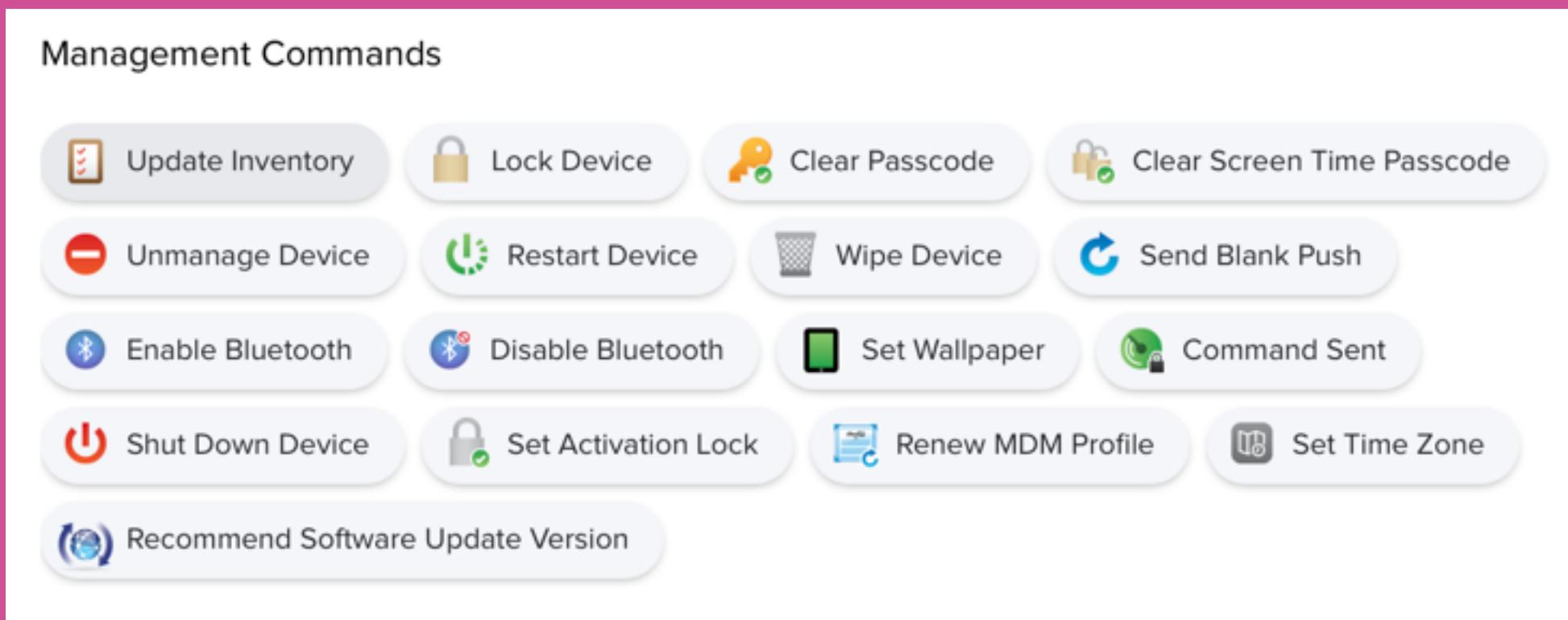


[https://docs.jamf.com/jamf-pro/administrator-guide/  
Remote\\_Commands\\_for\\_Mobile\\_Devices.html](https://docs.jamf.com/jamf-pro/administrator-guide/Remote_Commands_for_Mobile_Devices.html)



© copyright 2002-2021 Jamf





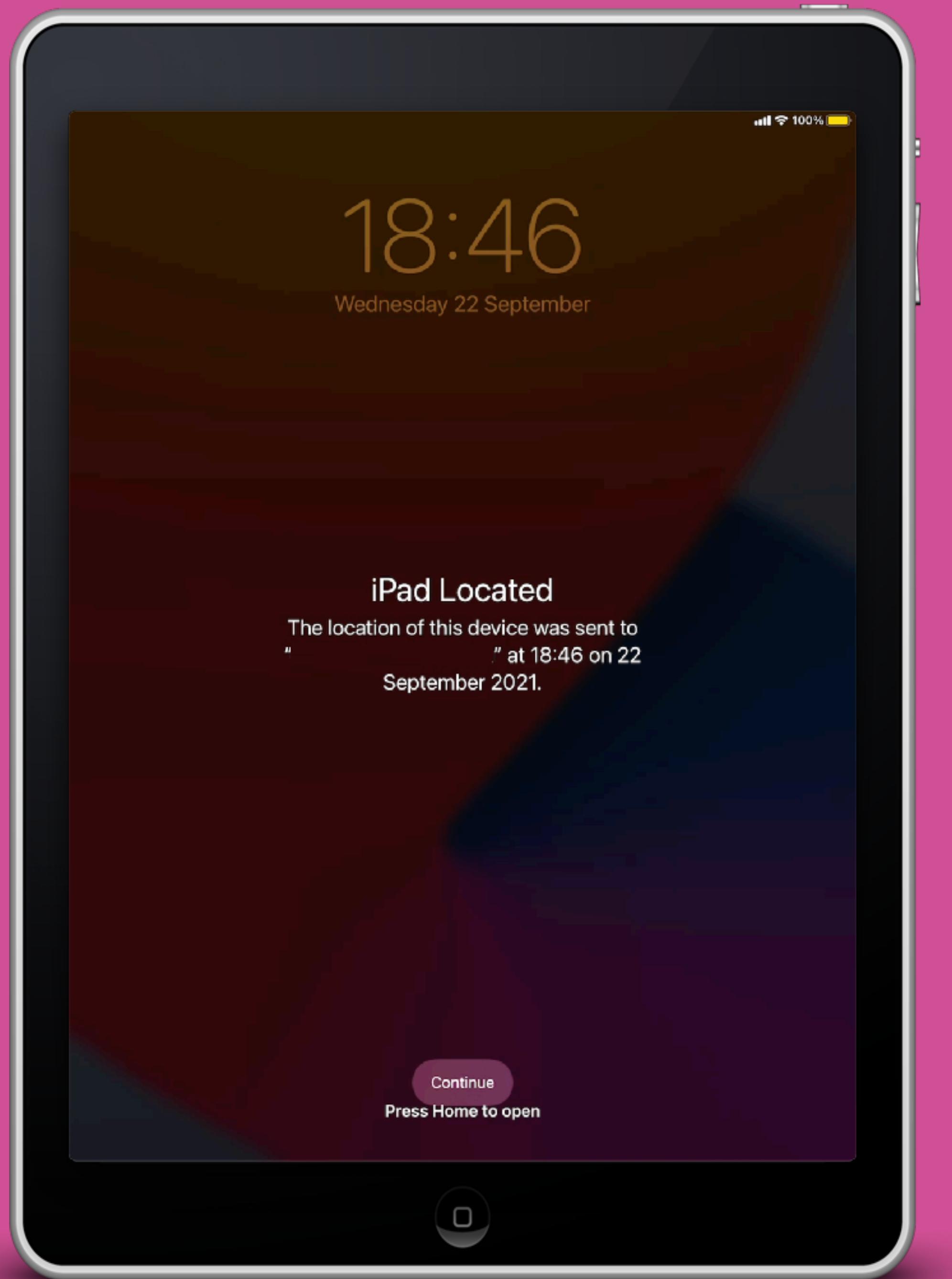
[https://docs.jamf.com/jamf-pro/administrator-guide/  
Remote\\_Commands\\_for\\_Mobile\\_Devices.html](https://docs.jamf.com/jamf-pro/administrator-guide/Remote_Commands_for_Mobile_Devices.html)

The screenshot shows the Jamf Pro administrator interface. On the left, a sidebar lists various management categories: Purchasing, Security (with a note: "Data protection is not enabled"), Apps (1 App), Managed eBooks (0 Managed eBooks), Network, Certificates (2 Certificates), Profiles (3 Profiles), Provisioning Profiles (0 Provisioning Profiles), Attachments (0 Attachments), and AirPlay Permissions. The main panel displays device location details for a lost mode event:

- Lost Mode (supervised only): Enabled**
- Always enforce Lost Mode: Enabled**
- Lost Mode Message: Message**
- Lost Mode Phone Number: Phone Number**
- Lost Mode Footnote: Footnote**
- Last Location Update: Less than a minute ago**
- Approximate Location: N W**
- Horizontal Accuracy: 65.00 meters**
- Vertical Accuracy: 10.00 meters**
- Altitude: 71.84 meters**
- Speed: Undetermined**
- Course: Undetermined**
- Timestamp: 22/09/2021 at 5:43 PM**

At the bottom right of the main panel are two buttons: "Play Sound" and "Update Location".

[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)

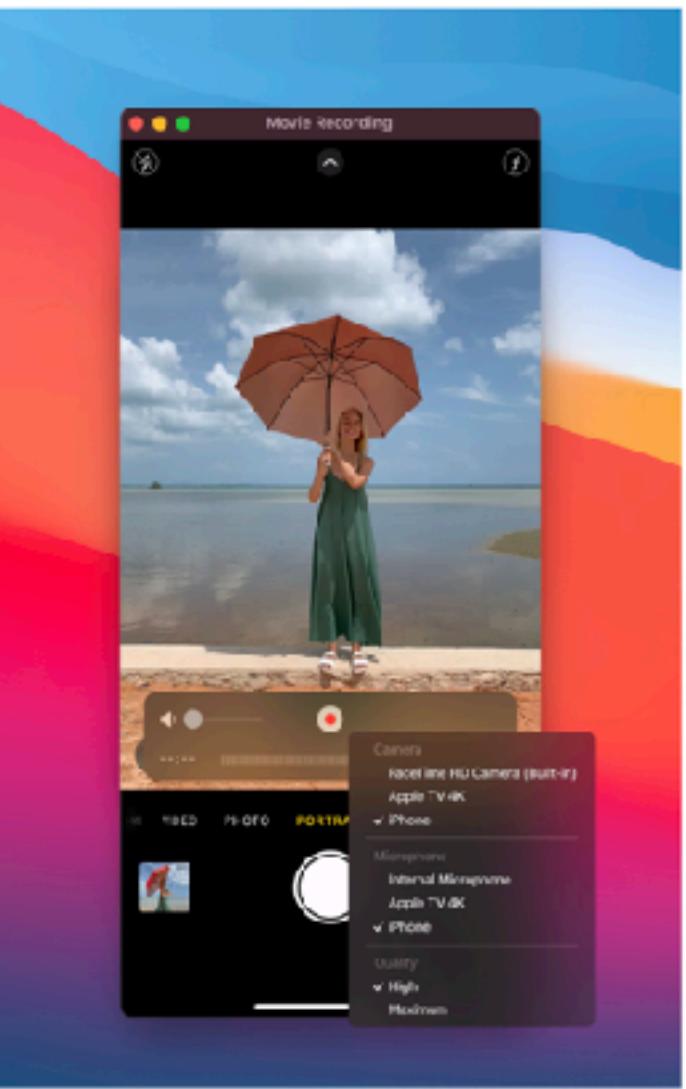


# Additional Tips



## 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.



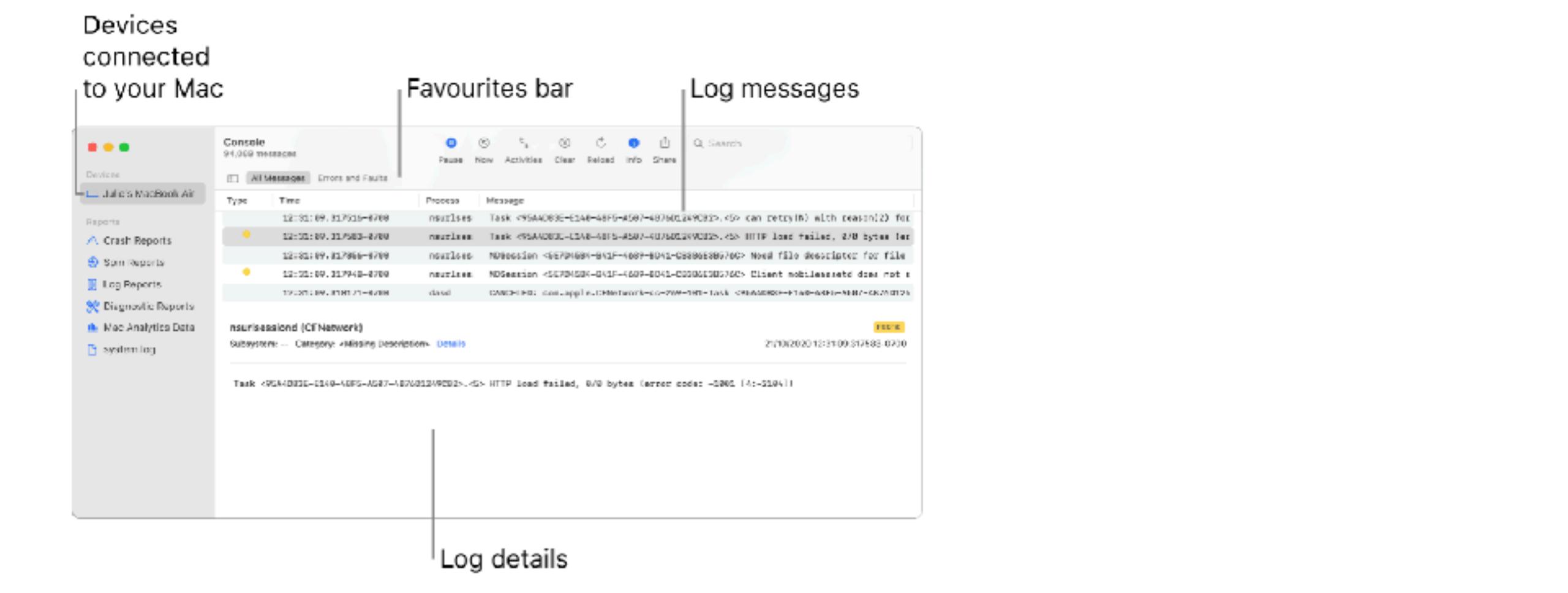
1. Connect your device to your Mac.
2. Open the QuickTime Player app  on your Mac.
3. Choose File > New Movie Recording.
4. Click the Options pop-up menu, then choose any of the following recording options:
  - **Camera:** Choose your connected iPhone, iPad or iPod touch.
  - **Microphone:** Choose a 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/>

# Thank you for listening!