iOS Devices - Intune

There is bookstack documentation for users

- iPhones Issued to Individuals
- iPhones Issued to Roles

- Onboarding iOS Devices into Intune
- Add Apps to Intune in Apple Business Manager
- Intune iOS Devices - FAQ
- Setup Better Impact iPad
- Setup Employment Hero iPad
- Setup Survey Legend iPad
- Migrating a User to a new iPhone from an existing iPhone (WIP)
- Renewing Apple Tokens in Intune

Onboarding iOS Devices into Intune

All new iOS devices (iPhones & iPads) at PBR are bring onboarded to Intune

Step 1 - Onboarding Device to Apple Business Manager

- If the device has been reimaged or is new and has not been enrolled by supplier, then start from **#**
- If the device has been enrolled by the phone supplier, you can skip to **

In order to onboard an iOS device into Apple Business Manager you must first install the Apple Configurator App on your personal phone. This phone must be also connected to Wi-Fi (PBR Corporate Wi-Fi doesn't work with this process) so needs to be connected to Internet Wi-Fi. iOS version of your personal phone and the new PBR phone need to be similar, but not necessarily exactly the same (it worked for me with my personal iPhone on 18.01 and PBR iPhone on 17.7)

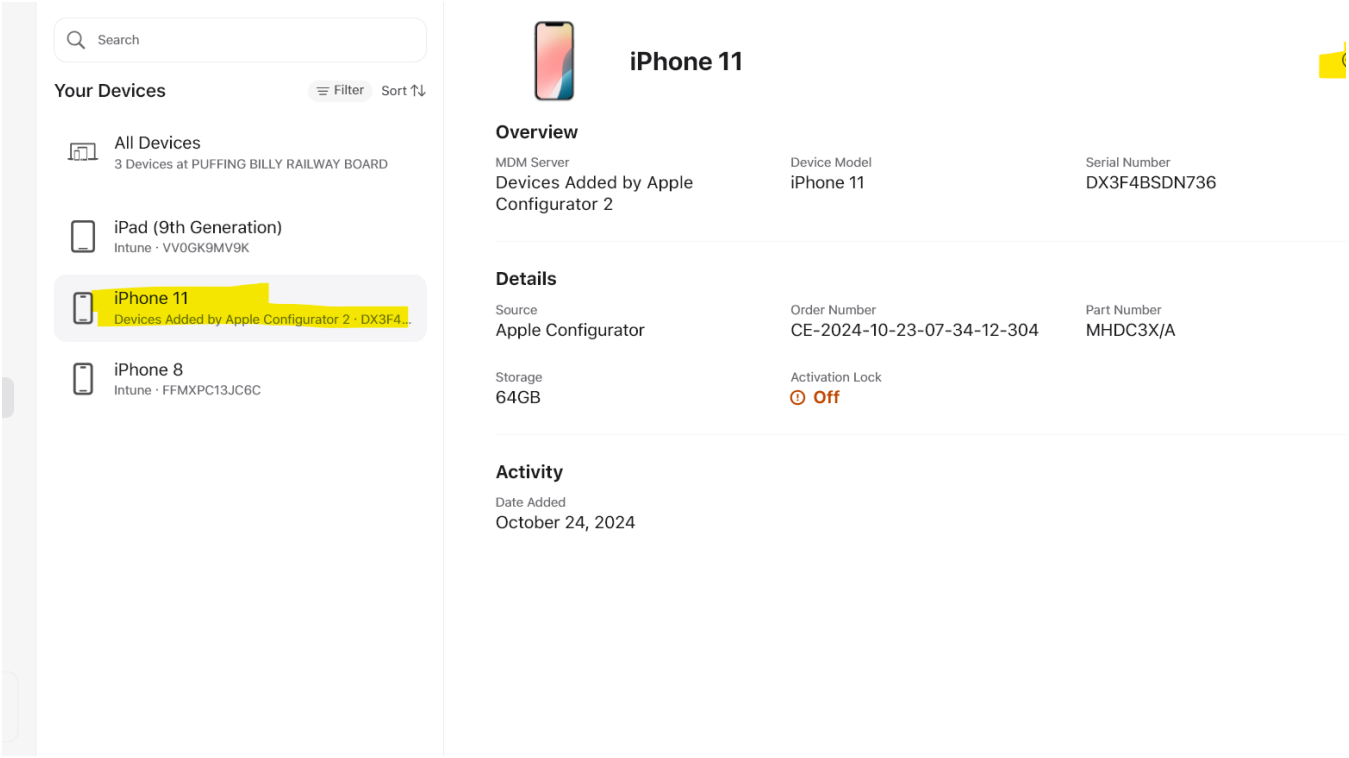
Apple Configurator App is available for the App Store, icon looks like 

 # If the device has been reimaged or is new and not enrolled by phone supplier then you can start here

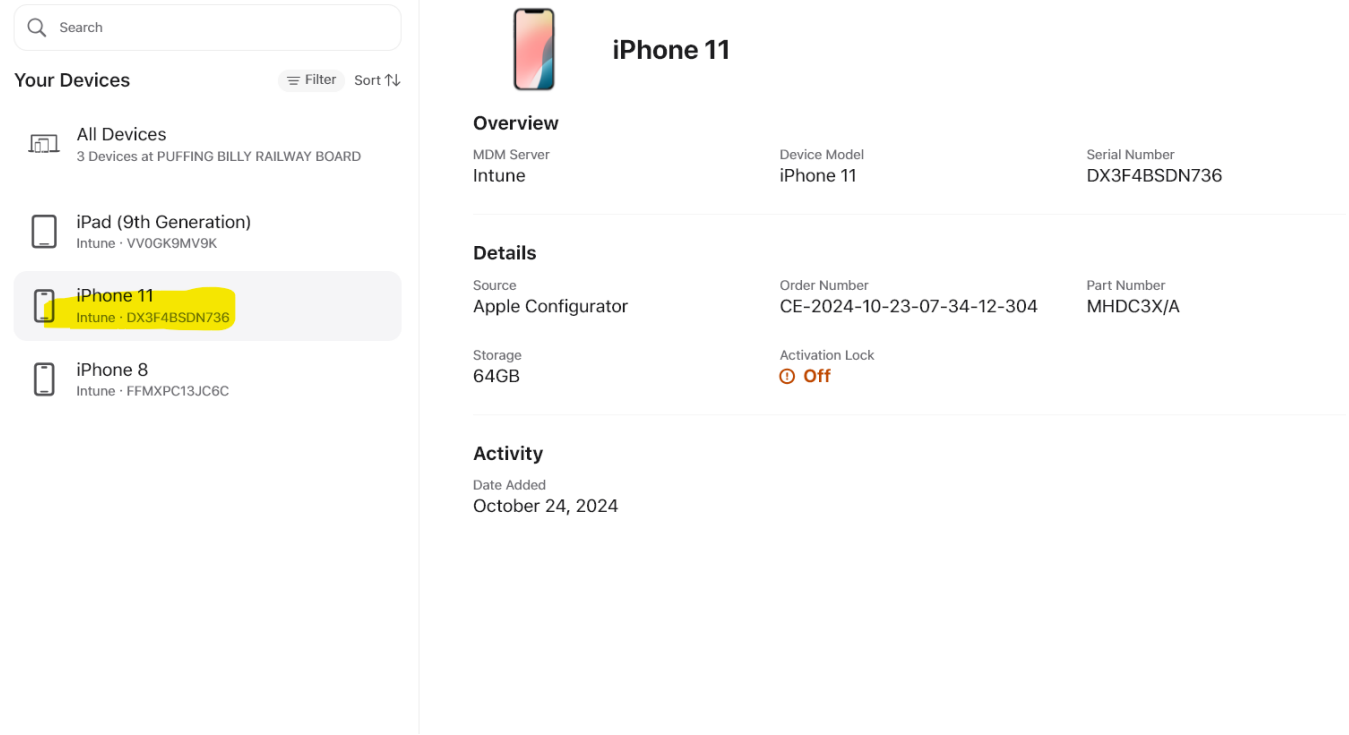
- Open Personal iPhone and log into Apple Configurator with PBR Apple Business Manager Username (apple@pbr.org.au) and Password (in 1Password) This MFA's via SMS to the IT Mobile,(messages can be accesses from the Who's On Call App). alternatively if you have a apple administrator account you can use that. Click on settings and ensure that 'Share Wi-Fi' is enabled
- If the phone has been used previously then it must first be erased, once erased or if new proceed with the guided setup until you get to the screen prompting to connect to a Wi-Fi network. (DO NOT CONNECT).
- On your personal phone scan the screen of the new PBR phone and a QR code will appear and then the new phone will go through the process to add to Apple Business Manager.
- Once complete log into Apple Business Manager https://business.apple.com with same creds as above. Navigate to Devices

****If the device has been enrolled by phone supplier then you can start here***

- Select the device you added (best done by serial number) you now need to assign the MDM server to the device, click on 3 dots top right, select edit MDM server and select Intune as the PBR MDM Server.



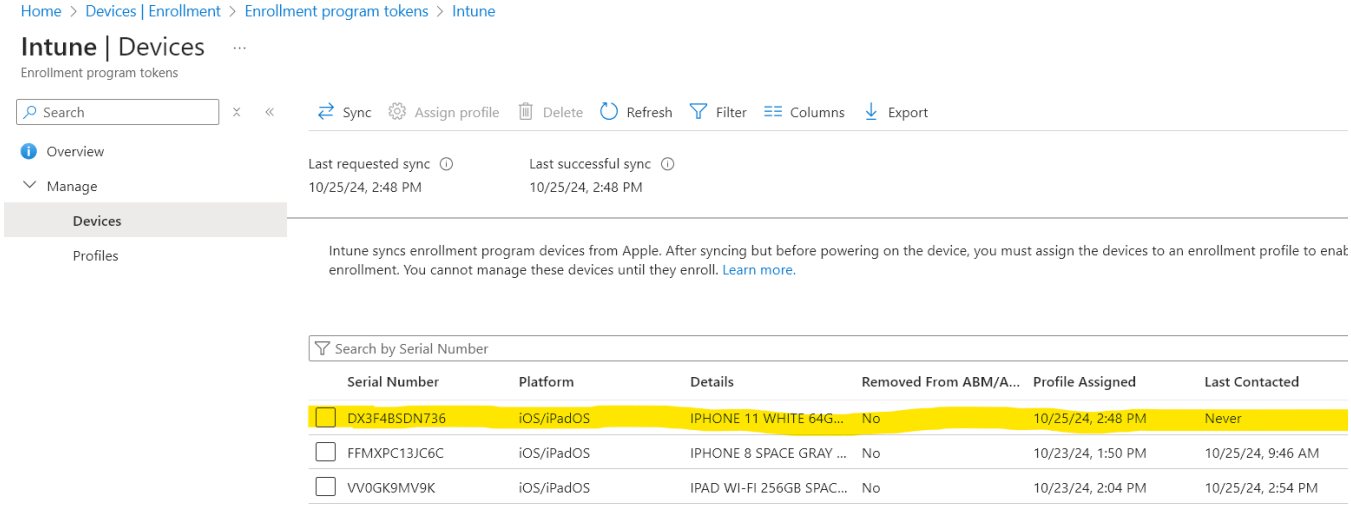
- Now the new device will be updated as per below



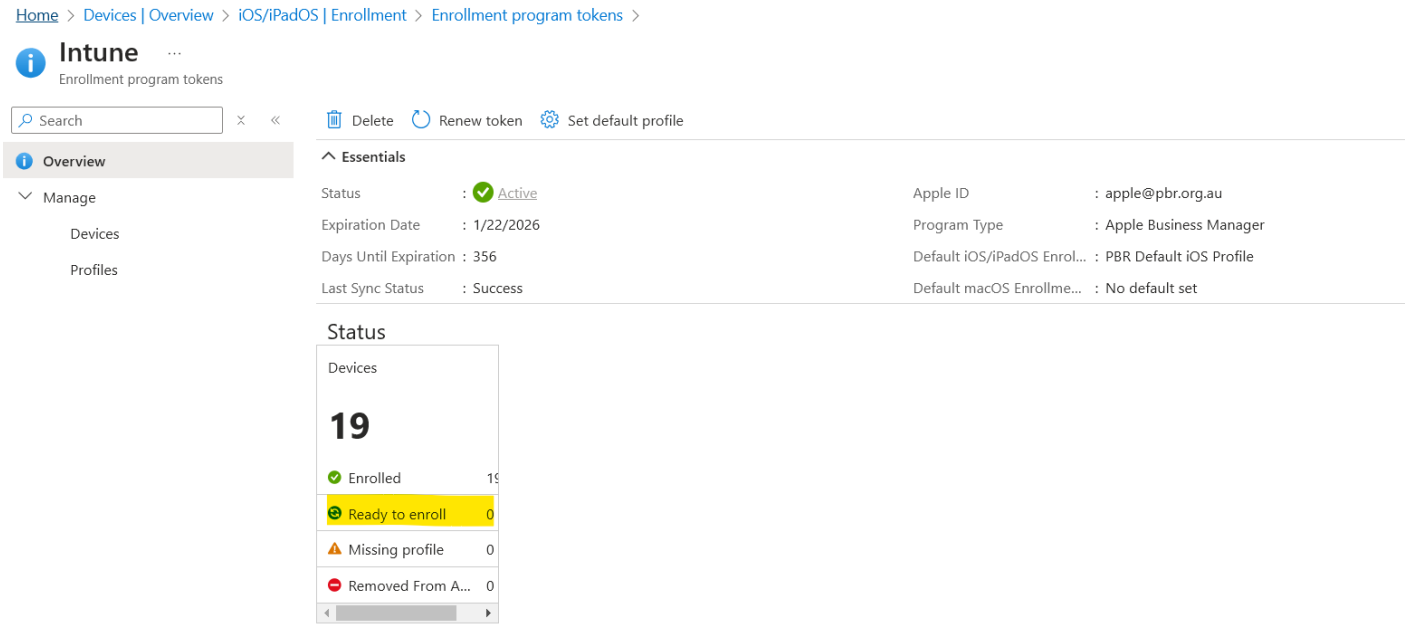
This is all that needs to be done in Apple Business Manager.

Step 2 - Onboarding Device to Intune

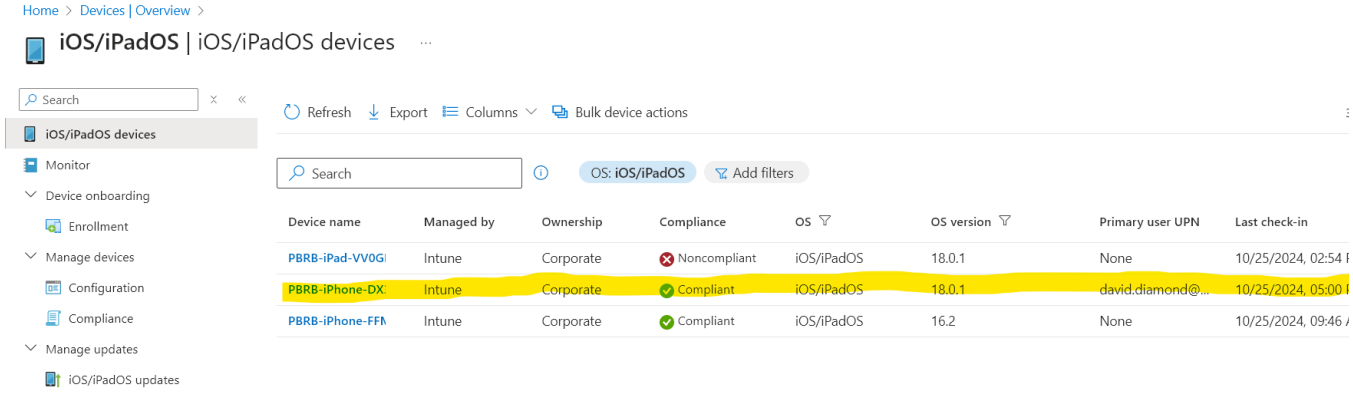
- Log into Intune, navigate to Devices | Enrolment | Apple tab | Enrolment Program Tokens | Select Intune Token | Devices. It can take some time to sync, if its not showing after a few minutes try a refresh and if still not showing try a sync (this will take 15 mins)



- Once the device is visible in Intune, you need to assign a profile. Select the device and click Assign Profile. Currently there are 3 profiles configured (See below for details of configuration for each profile) -
  - PBR Default iOS Profile - This is for staff that are being assigned a personal iPhone
  - PBR Shared iOS Profile - This is for role based iPhones & iPad's
  - PBR iPad Profile - This is for iPads running Survey Legend, Better Impact or Employment Hero
  - Fix Profile - Used for resolving issues with devices that are listed as never contacted - Refer Intune iOS Devices FAQ
- Select the required profile and ensure in Intune that click ensure that it has listed 1 ready to enroll before proceeding, if not try a refresh or sync



- Return to the iPhone you are onboarding and click Erase iPhone, the phone will then erase and restart
- Once restarted go through the setup prompts, language, country, appearance, quick start (select setup without another device), connect to wifi (choose internet), Remote Management, (choose enroll the iPhone), create a passcode (111111)
- Once you get to the home screen The device should now be visible in Intune Devices | iOS/iPadOS Devices. Its can take some time (like everything with Intune)



Step 3 - Configuring Device in Intune

- Once visible you need to assign the device (or user) to an AAD group, (this is where the majority of configuration gets applied) there are currently the following groups setup -
  - Intune_iOS_iPhones_Individual - User Group
  - Intune_iOS_iPhones_Role - Device Group
  - Intunue_iOS_iPads_BI - refer separate bookstack on setting up iPad for Better Impact
  - Intunue_iOS_iPads_SL - refer separate bookstack on setting up iPad for Survey Legend
  - Intunue_iOS_iPads_EH - refer separate bookstack on setting up iPad for Employment Hero
  - Intunue_iOS_Default_apps - User Group
  - Intune_iOS_Wifi

- For individually assigned devices ensure the user opens Company Portal App and sign in with PBR User Creds (not needed on iPad's or iPhones that are Role Based) Follow the prompts

Enrollment Profiles - These are assigned to devices as a part of the enrollment process above

- ***PBR Default iOS Profile -*** *This is for staff that are being assigned a personal iPhone*

    - Devices are enrolled with User Affinity
    - Company Portal is installed
    - Users can log into App store with own account and download apps
    - Setup Assistant has all options enabled
- ***PBR Shared iOS Profile -*** *This is for role based iPhones & iPad's*
    - Devices are enrolled ***without*** User Affinity
    - Setup Assistant is restricted to passcode
- ***PBR iPad Profile***
    - Devices are enrolled without User Affinity
    - Setup Assistant doesn't prompt for passcode

AAD Groups and resultant configurations - These are assigned by adding device (or user) to the AAD group)

- ***Intune_iOS_iPhones_Individual*** - Devices in this group are configured to -
    - Apps are deployed based on user (see below Intune_iOS_Default Apps)
    - iOS Update Policy Applied - Set to Latest update and update at next check-in
    - Restricted Apps List Policy Applied (Uninstalls TikTok)
    - PBR Wi-Fi Policy - connects device to 'internet' Wi-Fi automatically

- ***Intune_iOS_iPhones_Role*** - Devices in this group are configured to -
    - Get the following Apps automatically deployed
        - BOM
        - Vic Emergency
    - iOS Update Policy Applied - Set to Latest update and update at next check-in
    - Restricted Apps List Policy Applied (Uninstalls TikTok)
    - PBR Wi-Fi Policy - connects device to 'internet' Wi-Fi automatically
    - iPhone_Role_Based_Policy
        - Block App Store
        - Disable Face ID & Touch ID
        - Hide the following built in Apps -
            - iOS Native Mail App
            - Health App
            - Apple TV App
            - Podcasts App
            - Wallet App
            - Weather App
            - Home App
            - Books App
            - iTunes store App
            - Fitness App
            - Watch App
                - Freeform App
            - Journal App

        - GarageBand App
        - Apple Music App
        - Apple News App
        - Find My iPhone App
        - Shortcuts App
        - Tips App

- ***Intune_iPads_EH -*** *WIP*
    - Clock Me In Time & Attendance app is installed
    - Employment Hero Policy
        - Opens Clock Me In Time & Attendance app in Kiosk mode
        - Block autolock
        - Block screen sleep
        - Disable Face ID & Touch ID
        - Block passcode modification

- ***Intune_iPads_BI***
    - Better Impact Kiosk Policy
    - Better Impact URL Policy

- ***Intune_ipads_forms***
    - ***Microsoft Forms Kiosk Policy***
    - ***Microsoft Forms URL Policy***

- ***Intune_iPads_SL***
    - Survey Legend Kiosk Policy

- **Intune_iOS-Wifi**
    - PBR Wi-Fi Policy - connects device to 'internet' Wi-Fi automatically

- ***Intune_iOS_Default Apps*** - Members of this group get assigned the following Apps -
    - Required Apps - installed automatically on the device once the user signs into Company Portal
        - Outlook
        - OneDrive
        - BOM
        - Duo
    - Optional Apps - are available for download and installation by user from within Company Portal
        - Word
        - Excel
        - Teams
        - Employment Hero Work

- ***Intune_iOS_Finance_Apps***

    - Required Apps - installed automatically on the device once the user signs into Company Portal
    - Optional Apps - are available for download and installation by user from within Company Portal
        - CommBiz

Make a group for wifi policy and add individual devices to it

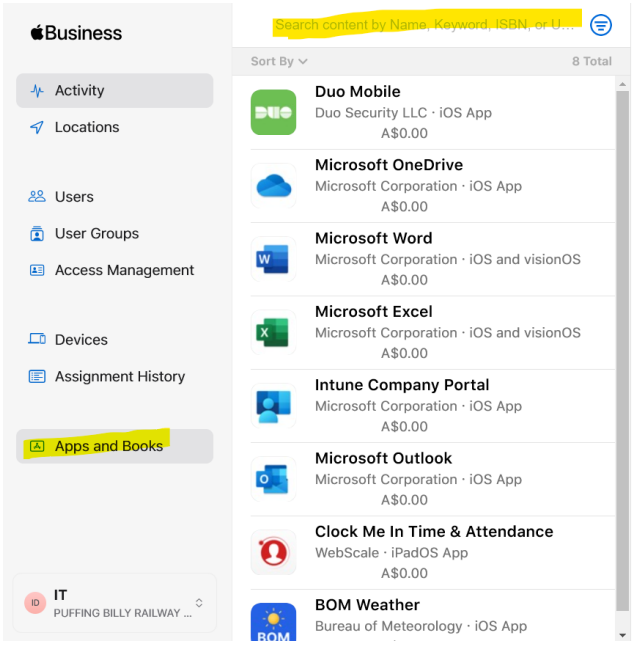
- Assigned Apps will be installed on the iPhone (apps are specified in Intune, Apps | iOS Apps)
  Select device and you can manage the device

Wifi policy is attached to a seperate AAD group, to avoid issues with devices in Kiosk mode losing network connectivity when changing policy's.. thiis way a device cabn be removed from its Kiosk Mode group, whislt enabling it to stay connected. I have expereinced issue where you can get locked out of a device if in kiosk mode that gets disconnected from wifi

Add Apps to Intune in Apple Business Manager

Log into Apple Business Manager at apple@pbr.org.au

Navigate to Apps & Books

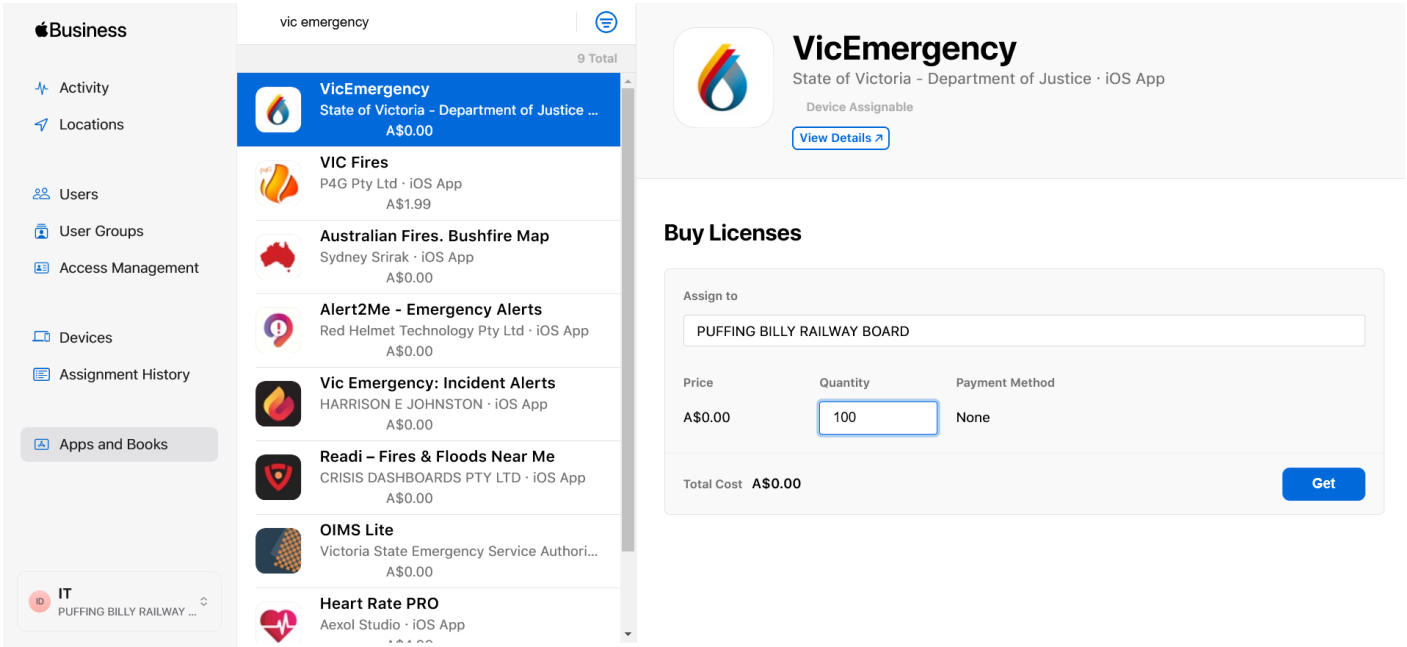




8 Apps · 0 Books

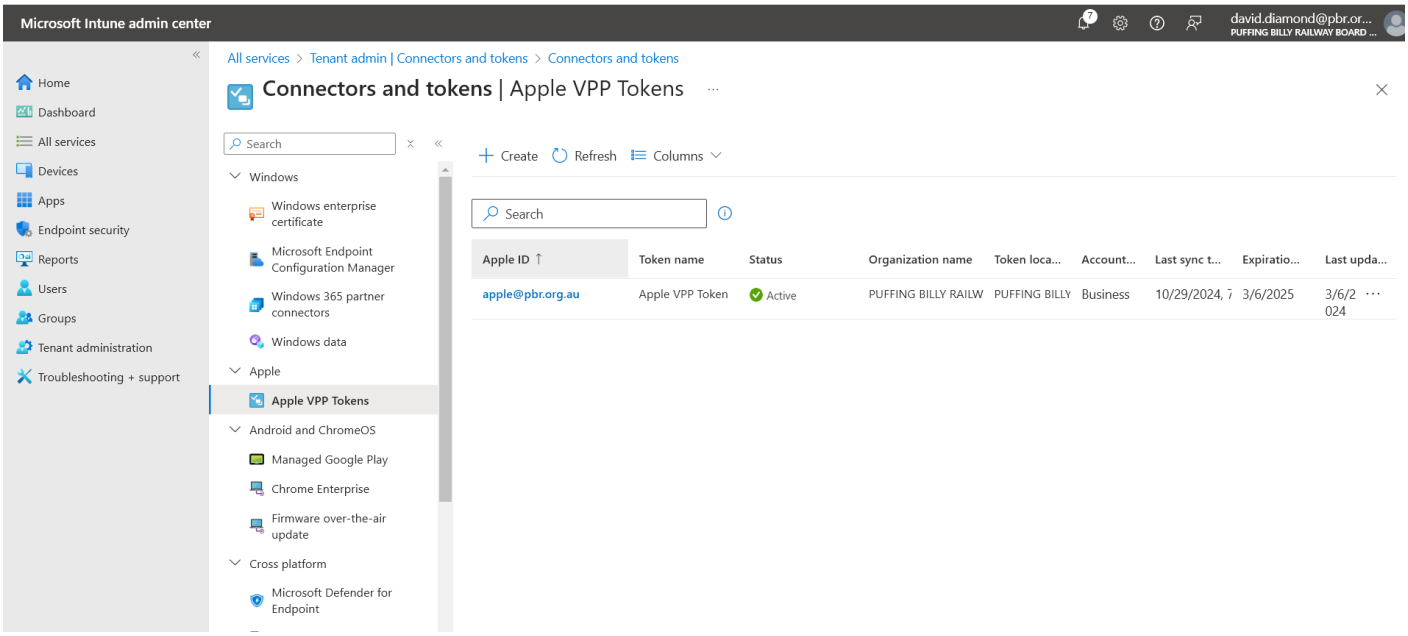
PUFFING BILLY RAILWAY BOARD

In search bar at the top search for the app you want to add

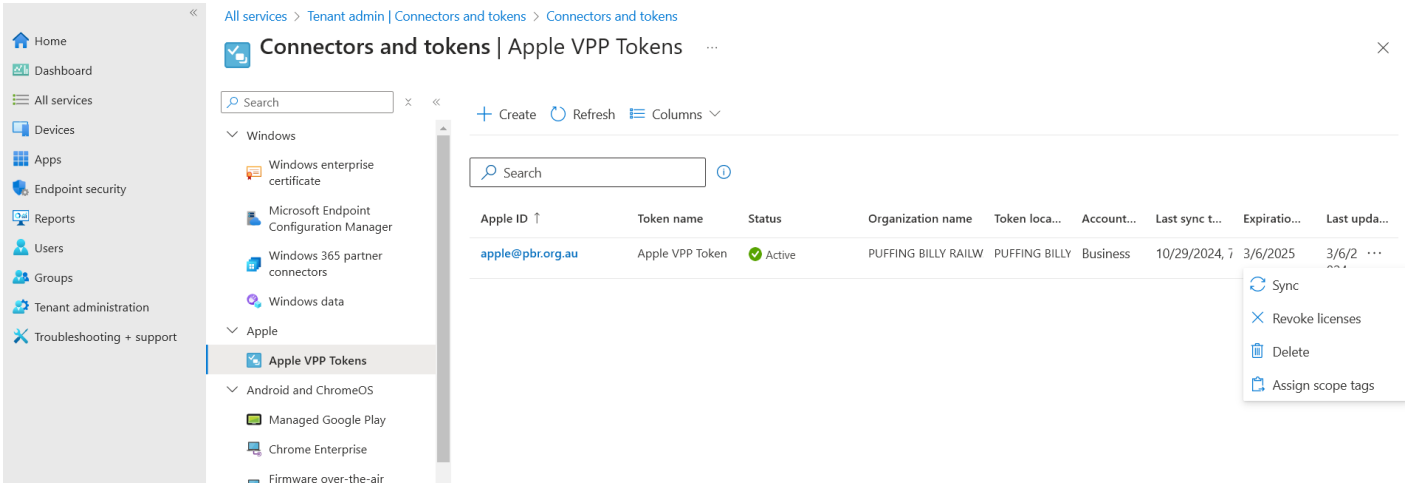


select the app, assign to Puffing Billy Railway Board and enter quantity and click Get

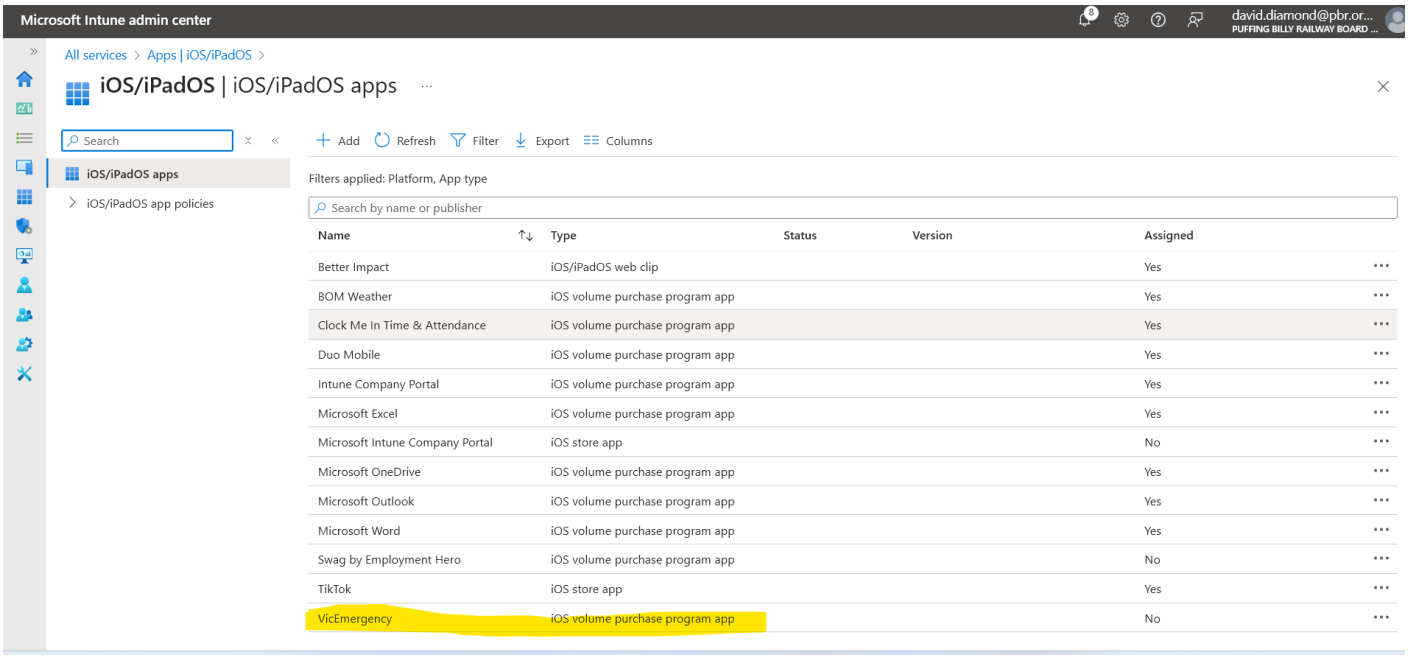
Now go to Intune Tenant Admin | Connectors and Tokens



On the line of apple@pbr.org.au go to far right and click on ... and select Sync



Once sync has completed navigate to Apps | iOS/iPadOS apps, and the app will be displayed in the list and is now successfully added to Intune


Microsoft Intune admin center
david.diamond@pbr.or...
PUFFING BILLY RAILWAY BOARD ...
All services > Apps | iOS/iPadOS >
iOS/iPadOS | iOS/iPadOS apps
Search
iOS/iPadOS apps
iOS/iPadOS app policies
Add
Refresh
Filter
Export
Columns
Filters applied: Platform, App type
Search by name or publisher
Name
Type
Status
Version
Assigned
Better Impact iOS/iPadOS web clip Yes
BOM Weather iOS volume purchase program app Yes
Clock Me In Time & Attendance iOS volume purchase program app Yes
Duo Mobile iOS volume purchase program app Yes
Intune Company Portal iOS volume purchase program app Yes
Microsoft Excel iOS volume purchase program app Yes
Microsoft Intune Company Portal iOS store app No
Microsoft OneDrive iOS volume purchase program app Yes
Microsoft Outlook iOS volume purchase program app Yes
Microsoft Word iOS volume purchase program app Yes
Swag by Employment Hero iOS volume purchase program app No
TikTok iOS store app Yes
VicEmergency iOS volume purchase program app No

Intune iOS Devices - FAQ

What to do if a device that is in Kiosk mode is unable to connect to the internet.

There is a PBR Wi-Fi Policy enabled in Intune that enables automatic connection to PBR Wi-Fi (Internet). If for some reason this Wi-Fi becomes unavailable whilst the device is in Kiosk mode then it is not possible to take the device out of Kiosk mode due to the fact the device needs to be connected to the internet to enable changes made in Intune to sync to the device.

A simple solution is to setup a hotspot from another phone, make the SSID internet and specify the same password as for the PBR internet Wi-Fi .. then the device should be able to connect and changes in Intune can then be sync'd to the device

What to do if a device is successfully in Apple Business Manager and listed in Intune under Devices | Enrolment | Apple tab | Enrolment Program Tokens | Select Intune Token | Devices but event though it has a profile assigned when you erase and restart the device it doesn't enroll in Intune

Set up a new enrollment profile and set it as the default profile and assigned the iPad to it, synced the token, reset the iPad again and this time it booted up with the Intune OBE and enrolled into Intune. Then I reassigned it to the proper enrollment profile and wiped it via the Intune console. It rebooted and came back up with all of my custom configuration settings. Didn't even have to go through OBE this time. Beautiful!

You can tell if its on the Fix iPad profile by looking at the device name locxally on the device.. if its iPhone-Serialnumber then its on the fix profile if its PBRB-iPhone-SerialNumber its on another profile

Kiosk Policy Notes

Always remove Kiosk policy before making changes to or adding or removing Wi-Fi policy

If you brick the iPad whilst in kiosk mode

Undertake a hard reset and restore - install iTunes on a windows device connect the iPad via cable to the computer, hold down the power and home button, keep holding once apple logo appears, wait for recovery screen. Then follow the prompts within iTunes.

Setup Better Impact iPad

Onboard the iPad into Intune by following this article https://bookstack.pbr.org.au/books/ios-devices-intune/page/onboarding-ios-devices-into-intune

Add the iPad to the following enrollment profile

- ***PBR iPad Profile*** - This is for iPads running Survey Legend, Better Impact or Employment Hero

Once you get to the home screen, the following settings need to be set manually -

- Enable the Favorites bar/Bookmarks Bar
  - Go to Settings > Apps > Safari
  - Turn on Show Favorites Bar
- Allow Camera Access for Safari
  - Go to Settings > Apps > Safari > Camera > Allow Access
- Set brightness to max
  - Go to Settings > Display & Brightness

Next step is to add the iPad to the ***Intune_iOS_Wifi*** Group. Its important to do this and ensure it is working before putting into Kiosk mode, as you can lock yourself out of the iPad. The best way to check the WiFi policy has been applied is go to Settings, Wi-Fi click on the connected wifi network 'internet' and see if the option to 'Forget This Network' is available . If this option is not available then the policy is applied. I have finding doing a remote restart can speed up this process

If you set a passcode earlier in the setup process, now you need to remove it, Intune | Devices | select the device and click 'remove passcode'

Now you need to assign the device to the ***Intune_iPads_BI*** AAD group. This will enable Kiosk Mode and create the bookmarks for Safari

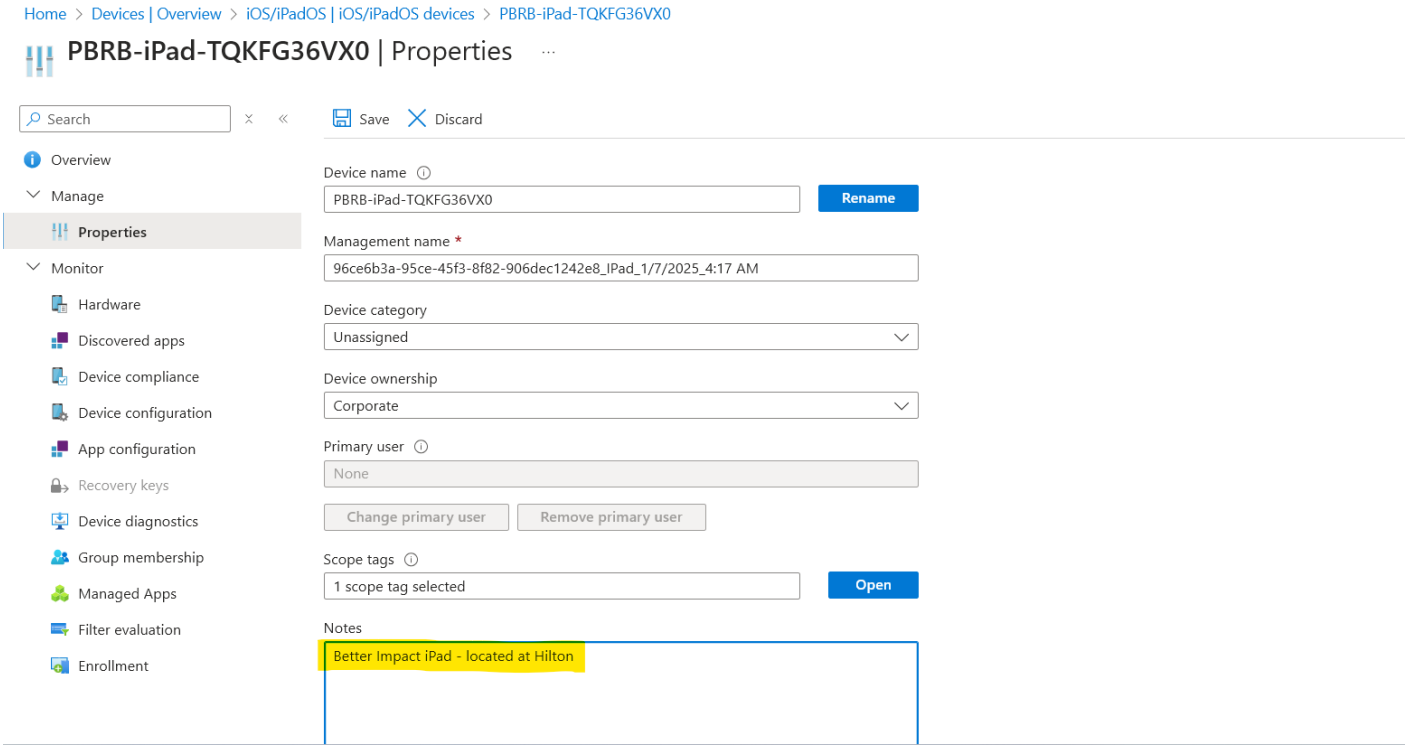
Once iPad is in Kiosk Mode, you just need to open the Better Impact bookmark within Safari and ensure its the only tab open

Make sure to update snipeit with the new hostname that has been assigned by Intune, it will be in the format of PBRB-iPad-<serial number>

and update the details of what the iPad is being used for and where it is located in Intune

Devices | Overview> iOS/iPadOS | iOS/iPadOS devices>

select the device and go to properties and enter details in the Notes section



Summary Of Applied Profiles & Policies for Better Impact iPads

Enrollment Profile

- PBR iPad Profile

Compliancy Policy applied

- iPad Compliance Policy

Configuration Policies applied

- Restricted Apps List
- Better Impact Kiosk Mode
- Better Impact URL
- PBR WiFi - internet
- iOS Updates

Manual Configuration

- Remove Passcode
- Show Safari Bookmarks Bar

Setup Employment Hero iPad

Onboard the iPad into Intune by following this article https://bookstack.pbr.org.au/books/ios-devices-intune/page/onboarding-ios-devices-into-intune

Add the iPad to the following enrollment profile

- ***PBR iPad Profile*** - This is for iPads running Survey Legend, Better Impact or Employment Hero

Once you get to the home screen, the following settings need to be set manually -

- Set brightness to max
  - Go to Settings > Display & Brightness
- You may also have to allow the camera for the employment hero app.

Next step is to add the iPad to the ***Intune_iOS_Wifi*** Group. Its important to do this and ensure it is working before putting into Kiosk mode, as you can lock yourself out of the iPad. The best way to check the WiFi policy has been applied is go to Settings, Wi-Fi click on the connected wifi network 'internet' and see if the option to 'Forget This Network' is available . If this option is not available then the policy is applied.

Now you need to remove the passcode set earlier, Intune | Devices | select the device and click 'remove passcode'

Now you need to assign the device to the ***Intune_iPads_EH*** AAD group. This will enable Kiosk Mode

Once iPad is in Kiosk Mode, you just need to logon to Employment Hero

Summary Of Applied Profiles & Policies for Employment Hero iPads

Enrollment Profile

- PBR iPad Profile

Compliancy Policy applied

- iPad Compliance Policy

Apps Assigned

- Clock Me In Time & Attendance

Configuration Policies applied

- Restricted Apps List
- Employment Hero
- PBR WiFi - internet
- iOS Updates

Manual Configuration

- Log into employment hero app

Setup Survey Legend iPad

Onboard the iPad into Intune by following this article https://bookstack.pbr.org.au/books/ios-devices-intune/page/onboarding-ios-devices-into-intune

Add the iPad to the following enrollment profile

- ***PBR iPad Profile*** - This is for iPads running Survey Legend, Better Impact or Employment Hero

- Add the iPad to the ***Intune_iOS_Wifi*** Group. Its important to do this and ensure it is working before putting into Kiosk mode, as you can lock yourself out of the iPad. The best way to check the WiFi policy has been applied is go to Settings, Wi-Fi click on the connected wifi network 'internet' and see if the option to 'Forget This Network' is available . If this option is not available then the policy is applied.

- Set display brightness to max

Now you need to remove the passcode set earlier, Intune | Devices | select the device and click 'remove passcode'

Now you need to assign the device to the ***Intune_iPads_SL*** AAD group. This will enable Kiosk Mode and create the bookmarks for Safari

Once iPad is in Kiosk Mode, you just need to configure Kiosk Pro Lite to - (this can all be done from app when in full kiosk mode)

  - open Survey Legend Site - https://s.surveylegend.com/-N4AITZs17ndh7Om04dX
  - open webpage when apps starts, set to be on touch gesture & passcode (setup same passcode for all Survey Legend iPads) in 1Password
  - hide address bar
  - hide navigation bar
  - set idle Time limit to 0 seconds

Summary Of Applied Profiles & Policies for Survey Legend iPads

Enrollment Profile

- PBR iPad Profile

Compliancy Policy applied

- iPad Compliance Policy

Apps Assigned

- Kiosk Pro - Lite (free version)\

Configuration Policies applied

- Restricted Apps List
- Survey Legend Kiosk Mode
- PBR WiFi - internet
- iOS Updates

Manual Configuration

- Remove Passcode
- Set display brightness to max
- Configure Kiosk Pro Lite to - this can all be done from app when in full kiosk mode
  - Set homepage - https://s.surveylegend.com/-N4AITZs17ndh7Om04dX
  - Change show settings to 'on touch gesture & passcode'
  - Set passcode (use creds in 1 password for all iPads using Kiosk Pro Lite)
  - hide address bar
  - hide navigation bar
  - set idle Time limit to 0 seconds

Migrating a User to a new iPhone from an existing iPhone (WIP)

Migrating a user with an existing PBR issued iPhone to a new PBR issued iPhone that is MDM enrolled

Step 1 - Backup Device

Use Apple Devices App from Microsoft Store to backup existing iPhone

Step 2 - Restore Backup on new Device

Device must be enrolled in Apple business manage and intune

- If using a ***new phone***, this can be done by turning on the new iPhone when it prompts for language plug in USB cable connected to PC, make sure you have Apple Devices App open. Then you will have the option to restore
- If enrolling an ***existing device***, erase the phone, when it restarts and prompts for language plug in USB cable connected to PC, make sure you have Apple Devices App open. Then you will have the option to restore

When restore is complete the iPhone will restart. remove the cable from the computer when apple logo is displayed

Step 3 - Enrollment Process

- When phone restarts should come up with restore complete
- Connect to 'internet' Wi-Fi
- Enroll this iPhone

- Setup face id
- Create a passcode
- Sign in to users apple account
- Accept terms and conditions
- Turn on location services

Everything should come across, photo's contacts, settings, apps etc.

Notes:

- Backups done via Apple Devices App are found stored on your local PC in C:\Users\User name\Apple\MobileSync\Backup\

Renewing Apple Tokens in Intune

There are 3 Apple Tokens that need to be renewed in Intune

Refer https://c7solutions.com/2024/01/renewing-apple-tokens-in-intune for instructions

Apple MDM Push Certificate

This certificate expires ever 365 days and must be renewed prior, otherwise all iOS devices will need to be reenrolled.
there's lots of documentation out there about how to do this, such as the below, the main things to remember is to log into Apple Push Certificates Portal with apple@pbr.org.au and to renew the existing certificate, rather than creating a new one

https://www.recastsoftware.com/resources/renewing-your-apple-mdm-certificate-for-intune/

https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

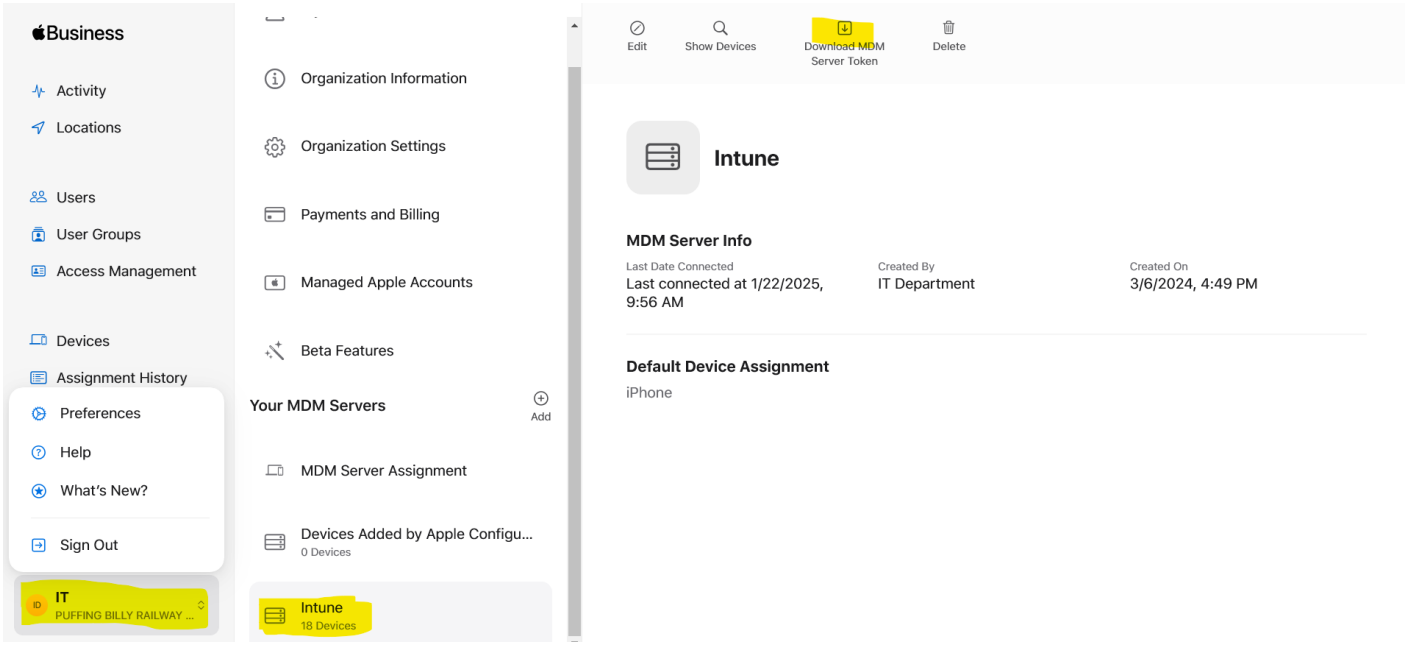
Apple Business Manager Enrolment Program Token (DEP)

This token expires ever 365 days and must be renewed prior

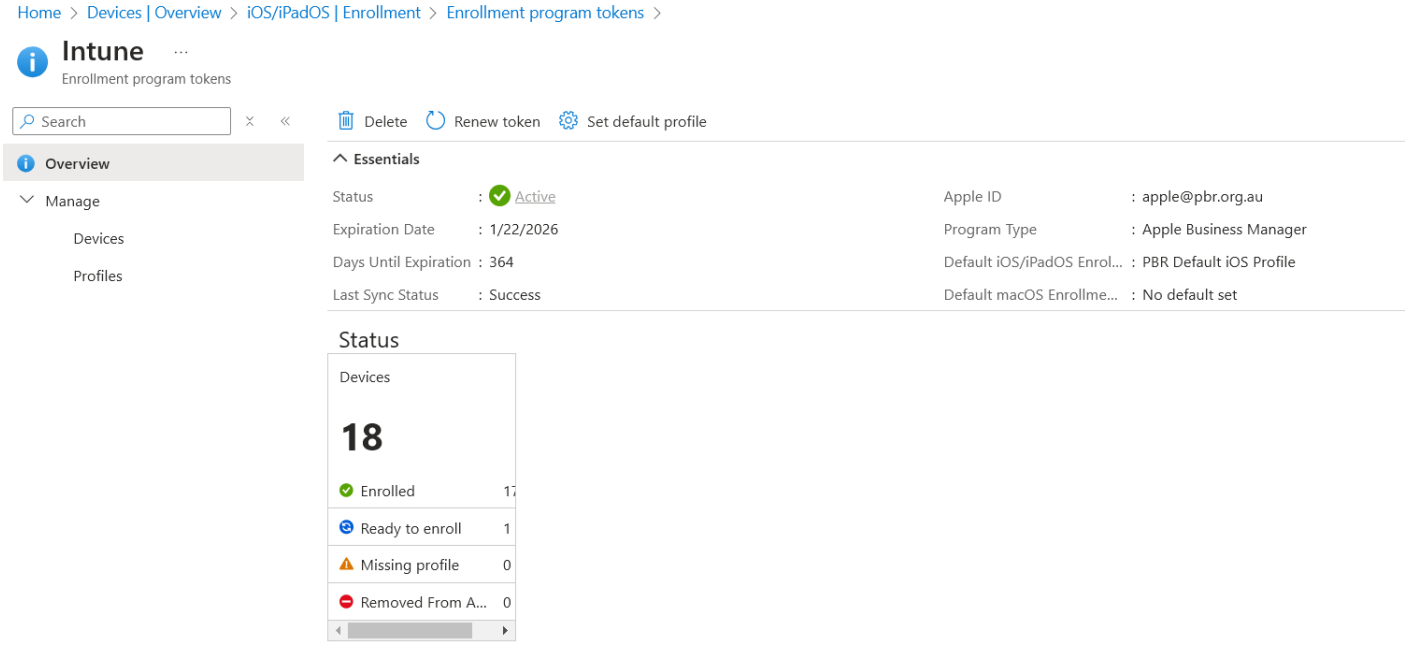
In Apple Business Manager, on the LHS click on IT - Puffing Billy Railway and select Preferences

Scroll to the bottom and Select Intune under Your MDM Servers

Then select Download MDM Server Token



In Intune navigate to Devices | Overview > iOS/iPadOS | Enrollment > Enrollment Program Tokens



Click on Renew Token

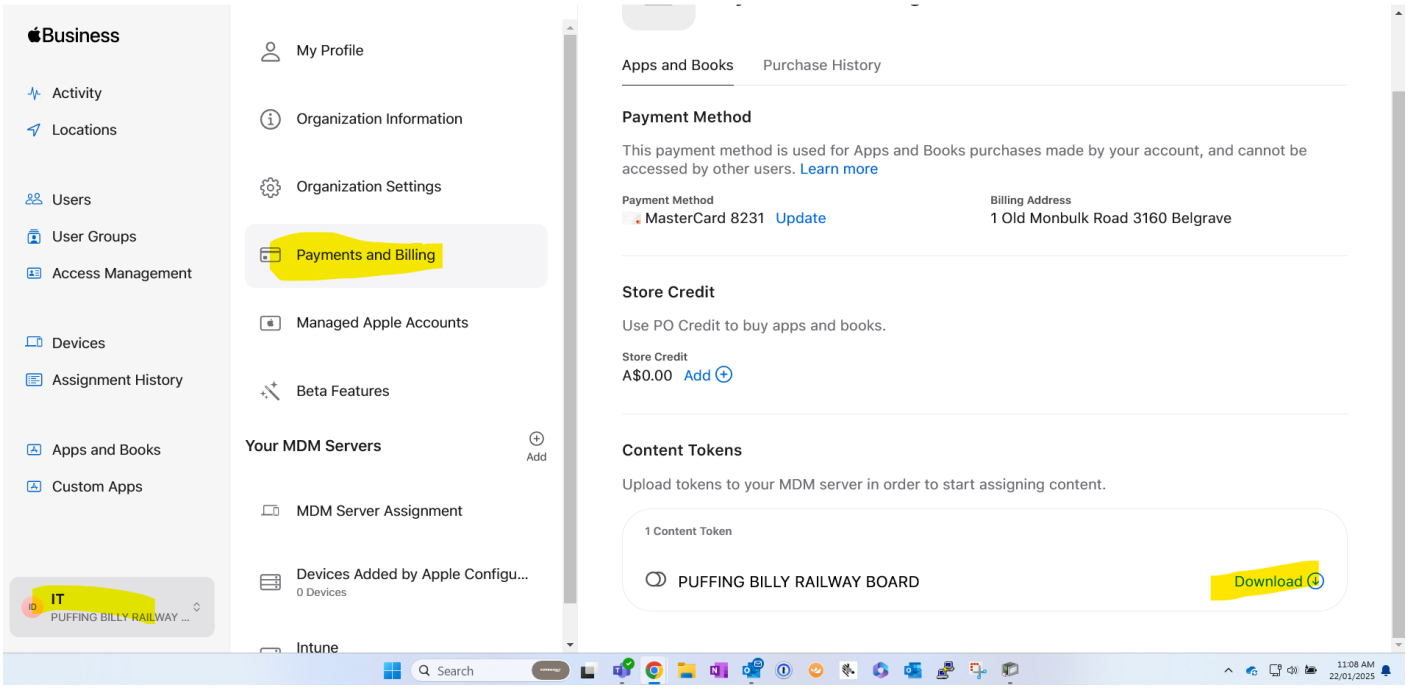
Apple ID apple@pbr.org.au

Select the token you downloaded from Apple Business Manager

The expiry date should now updated and the token renewed

Apple VPP Token

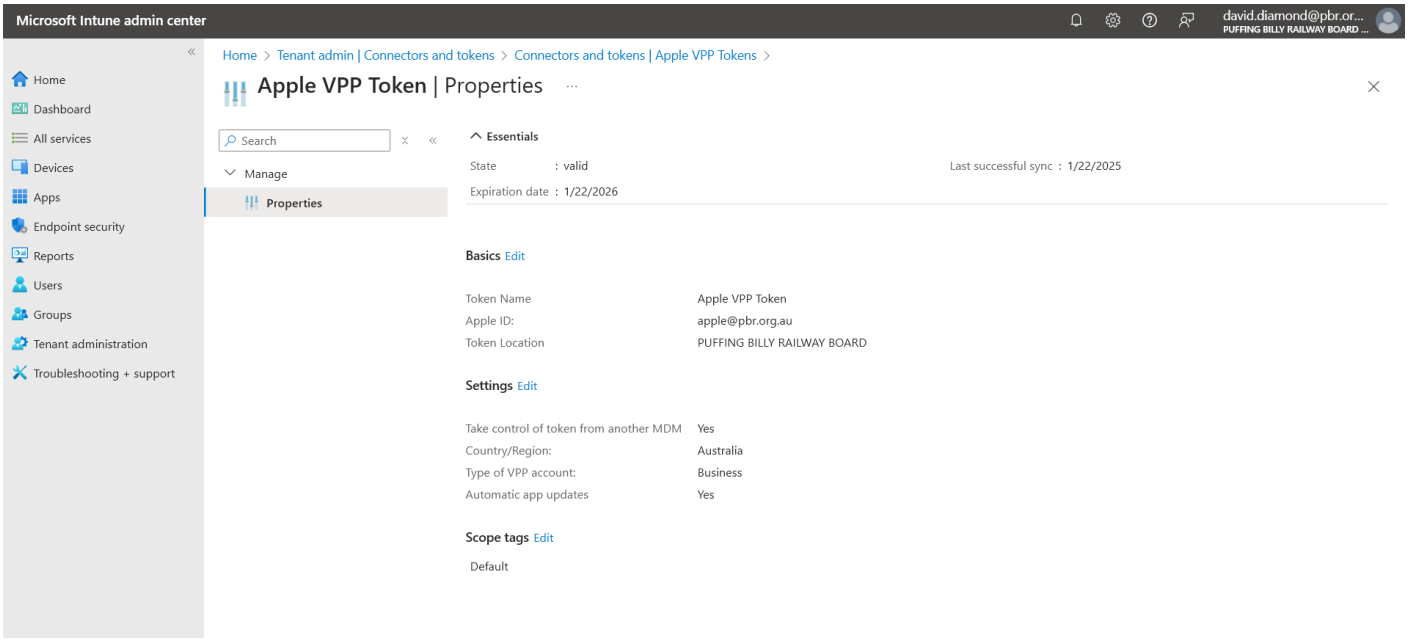
There is a recurring ticket in helpdesk for this to be done
In Apple Business Manager, download content token



in Intune

Tenant Administration > Connectors and Tokens > Apple VPP Tokens

select the token, and click edit next to basics



Browse to the token file you downloaded

