How to Configure Account-Driven Enrollment and Enroll a Personal Device in Jamf Pro

Rev. 20230830

Contents

Preface

Account-driven User Enrollment Explained

Account-driven User Enrollment is designed for organizations that need personal devices enrolled into Mobile Device Management. This method of enrollment supports Bring Your Own Devices (BYOD) scenarios, where the user owns the device but need access to the organization's resources. This provides for a combination of security for the organization, and privacy for the user.

What are the core components of Account-driven User Enrollment?

- A Managed Apple ID - An Apple ID managed by the organization.
- Data separation - A secure APFS volume to keep organizational data separate from personal.
- Limited management capabilities - Limited management capabilities due to user ownership.

Requirements:

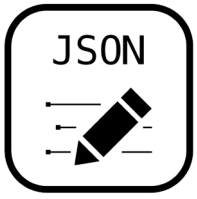
- Access to organization's web host
- An MDM solution (in this guide, we will use Jamf Pro)
- An unsupervised iOS/iPadOS device

Section 1: Setting Up the Discovery URL

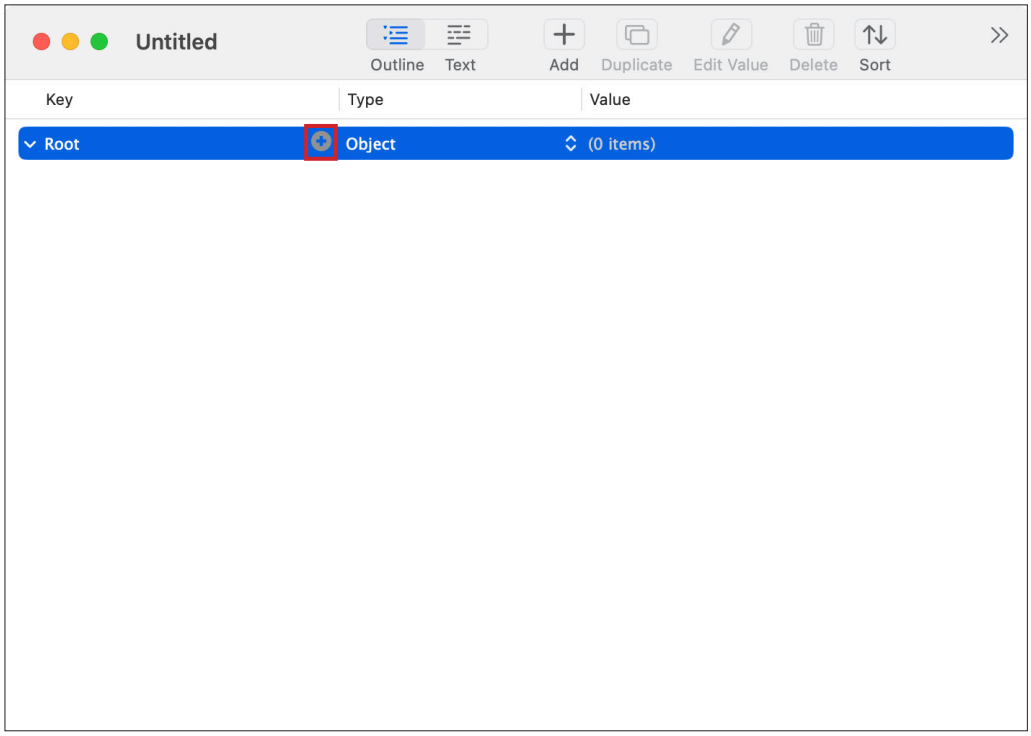
You will need an application to create your JSON file in. Although this can be done in a text editor, it would be recommended to use an application that can verify your input. This guide will use JSON Editor, which is available for free from the App Store.

https://apps.apple.com/us/app/json-editor/id567740330?mt=12

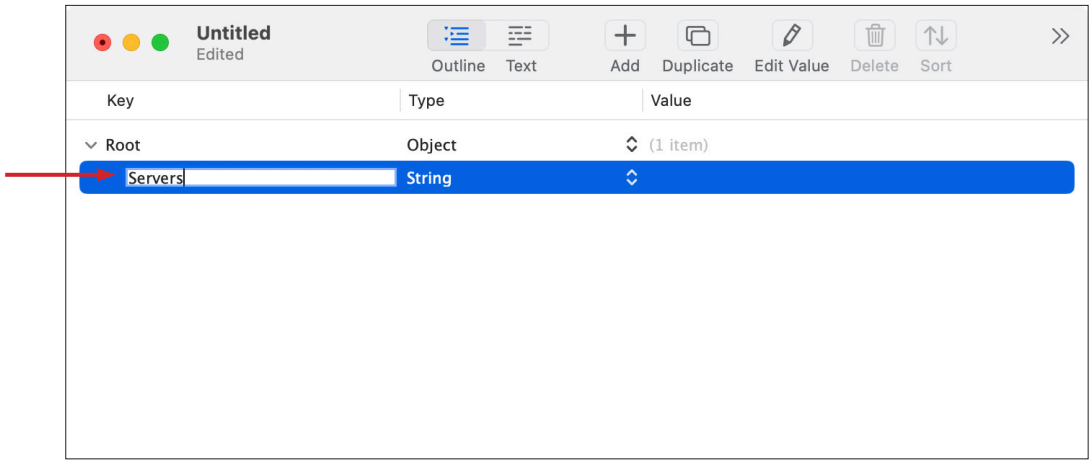
1. Open JSON Editor.



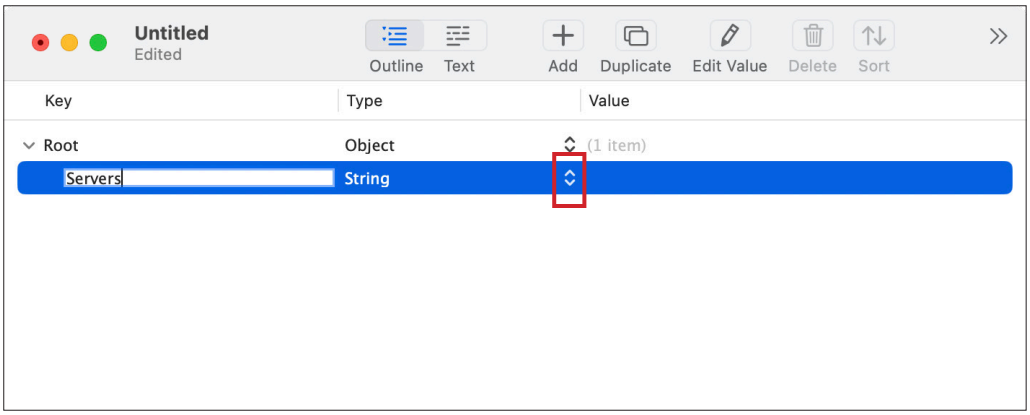
2. Hover over the Root key and click Add (⊕) to create a new item.



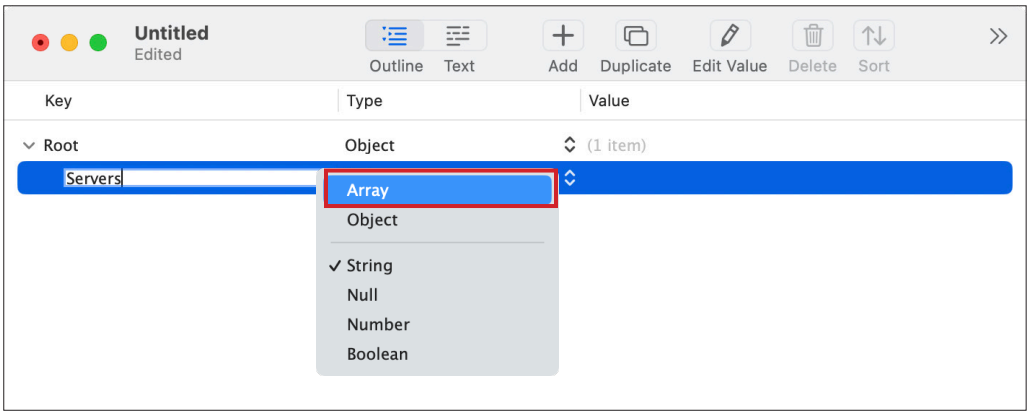
3. Label the object, Servers.



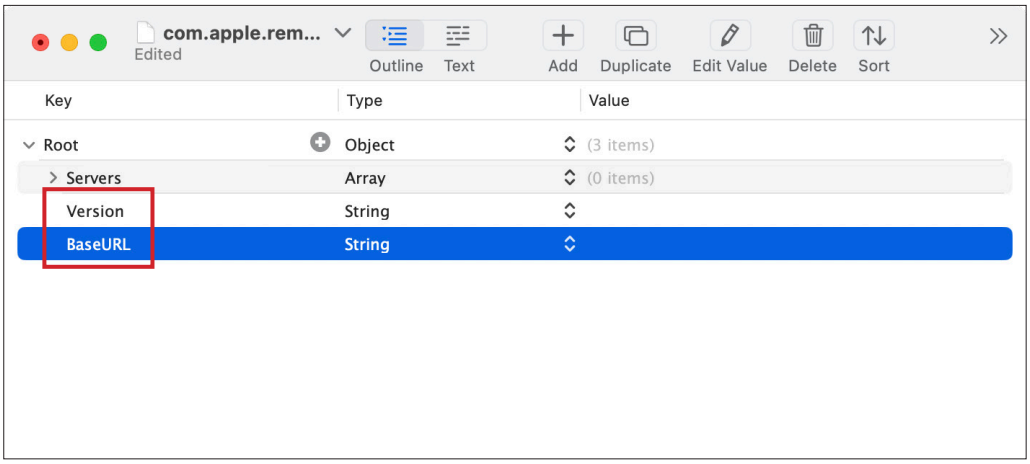
4. Click the Type menu (⇕) to the right of the Servers string.



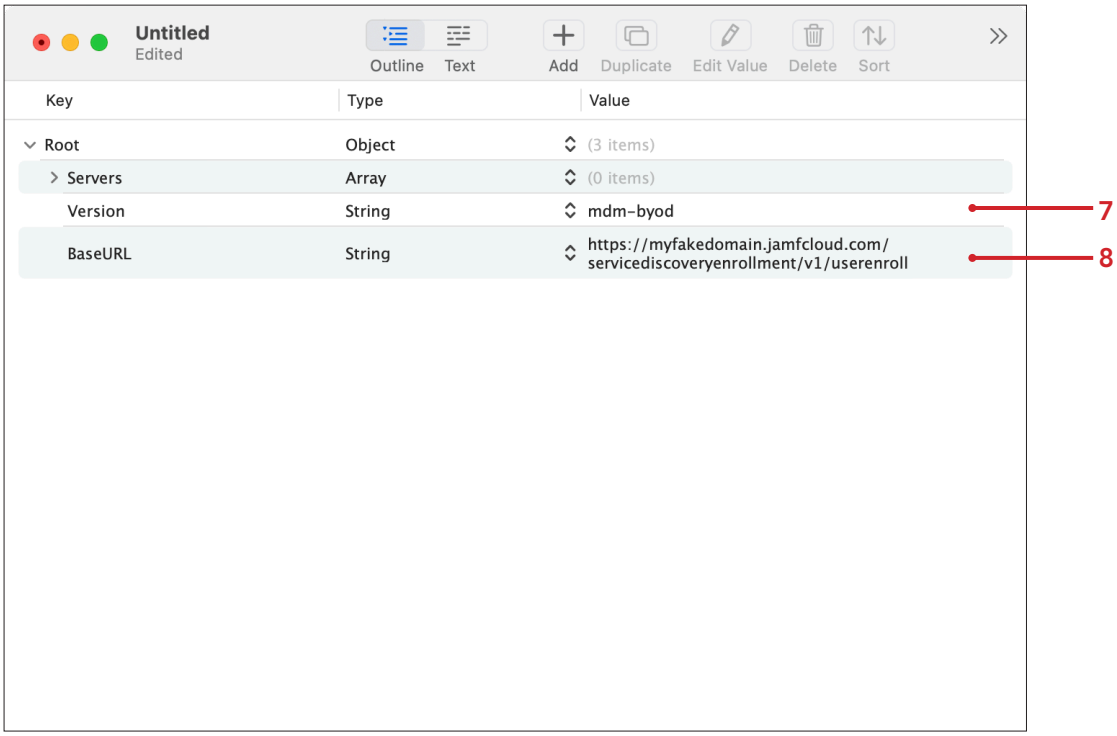
5. Select Array from the menu



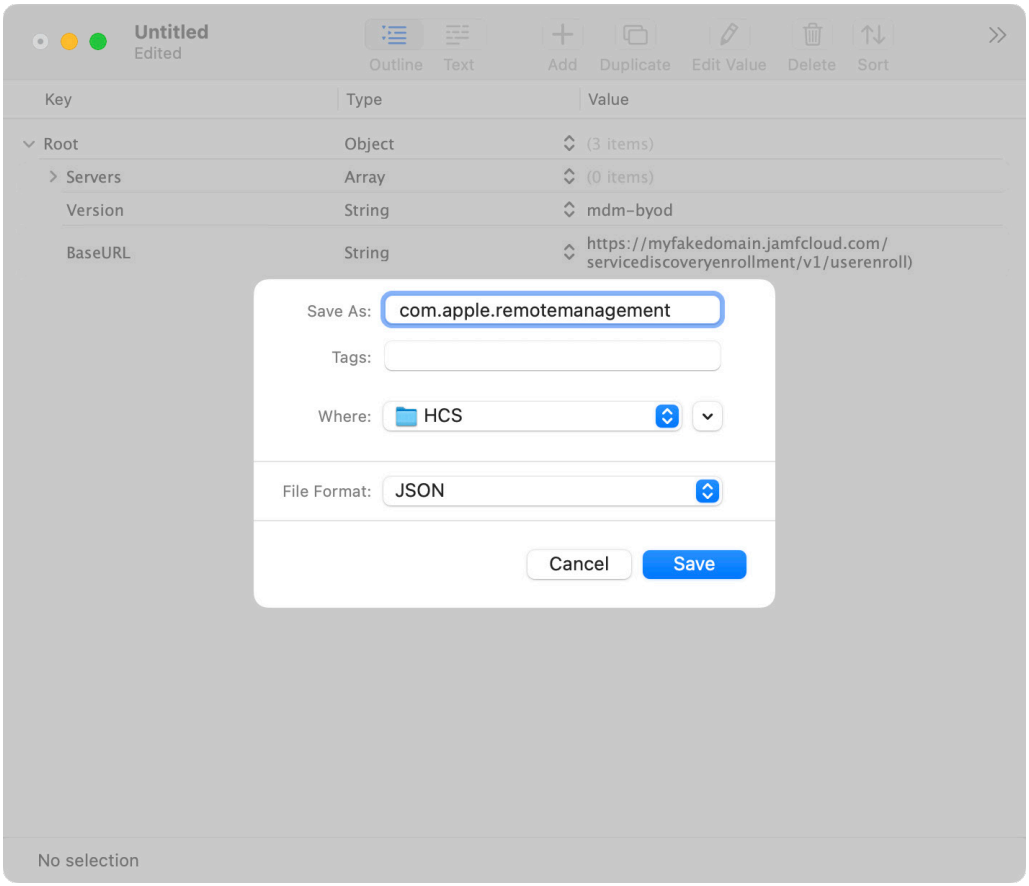
6. Create two new additional String objects below Servers and label them Version and BaseURL.



7. In the Value column for Version, enter mdm-byod.
8. In the value for BaseURL, enter the following:
   https://[Your-MDM-URL]/servicediscoveryenrollment/v1/userenroll
   (ie. https://myfakedomain.jamfcloud.com/servicediscoveryenrollment/v1/userenroll)

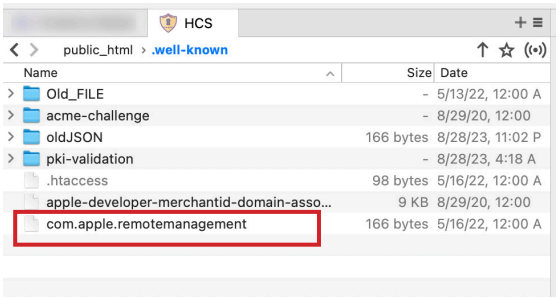


9. Save with the specific file name of com.apple.remotemanagement.
   IMPORTANT: This file name is critical since it is what the enrollment process will look for.



10. Upload this file to your domain host in this specific location:
    https://YOUR-WEB-SERVER-FQDN-HERE/.well-known/com.apple.remotemanagement

    NOTE: The steps to upload your JSON file will differ based on the entity that hosts your domain services.



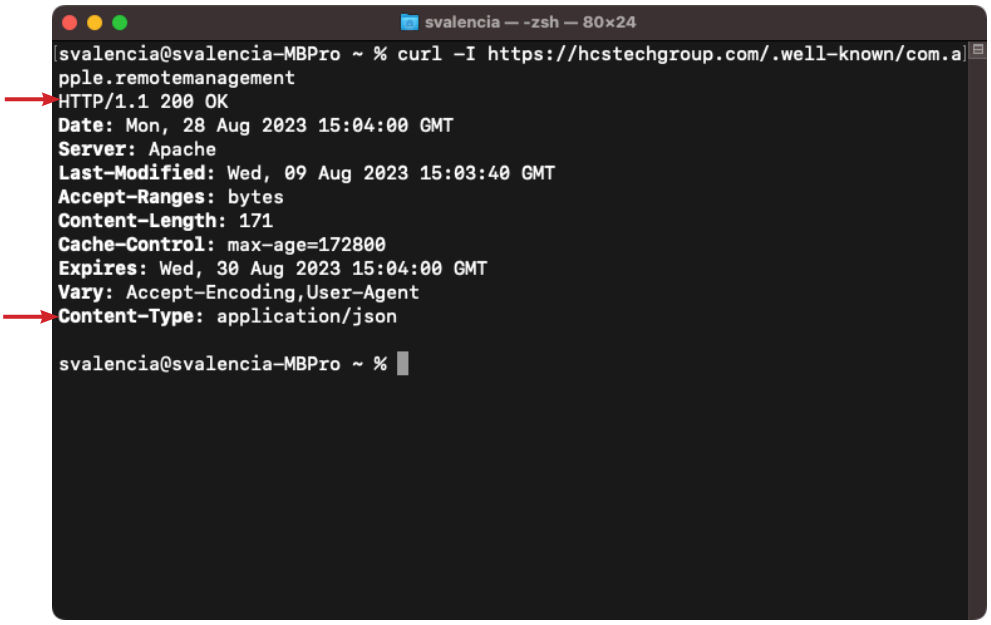
11. Open Terminal from /Applications.

12. Enter the following command:

```
curl -I https://YOUR-WEB-SERVER-FQDN-HERE/.well-known/com.apple.remotemanagement
```

(ie. curl -I https://hcstechgroup.com/.well-known/com.apple.remotemanagement)

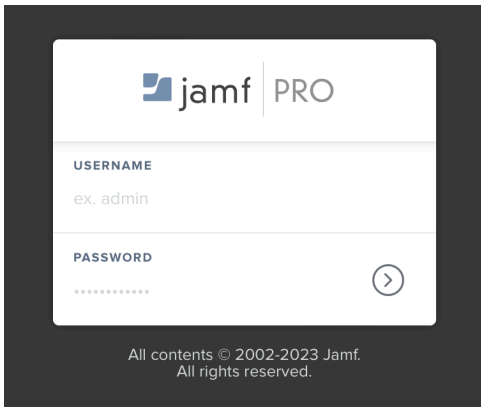
13. Verify the response shows OK and Content-Type is application/json.



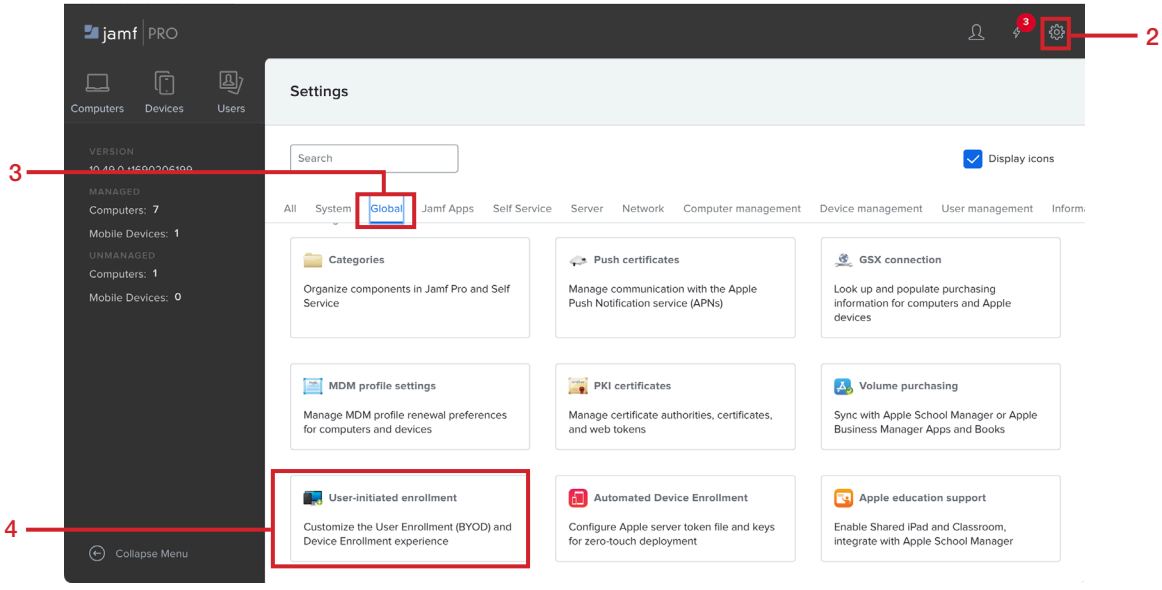
Section 2: Configuring Account-driven User Enrollment in Jamf Pro

The steps detailed in this section are specific to Jamf Pro. Check with your MDM vendor for steps on how to enable Account-driven User Enrollment.

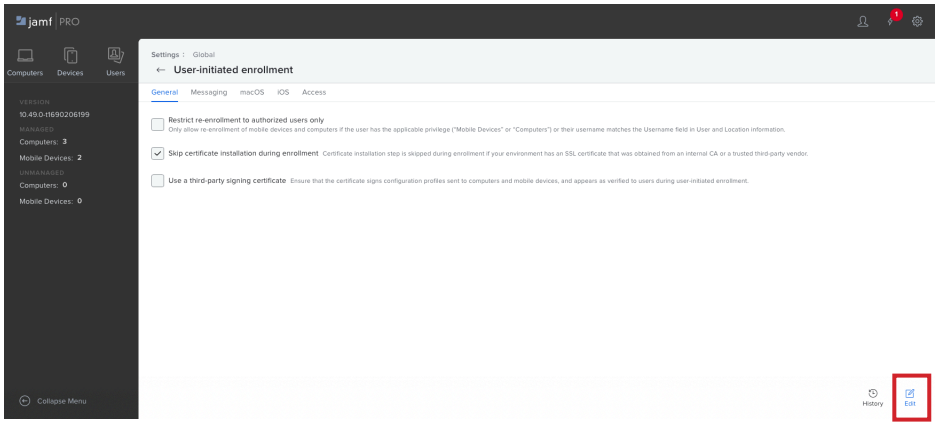
1. Log into Your Jamf Pro Server.



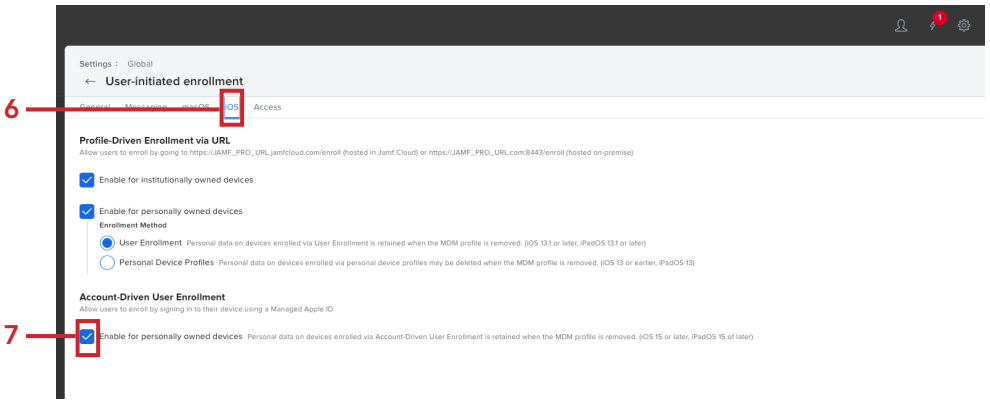
2. On the top-right corner, click Settings (⚙).
3. Click Global.
4. Click User-initiated Enrollment.



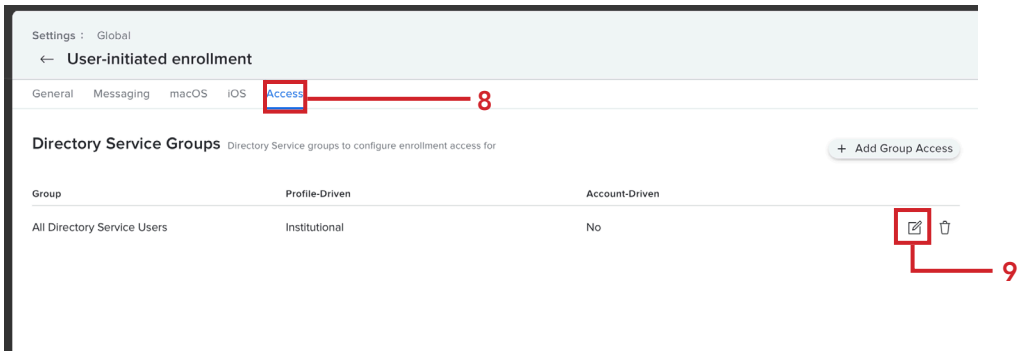
5. Click Edit.



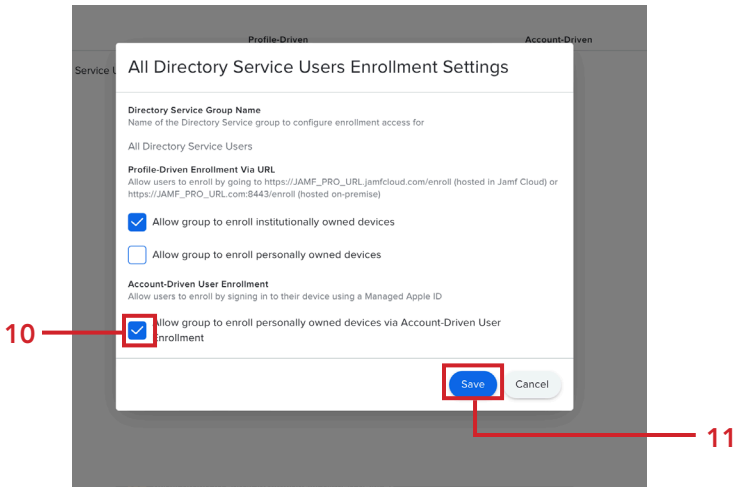
6. Click iOS
7. Under Account-Driven User Enrollment, select the checkbox for personally owned devices.



8. Click Access.
9. Click Edit (☑)

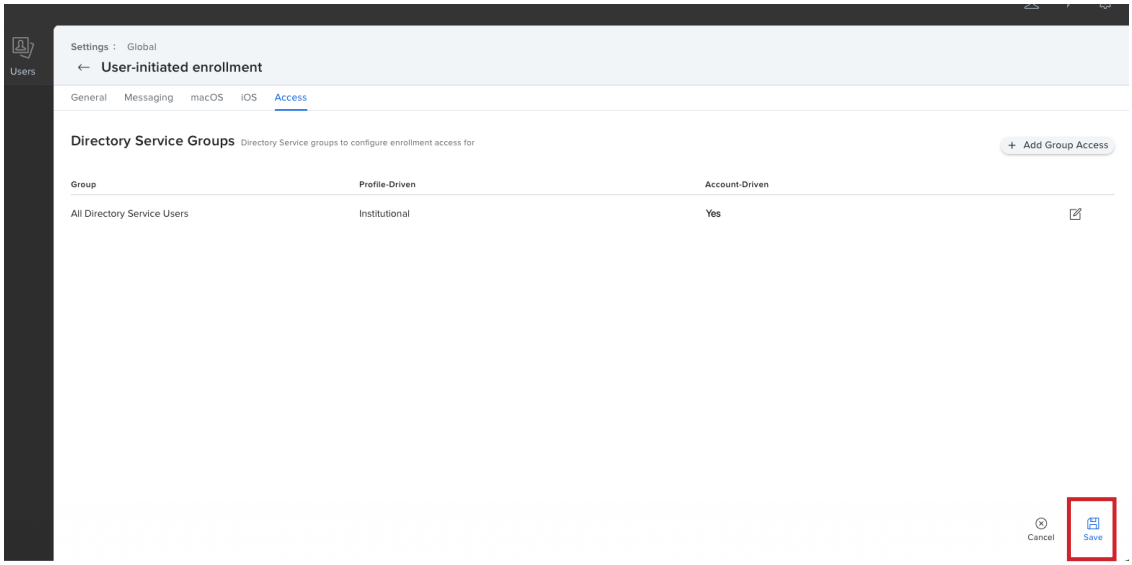


10. Select the checkbox for Allow group to enroll personally owned devices via Account-Driven User Enrollment.
11. Click Save.



12. Click Save.
    NOTE: The ability to allow directory service users to participate in Account-driven User Enrollment is due to previously configuring Cloud Identity Providers within Jamf. For more details, please see our guide on Microsoft Azure Active Directory with Jamf Pro.

    https://hcsonline.com/support/white-papers/a-guide-to-integrate-azure-active-directory-with-jamf-pro

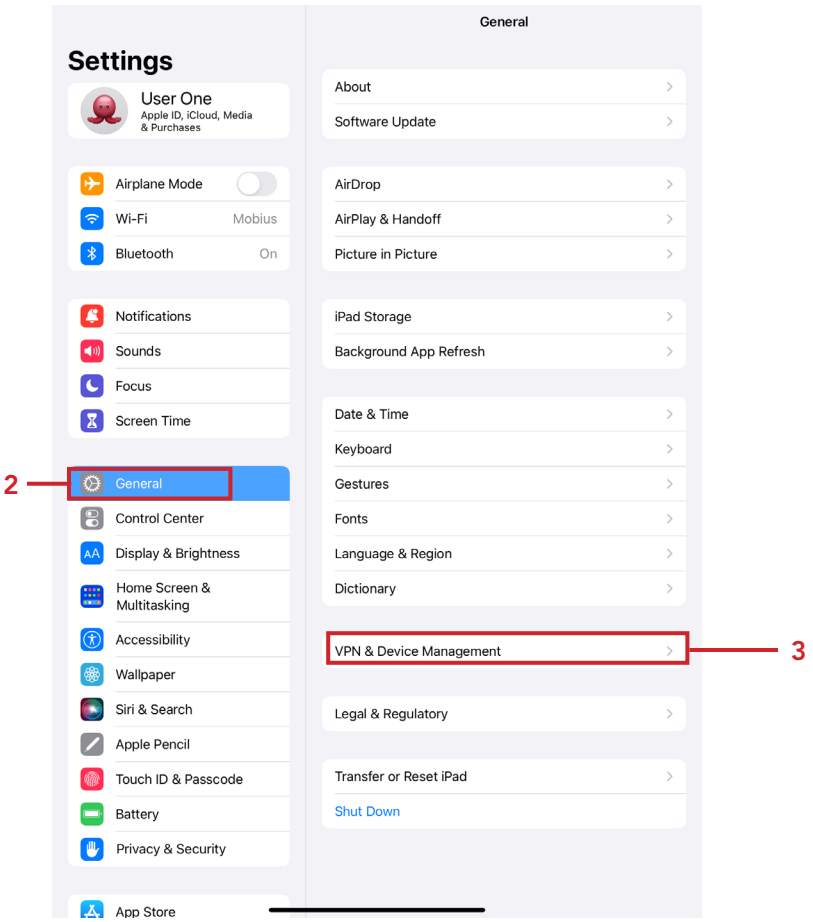


Section 3: Enrolling an iOS or iPadOS Device

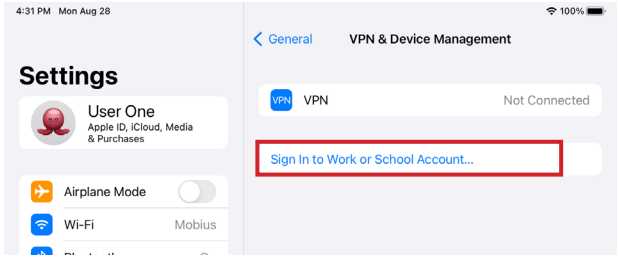
Before enrolling BYOD into an MDM solution, it is important to know what functions are possible on a personally owned device:

MDM can	MDM can't
☑ Configure accounts	☒ See personal information, usage data or logs
☑ Configure Per App VPN	☒ Access inventory of personal apps
☑ Install and configure apps	☒ Remove any personal data
☑ Require a passcode on iPhone or iPad	☒ Take over management of a personal app
☑ Enforce certain restrictions	☒ Require a complex iPhone and iPad passcode
☑ Access inventory of work apps	☒ Remotely wipe the entire device
☑ Remove work data only	☒ Access unique device identifiers
	☒ Access device location
	☒ Manage Activation Lock
	☒ Access roaming status
	☒ Turn on Lost Mode

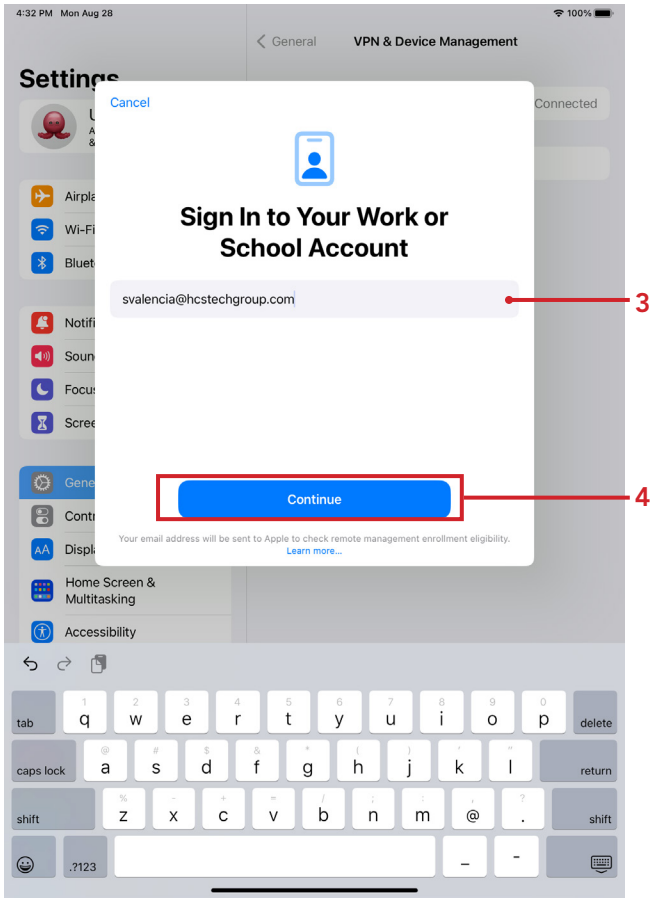
1. On your iPad, tap Settings.
2. Tap General
3. Tap VPN & Device Management.



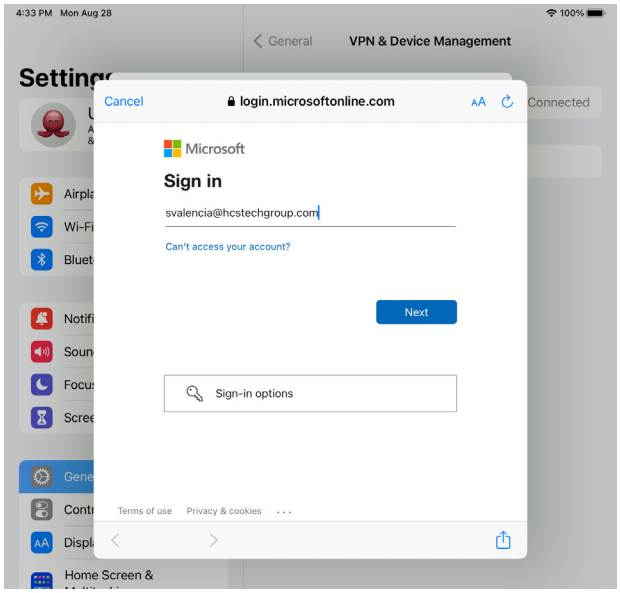
2. Tap Sign In to Work or School Account.



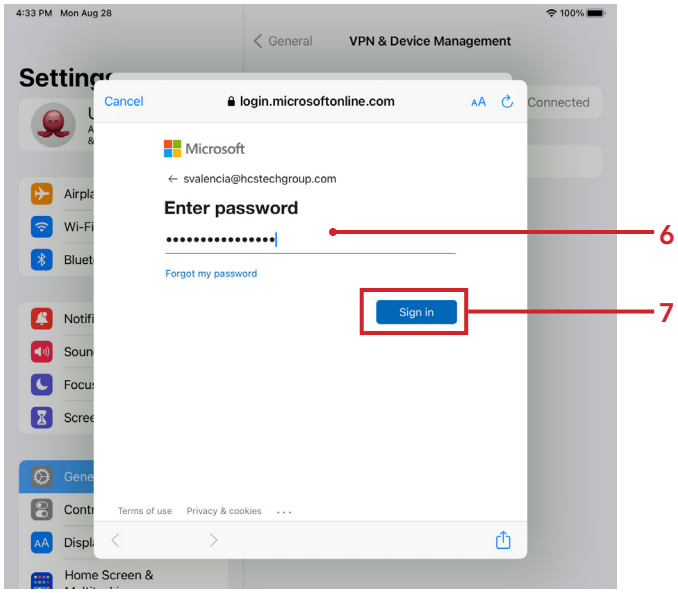
3. Enter your Managed Apple ID.
4. Tap Continue.



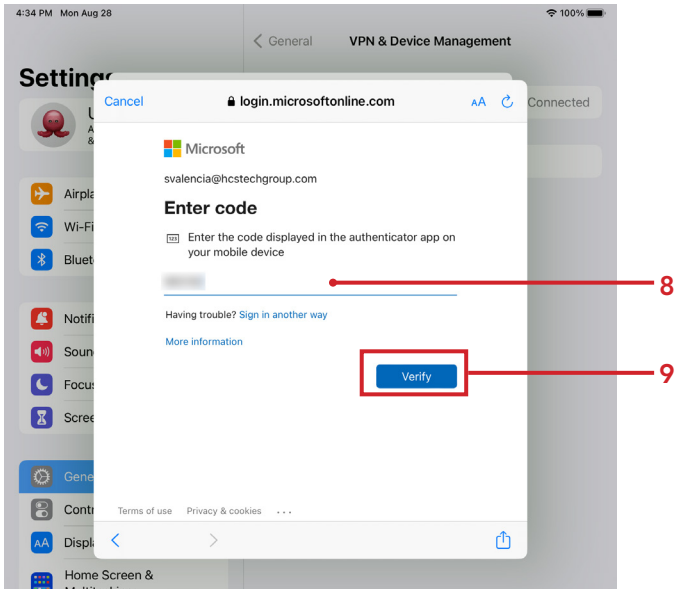
5. Tap Next.
   NOTE: This can be a built-in Jamf Pro account or you can connect Jamf Pro with your Identity Provider. This guide uses Managed Apple ID federation with Microsoft Azure.



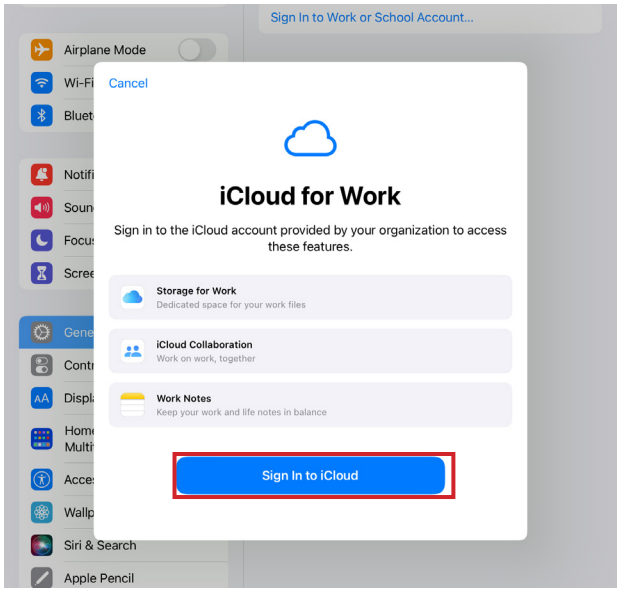
6. Enter your password.
7. Tap Sign in.



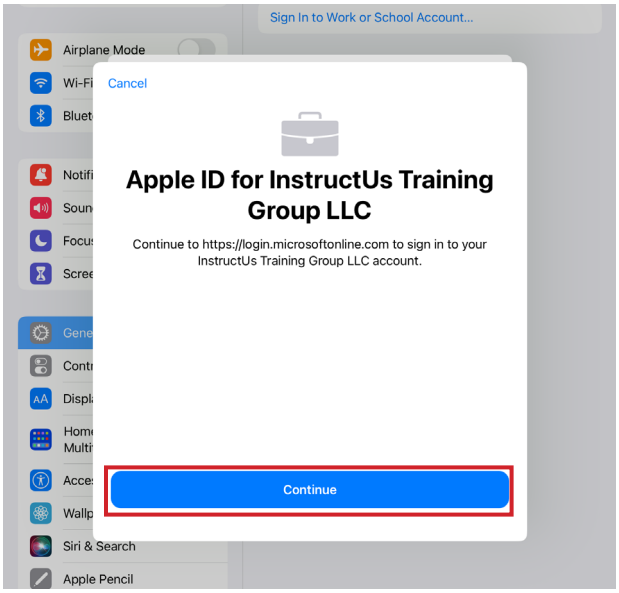
8. Enter the code displayed in the authenticator app on your mobile device.
9. Tap Verify.



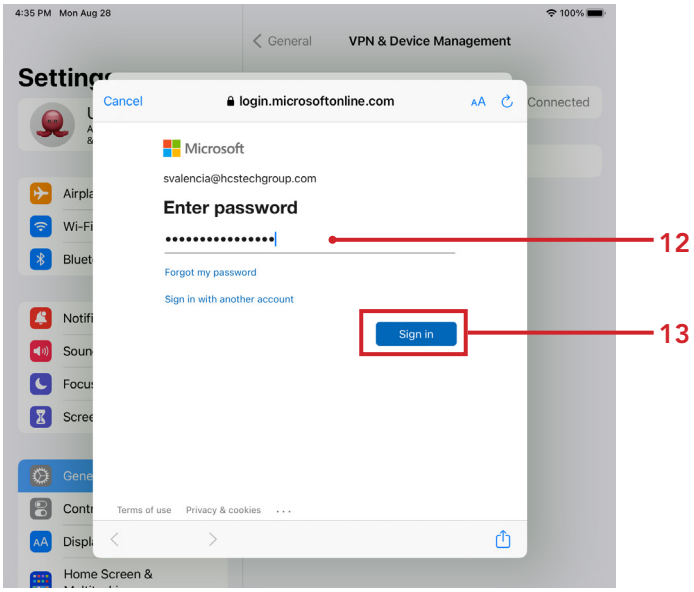
10. Tap Sign In to iCloud.



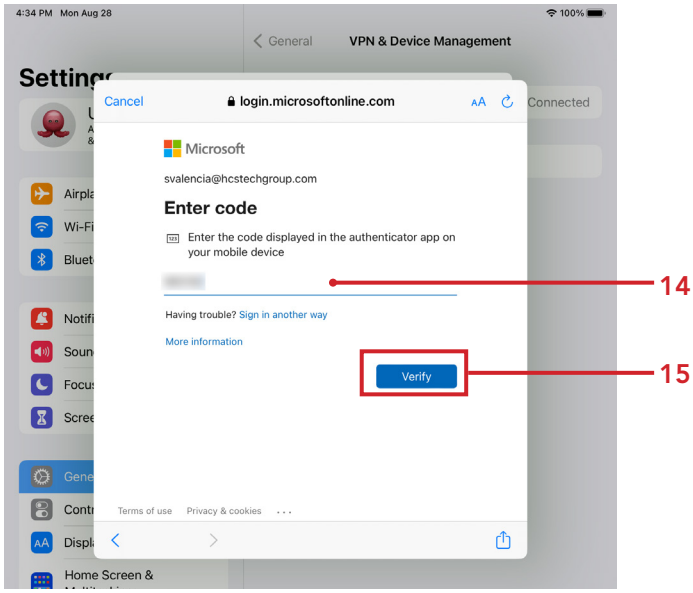
11. Tap Continue to proceed to Microsoft Online to enter federated credentials.
    NOTE: Alternatively, this can be a standard Managed Apple ID and password.



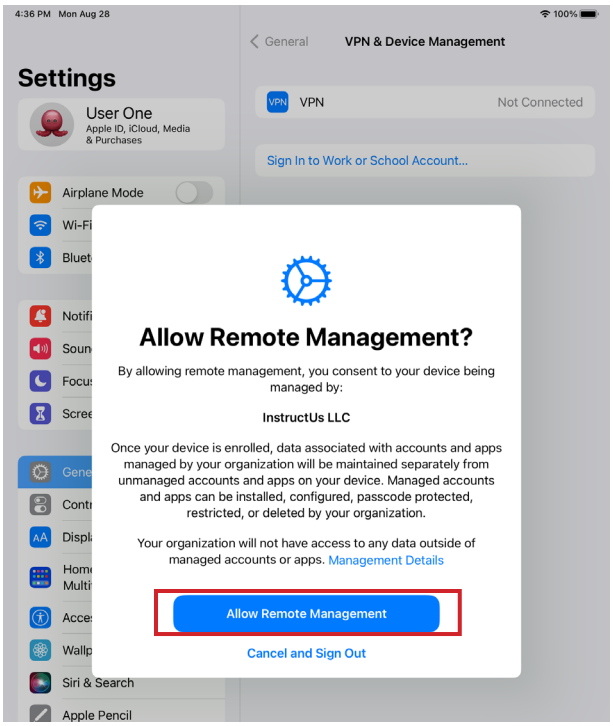
12. Enter your password.
13. Tap Sign in.



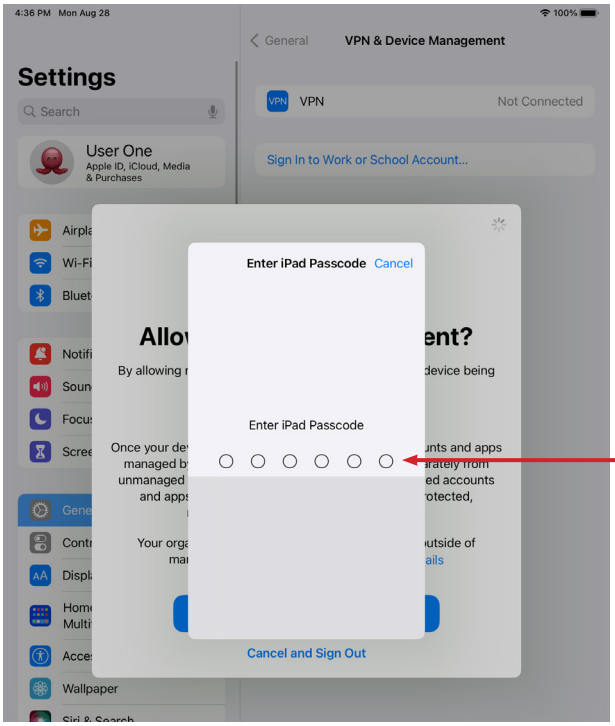
14. Enter the code displayed in the authenticator app on your mobile device.
15. Tap Verify.

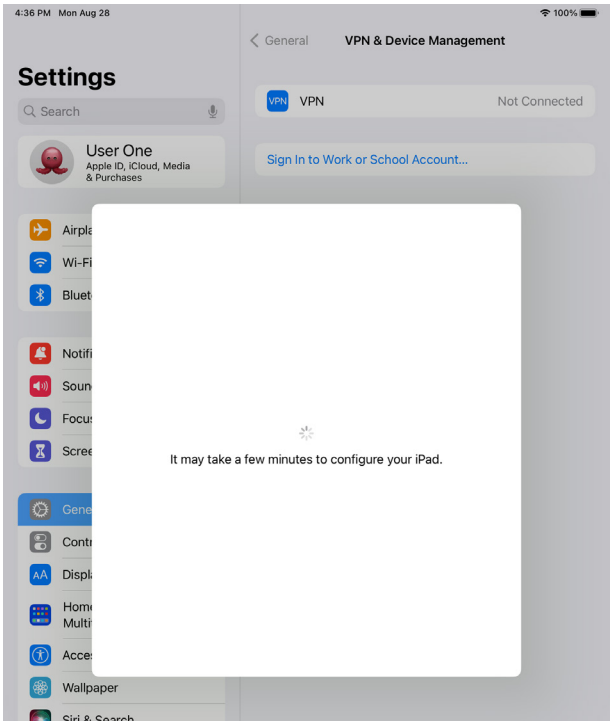


16. Tap Allow Remote Management.



17. Enter your device passcode.





19. The iCloud settings for your Managed Apple ID will appear.