

How to setup IOS and ANDROID device enrollment within Intune

In this post, I am going to share the steps to complete IOS and Android device setup/enrollment within Intune.

APPLE DEVICES (iPhone, iPad & MacBook Pro)

The pre-requisites for IOS are as follows:

- ✚ Your device must be running iOS 13.0 and later.
- ✚ You must Install Company Portal app from App Store.
- ✚ To log in to the company portal, you'll need a user account with Intune license.
- ✚ Maintain a Wi-Fi connection until all steps are complete.
- ✚ Have access to Safari web browser on your device.

Basic steps

- Check the prerequisites and ensure you are using supported iOS devices for enrollment.
- Apple MDM Push certificate configuration – Involves downloading Intune certificate signing request and creating a new push certificate. Later upload this push certificate in Intune portal.
- Install Company Portal app on iOS device from App Store and authenticate.
- Set up iOS/iPad OS Device Access to your company resources.
- Manage iOS devices from Intune Portal.

MDM PUSH CERTIFICATE:

Login to Intune portal -> Devices -> Enroll Devices -> Apple Enrollment -> Apple MDM Push Certificate

Home > Devices | Enroll devices > Enroll devices

Enroll devices | Apple enrollment

Search

- Windows enrollment
- Apple enrollment**
- Android enrollment
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- Corporate device identifiers
- Device enrollment managers

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. [Learn more.](#)

Prerequisites

Apple MDM Push certificate
Certificate required to manage Apple devices

Bulk enrollment methods

- Apple Configurator**
Manage Apple Configurator enrollment
- Enrollment program tokens**
Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

Enrollment options

- Enrollment notifications (preview)**
Send email or push notifications to devices after they enroll.
- Enrollment types (preview)**
Manage User Enrollment and Device Enrollment options

Select I agree and Download CSR (Certificate signing request)

Configure MDM Push Certificate

Delete

Essentials

| | |
|---------------|-----------------------|
| Status | Days until expiration |
| Not set up | Not available |
| Last updated | Expiration |
| Not available | Not available |
| Apple ID | Subject ID |
| Not set up | Not set up |
| Serial number | |
| Not set up | |

You need an Apple MDM push certificate to manage Apple devices with Intune.

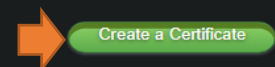
Steps:

- I grant Microsoft permission to send both user and device information to Apple. [More information on Microsoft permission.](#)
☒ I agree. *
- Download the Intune certificate signing request required to create an Apple MDM push certificate.
[Download your CSR](#)

Now we will create Apple MDM push certificate. Sign in with your appleid and create a certificate

- Create an Apple MDM push certificate. [More information on Apple MDM push certificate.](#)
[Create your MDM push Certificate](#)

Certificates for Third-Party Servers



Terms of Use

PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.

MDM Certificate Agreement (for companies deploying mobile device management for iOS and/or OS X products)

Purpose

Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile device management for iOS and/or OS X products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.

1. Accepting this Agreement; Definitions

1.1 Acceptance

In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational institution's, or agency's, instrumentality, or department of the federal government's behalf, as its authorized legal

☒ I have read and agree to these terms and conditions.

[Printable Version >](#)

Decline

Accept

Select IntuneCSR file to upload

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

IntuneCSR.csr

Now download the certificate to complete final steps at Intune portal

Confirmation

You have successfully created a new push certificate with the following information:


| | |
|-----------------|--------------------------|
| Service | Mobile Device Management |
| Vendor | Microsoft Corporation |
| Expiration Date | Dec 28, 2023 |

Certificates for Third-Party Servers

| Service | Vendor | Expiration Date* | Status | Actions |
|--------------------------|-----------------------|------------------|--------|--------------------------------------------------------------------------------------------------------------------|
| Mobile Device Management | Microsoft Corporation | Dec 28, 2023 | Active | <input type="button" value="Renew"/> <input type="button" value="Download"/> <input type="button" value="Revoke"/> |


4. Enter the Apple ID used to create your Apple MDM push certificate.






Apple ID *


ramlan@rogers.com 

5. Browse to your Apple MDM push certificate to upload

Apple MDM push certificate *


"MDM_Microsoft Corporation_Certificate.pem" 

administrator@ramlan.ca
RAMLAN INC (RAMLAN.CA) 

Notifications

More events in the activity log →

 **Uploading your MDM push certificate**

Your MDM push certificate was successfully created.

Now we have other options available within Apple Enrollment. Let's complete Enrollment Options.

Home > Devices | Enroll devices > Enroll devices

Enroll devices | Apple enrollment

Search

- Windows enrollment
- Apple enrollment**
- Android enrollment
- Enrollment device limit restrictions
- Enrollment device platform restrictions
- Corporate device identifiers
- Device enrollment managers

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. [Learn more.](#)

Prerequisites

- Apple MDM Push certificate**
Certificate required to manage Apple devices

Bulk enrollment methods

- Apple Configurator**
Manage Apple Configurator enrollment
- Enrollment program tokens**
Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

Enrollment options

- Enrollment notifications (preview)**
Send email or push notifications to devices after they enroll.
- Enrollment types (preview)**
Manage User Enrollment and Device Enrollment options

ENROLLMENT NOTIFICATIONS – We will create 2 notifications (iOS and MacOS)

Home > Devices | Enroll devices > Enroll devices | Apple enrollment >

Enrollment notifications (preview)

Apple enrollment

iOS Notifications macOS Notifications

Configure email and push notifications to be sent to users after they enroll. Notifications improve security by notifying users if someone enrolls a device with their credentials. IT admins can also use enrollment notifications to send users a welcome email or onboarding information following enrollment. [Learn more about enrollment notifications](#)

+ Create notifications

Create an enrollment notification

Enrollment Notifications

1 Basics 2 Notification settings 3 Scope tags 4 Assignments 5 Review + create






Name * iPhone iPad ✓

Description This is for iPhone and iPad devices ✓

Platform iOS/iPadOS ✓

Create an enrollment notification ...

Enrollment Notifications

 Basics  Notification settings  Scope tags  Assignments  **Review + create**

Summary

Basics

| | |
|-------------|-------------------------------------|
| Name | iPhone iPad |
| Description | This is for iPhone and iPad devices |
| Platform | ios |

Notification settings

Push Notification

| | |
|------------------------|--------------------------------------|
| Send Push Notification | On |
| Subject | Device Enrollment |
| Message | You have enrolled a new apple device |

Email Notification

| | |
|-------------------------|-------------------------------------------------|
| Send Email Notification | On |
| Subject | Device Enrollment |
| Message | You have successfully enrolled new apple device |

Email Header

| | |
|-------------------|----|
| Show company logo | On |
|-------------------|----|

Email Footer

| | |
|----------------------------------|----|
| Show device details | On |
| Show company name | On |
| Show contact information | On |
| Show company portal website link | On |

Scope tags

Default

Assignments

| | |
|-----------------|-----------|
| Included groups | All users |
|-----------------|-----------|

[Previous](#)

[Create](#)

Do the same for MacOS

Create an enrollment notification

Enrollment Notifications

1 Basics 2 Notification settings 3 Scope tags 4 Assignments 5 Review + create

Name * MacBook Pro ✓

Description This is for MacBook Pro device ✓

Platform macOS

Create an enrollment notification

Enrollment Notifications

✓ Basics ✓ Notification settings ✓ Scope tags ✓ Assignments 5 Review + create

Summary

| Basics | |
|-------------|--------------------------------|
| Name | MacBook Pro |
| Description | This is for MacBook Pro device |
| Platform | mac |

Notification settings

Push Notification

| | |
|------------------------|---------------------------------|
| Send Push Notification | On |
| Subject | Device Enrollment |
| Message | Thanks for enrolling Mac Laptop |

Email Notification

| | |
|-------------------------|--------------------------------------------|
| Send Email Notification | On |
| Subject | Device Enrollment |
| Message | You have successfully enrolled Macbook Pro |

Email Header

| | |
|-------------------|----|
| Show company logo | On |
|-------------------|----|

Email Footer

| | |
|----------------------------------|-----|
| Show device details | Off |
| Show company name | On |
| Show contact information | On |
| Show company portal website link | On |

Scope tags

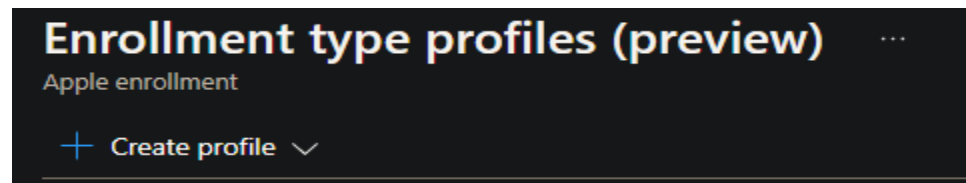
Default

Assignments

| | |
|-----------------|-----------|
| Included groups | All users |
|-----------------|-----------|

Previous Create

ENROLLMENT TYPES – We will create 3 different profiles - https://learn.microsoft.com/en-us/mem/intune/enrollment/ios-user-enrollment?WT.mc_id=Portal-Microsoft_Intune_Enrollment



Create enrollment type profile

Apple enrollment

✓ Basics ✓ Settings ✓ Assignments **4 Review + create**

Summary

Basics

Name Apple Device Enrollment

Description --

Settings

Enrollment type **Device enrollment**

Assignments

Included groups All users

Excluded groups --

Create enrollment type profile

Apple enrollment

✓ Basics ✓ Settings ✓ Assignments **4 Review + create**

Summary

Basics

Name Apple Device Enrollment

Description --

Settings

Enrollment type **User enrollment**

Assignments

Included groups All users

Excluded groups --

Enrollment type profiles (preview)

Apple enrollment

+ Create profile ▾

Create and manage enrollment type profiles for iOS/iPadOS users that have personal or corporate devices. This profile deploys device and enrollment type options to users setting up their devices in Company Portal. [Learn more.](#)

| Priority | Name | Description | Assigned | Last Modified |
|----------|---------------------------------------|-------------|----------|-------------------|
| 1 | Apple Device Enrollment - User Choice | | Yes | 12/28/22, 7:22 AM |
| 2 | Apple Device Enrollment - Device | | Yes | 12/28/22, 7:22 AM |
| 3 | Apple Device Enrollment - User | | Yes | 12/28/22, 7:23 AM |

We can change priority, if needed and higher priority takes precedence during device enrollment.

APPLE CONFIGURATOR – <https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios> - You can learn more about it from above link..

Set up iOS/iPadOS device enrollment with Apple Configurator

Article • 12/05/2022 • 8 minutes to read • 8 contributors

[Feedback](#)

Intune supports the enrollment of iOS/iPadOS devices using [Apple Configurator](#) running on a Mac computer. Enrolling with Apple Configurator requires that you USB-connect each iOS/iPadOS device to a Mac computer to set up corporate enrollment. You can enroll devices into Intune with Apple Configurator in two ways:

- **Setup Assistant enrollment** - Wipes the device and prepares it to enroll during Setup Assistant.
- **Direct enrollment** - Does not wipe the device and enrolls the device through iOS/iPadOS settings. This method only supports devices with **no user affinity**.

Apple Configurator enrollment methods can't be used with the [device enrollment manager](#).

Prerequisites

- Physical access to iOS/iPadOS devices
- [Set MDM authority](#)
- [An Apple MDM push certificate](#)
- Device serial numbers (Setup Assistant enrollment only)
- USB connection cables
- macOS computer running [Apple Configurator 2.0](#)

Apple Configurator | Profiles

Apple enrollment

Overview

Manage

Devices

Profiles

+ Create

To enroll iOS devices through Apple Configurator, create an enrollment profile. [Learn more.](#)

Search by profile name

| Name | Description | User Affinity |
|-------------|-------------|---------------|
| No Profiles | | |

Create Enrollment Profile

✓ Basics

✓ Settings

3 Review + create

Summary

Basics

NameCorporate Apple Device Apple Configurator

Description--

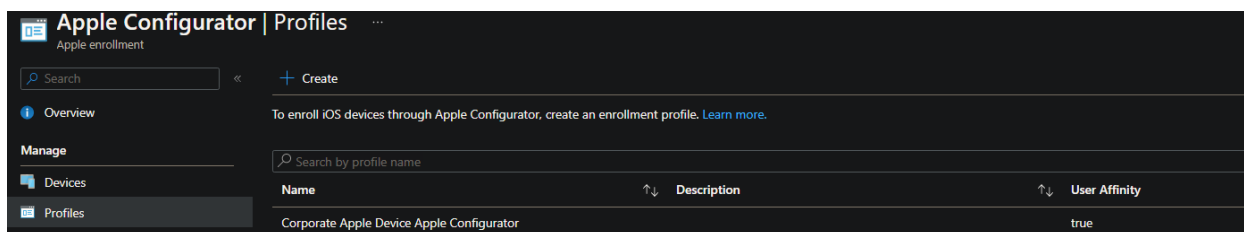
Settings

User affinityEnroll with user affinity

Select where users must authenticateCompany Portal

Previous

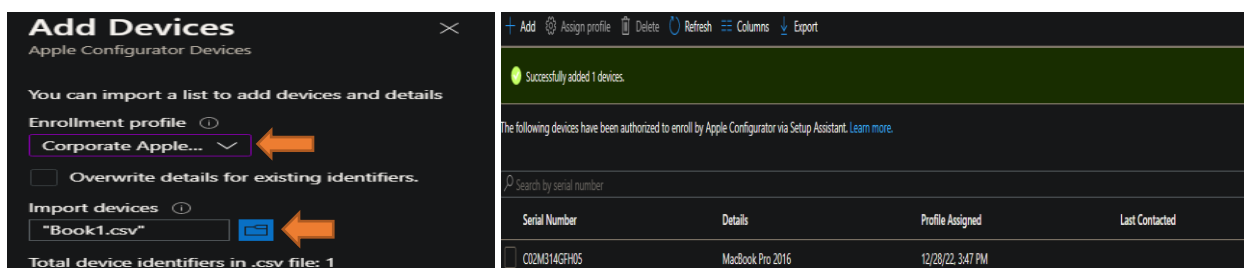
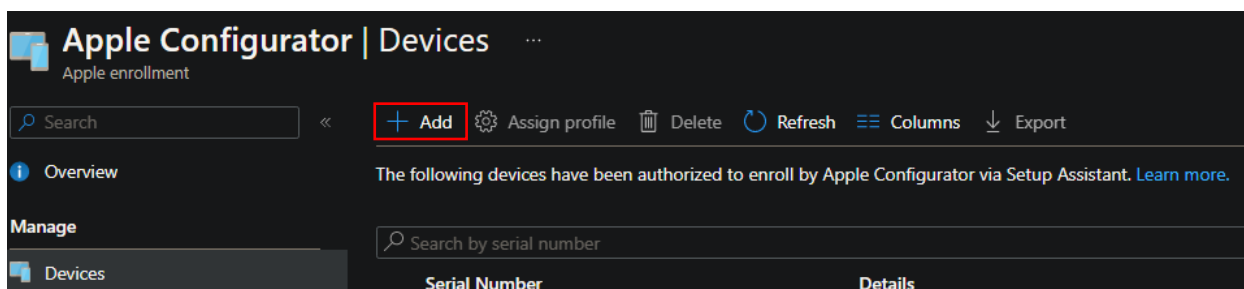
Create



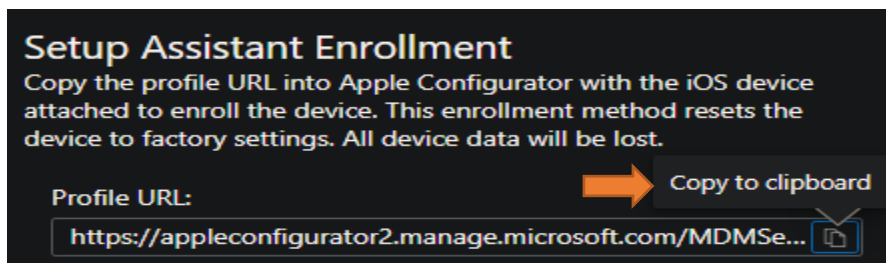
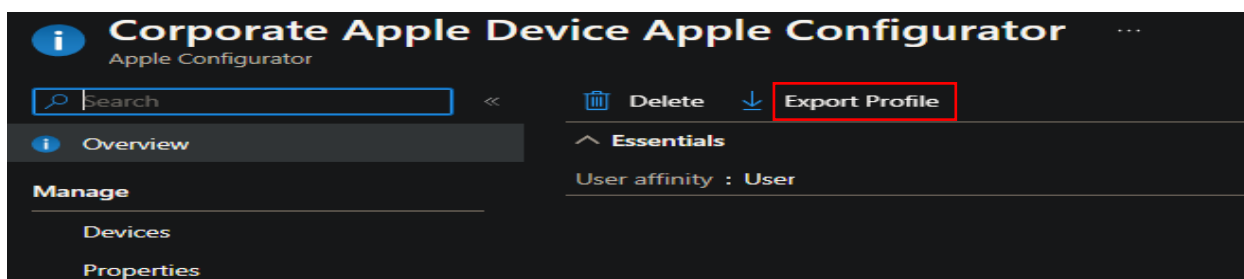
Now add iPhone, iPad and MacBook Pro serial # if you have any. I have a MacBook Pro which, I am going to add.

Open Excel – New Sheet – Create 2 Columns detailed below. Save file as csv so we can upload to Intune.

| A | B |
|--------------|------------------|
| C02M314GFH05 | MacBook Pro 2016 |



Export the profile – Now export the profile so we can use it on Mac machine using Apple Configurator 2



<https://appleconfigurator2.manage.microsoft.com/MDMServiceConfig?id=925ea719-1580-4bed-b33e-32b4140c9d0a&AADTenantId=5e11113d-da15-40e6-b616-07c2>

We are not going for Direct Enrollment – you can ignore this - <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-direct-enroll-macos>

Direct Enrollment

Download the enrollment profile to Apple Configurator to push directly as a management profile to a connected iOS device. No factory reset required.

Only Profiles without user affinity can be used for direct enrollment.

[Download profile](#)

Direct Enrollment

Because Direct Enrollment only supports enrollment without user affinity, the company portal cannot be used to install available applications.

Export the profile and install on macOS devices

1. In the [admin center](#), go to **Devices > Enroll devices**.
2. Select **Apple enrollment > Apple Configurator > Profiles**.
3. Select the profile you want to export, and then select **Export Profile**.
4. Under **Direct enrollment**, choose **Download profile**, and then save the file.

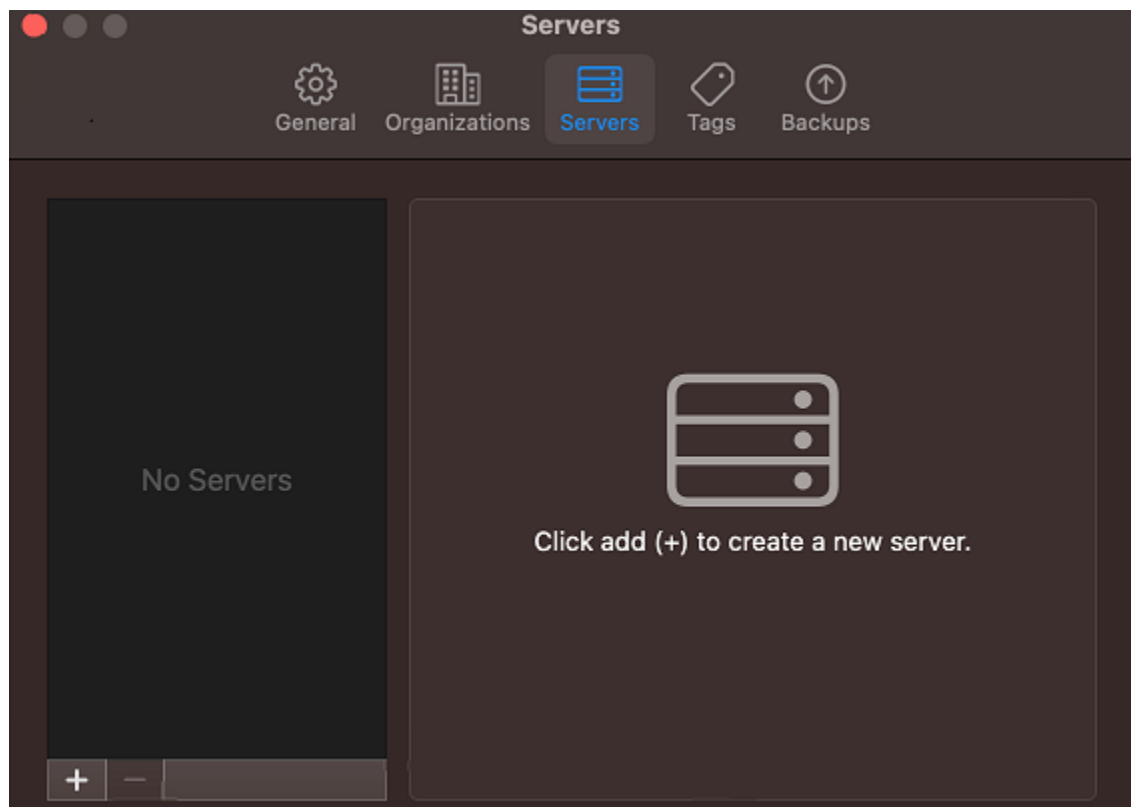
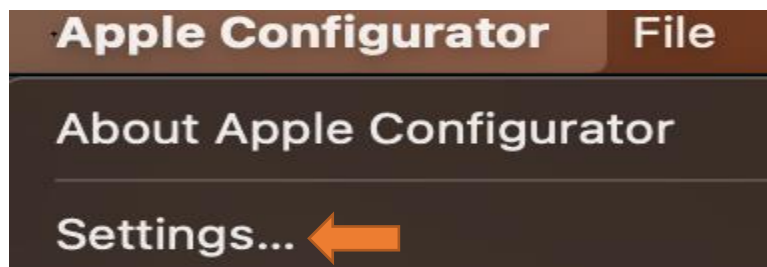
Note

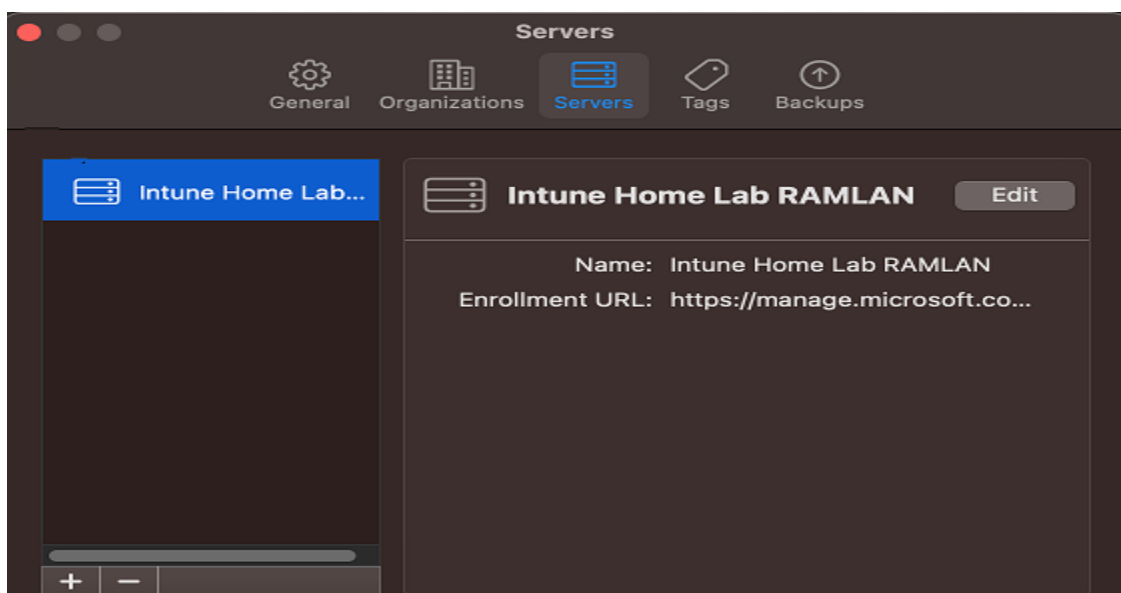
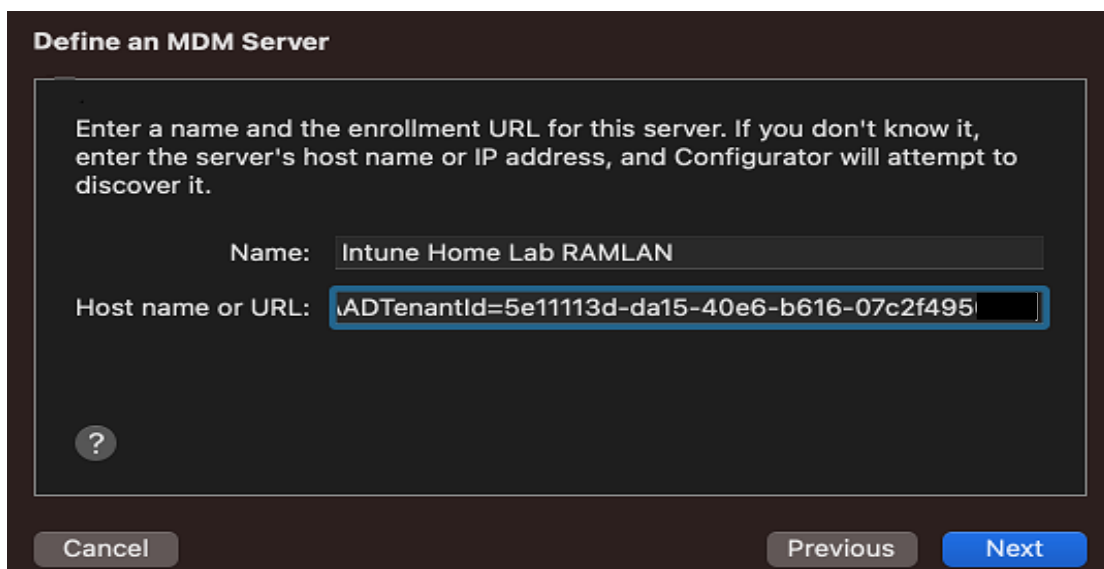
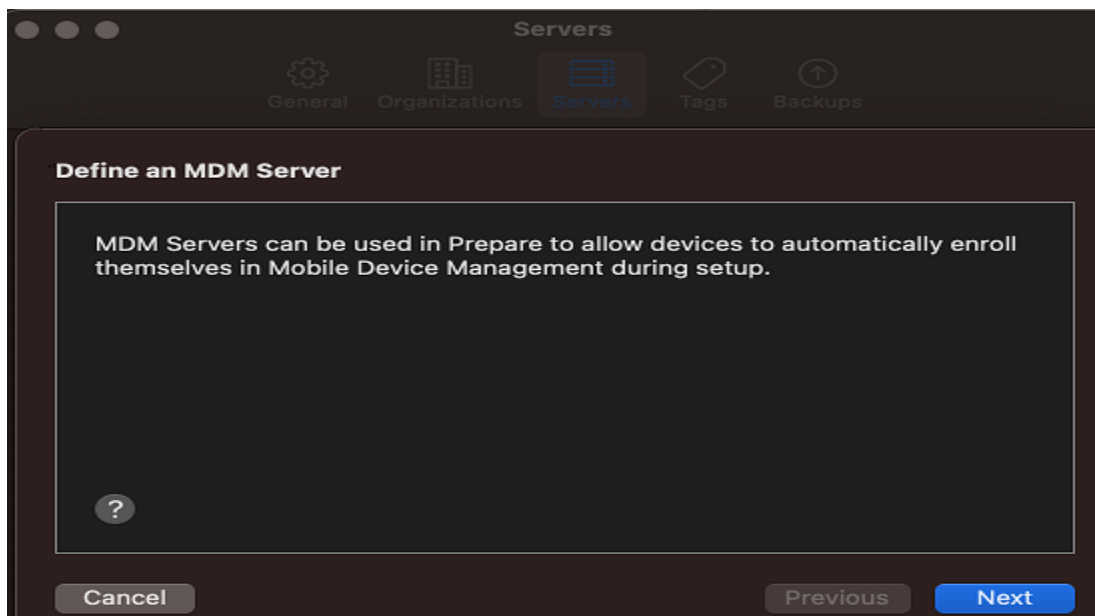
A downloaded enrollment profile is valid for two weeks after download. You can download as many enrollment profiles using this link as you need. Downloading a new profile does not render the previous one invalid, however it also doesn't extend the previously downloaded file expiry time.

5. Transfer the file to a macOS computer to install it directly.
6. Double-click on the saved **.mobileconfig** to open the file in Profiles.
7. When prompted to install the management profile, select **Install**.
8. Confirm on the next prompt you want to install the management profile by selecting **Install**.
9. Sign in with an admin account on the macOS device, and then select **OK**.

The macOS device is now enrolled in Intune and ready-to-manage. Targeted profiles begin downloading.

Enroll device with Setup Assistant – On Mac computer install Apple Configurator from AppStore → Open → Complete the following.



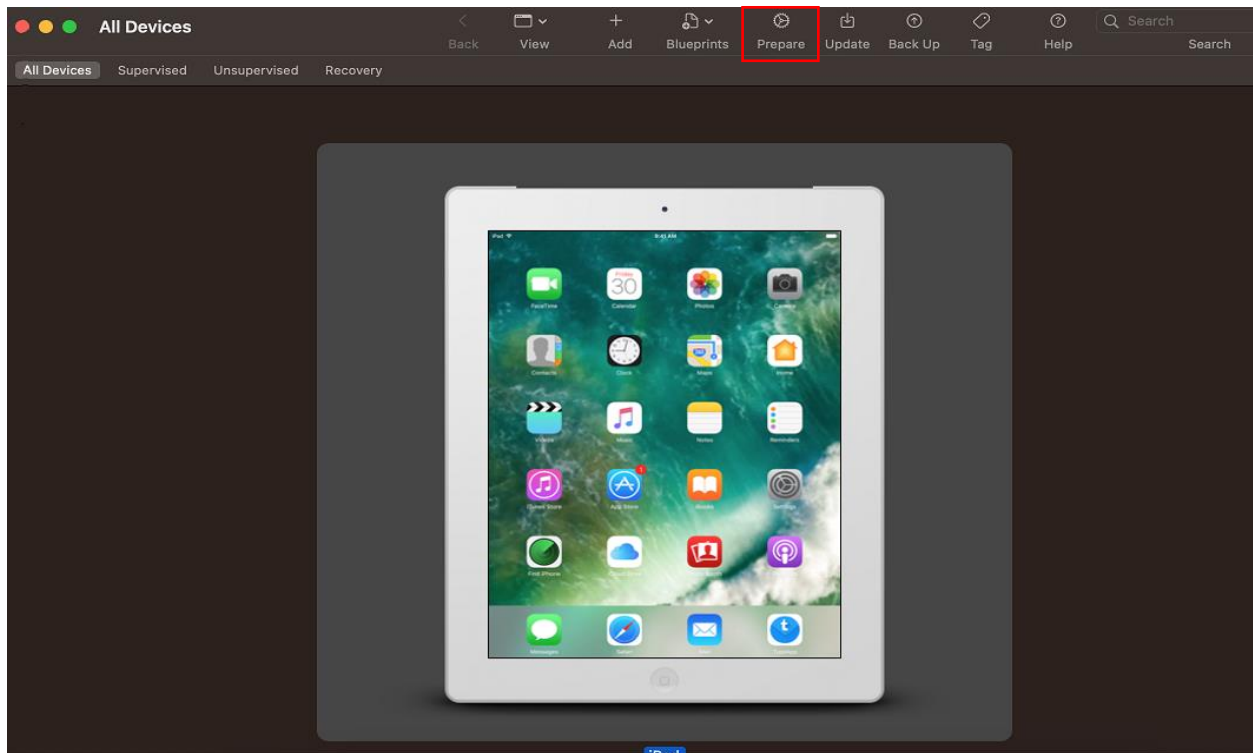


Now we need a spare device to complete Setup Assistant Configuration. Connect iPhone or iPad to Mac Computer with USB adapter. I am using old iPad that is already setup. Normally you will see Hello screen on a brand new iPad or iPhone. So don't worry about my iPad already setup. When you prepare the iPad using Apple Configurator it will erase. You will see later. I will post the screen shoot.

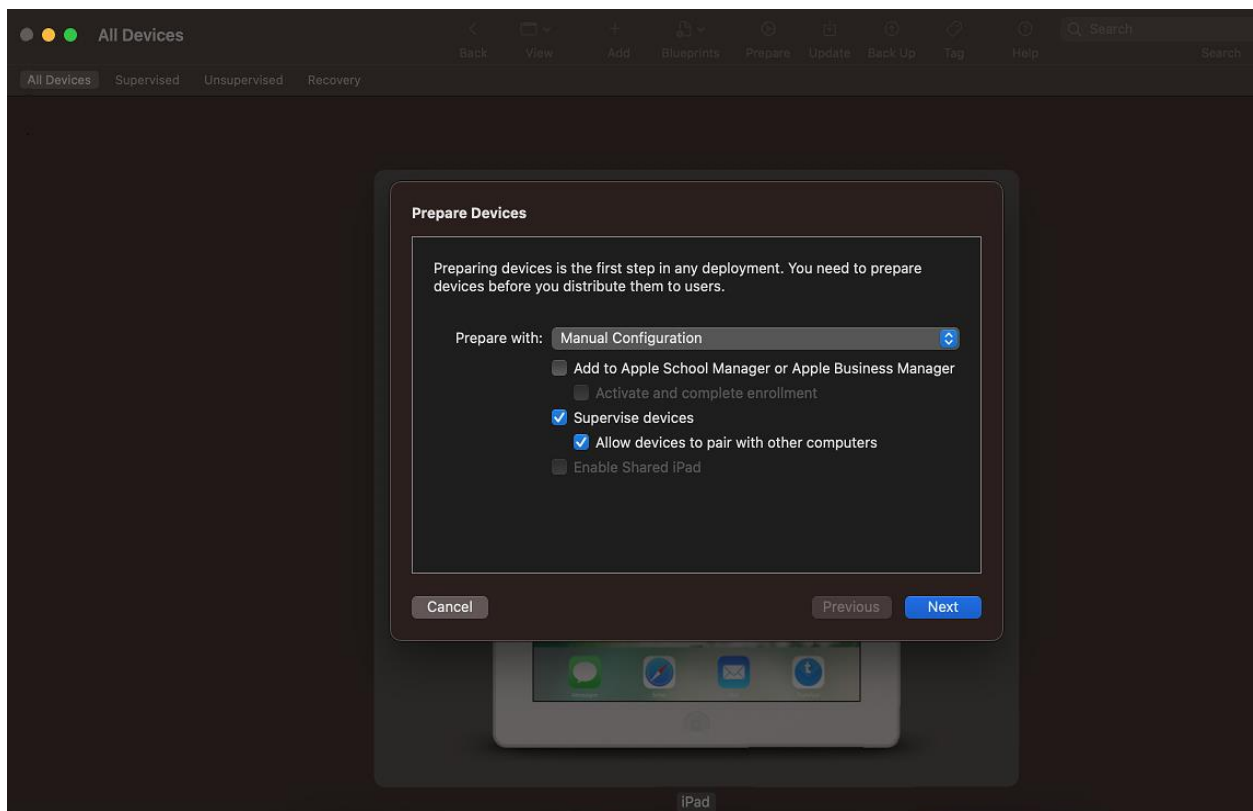
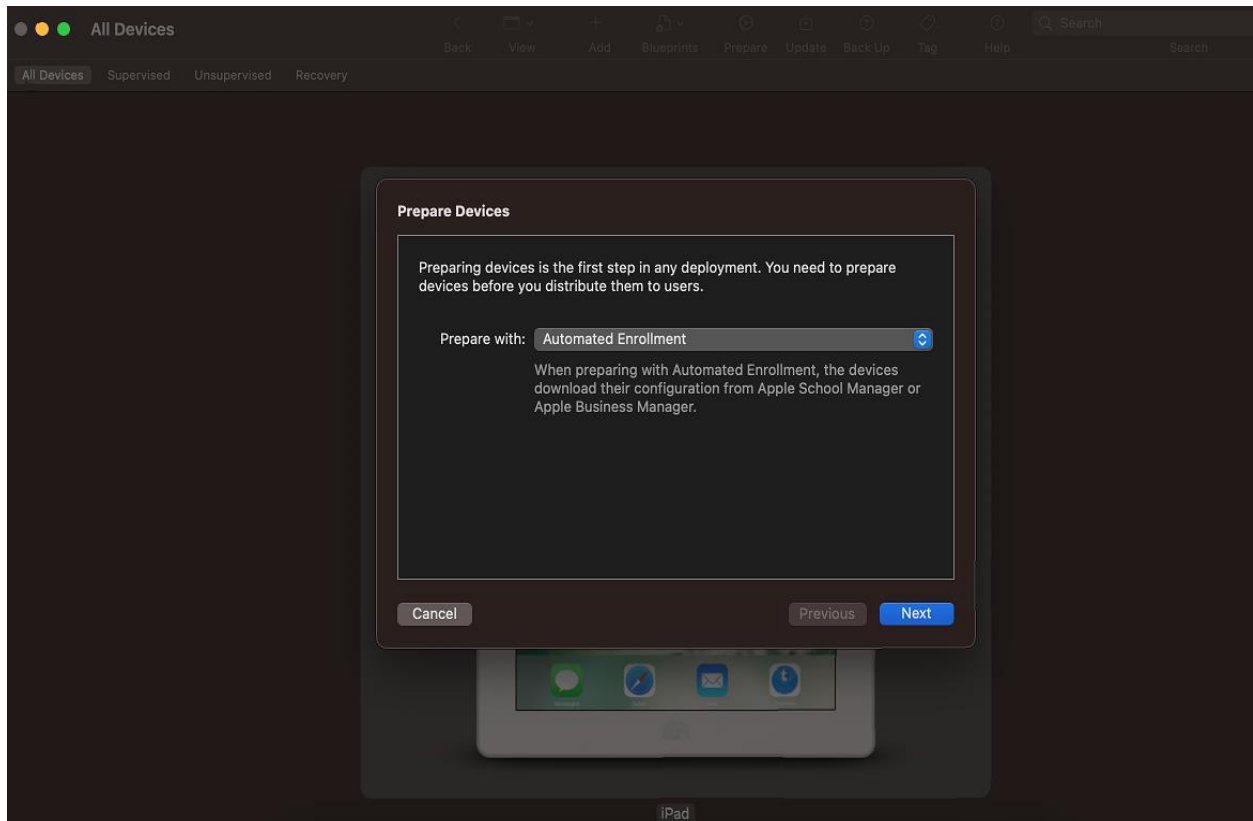
When you connect iPad or iPhone you will see a message to Trust the device – click Trust.



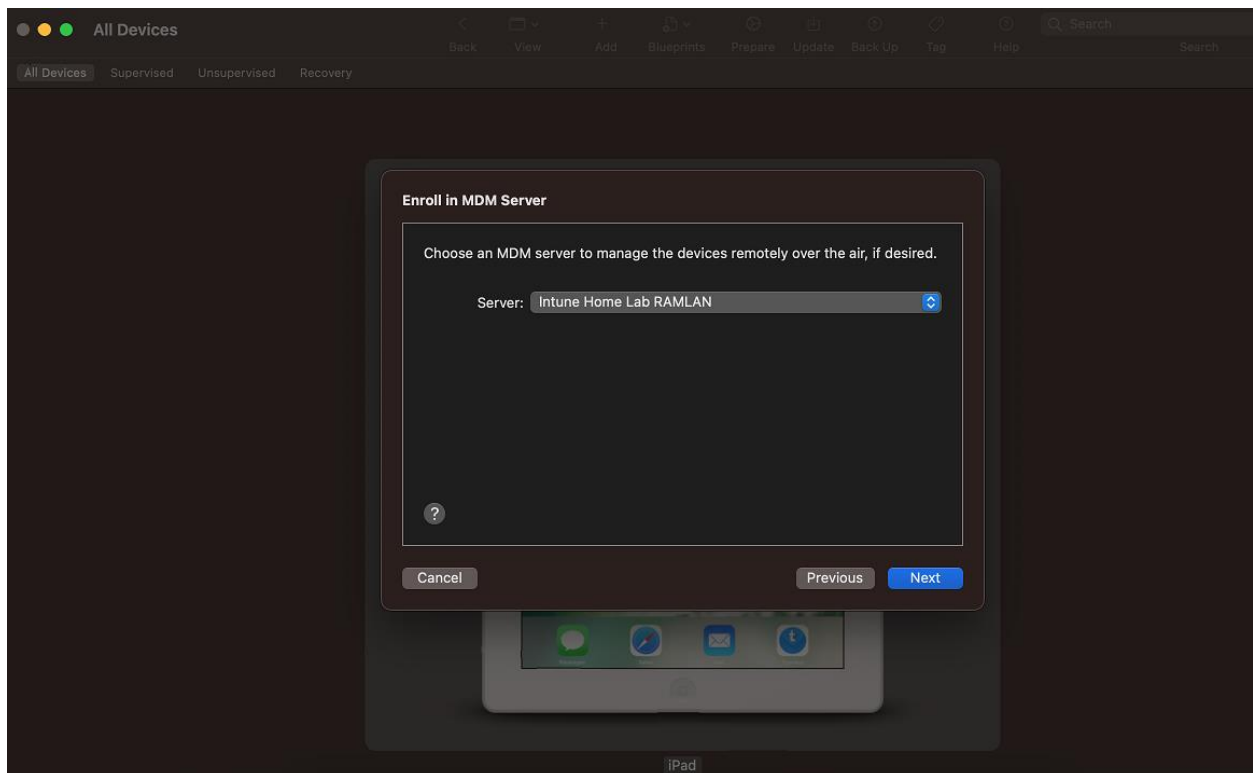
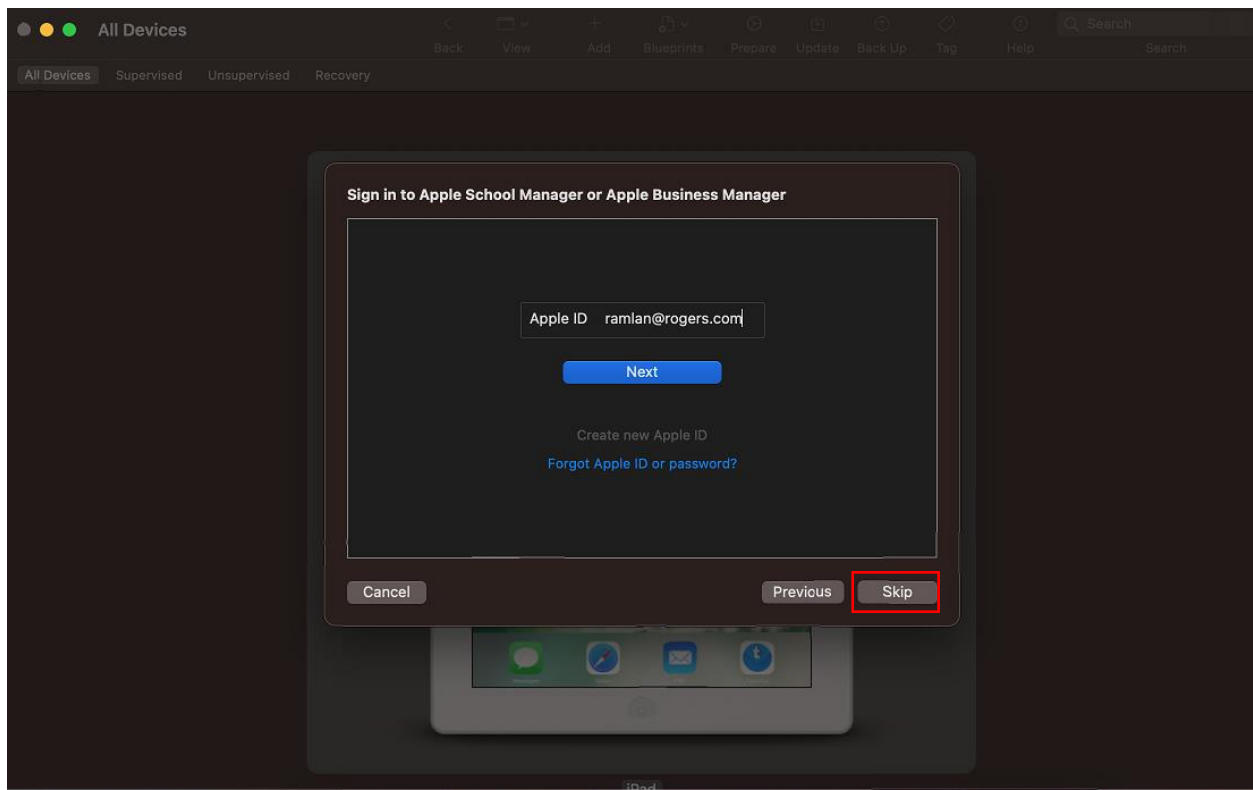
After that select the device and click Prepare.



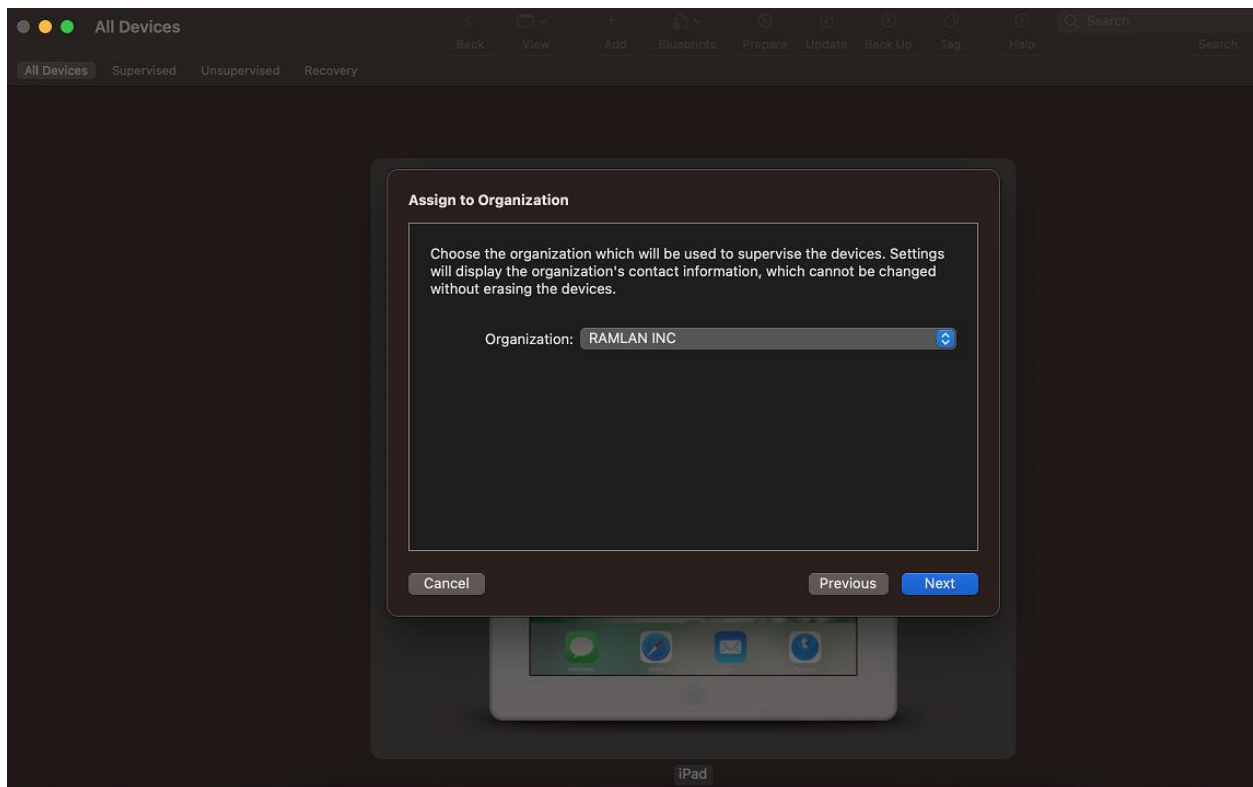
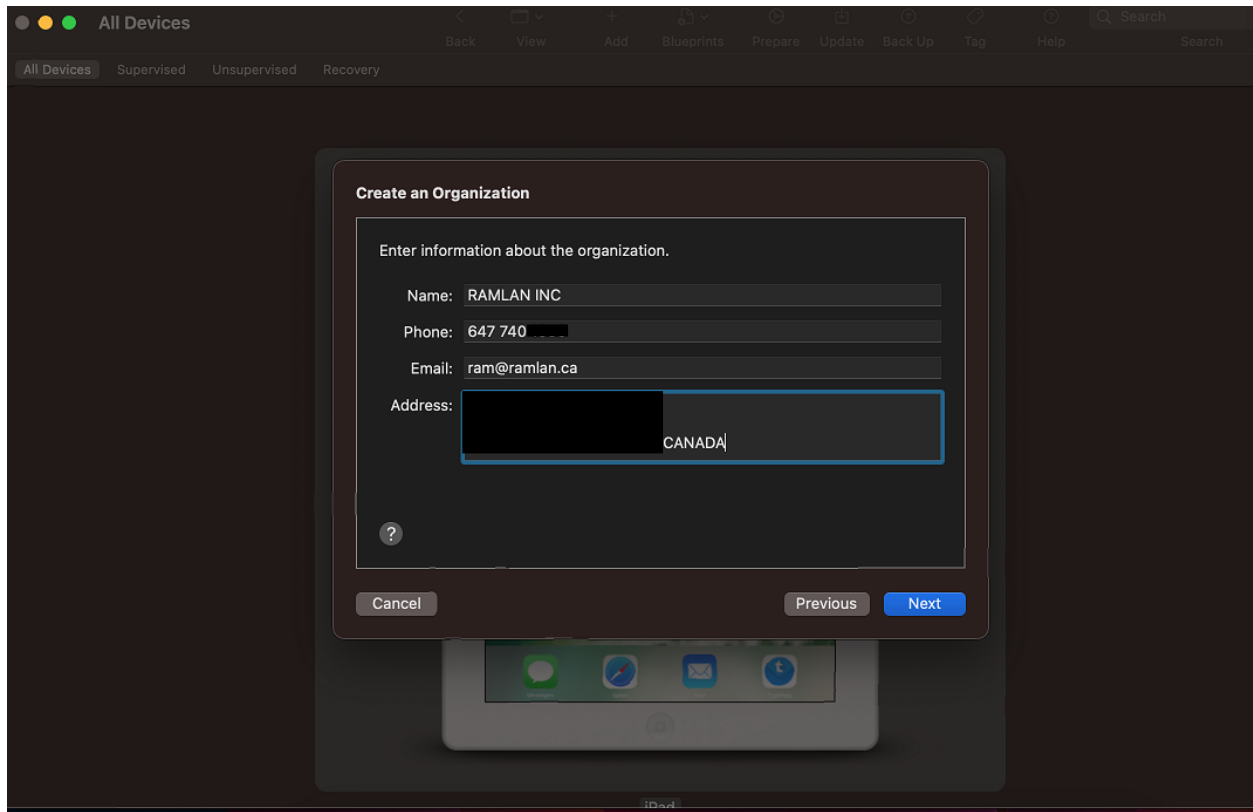
Here you have 2 options (Automated Enrollment and Manual Configuration). They are self explanatory. I am going with Manual Configuration because, I don't have account with Apple Business Manager. I tried applying for an account but they declined my request. I guess it is for available for lab use.

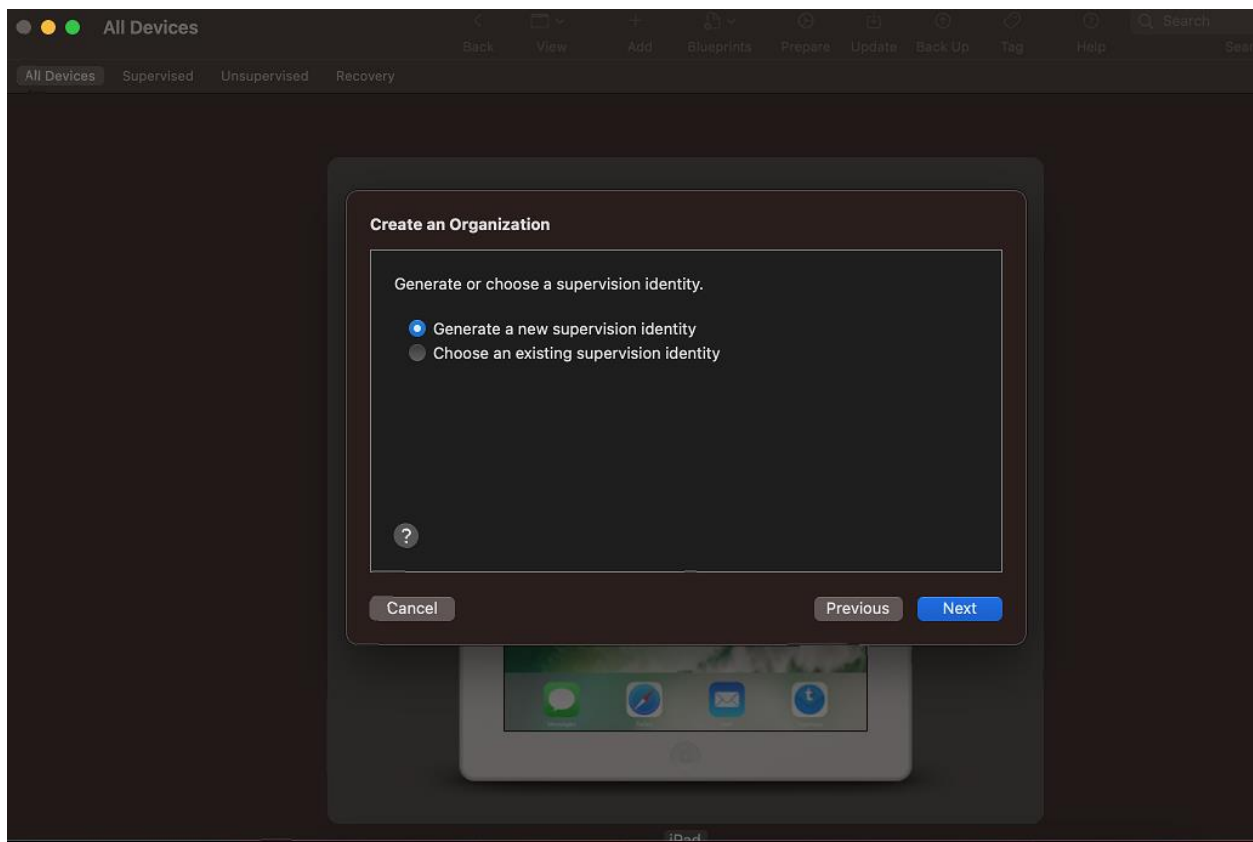


On the next screen you will be prompted to enter ABM ID and password. I don't have account with ABM. So, I am going to skip.

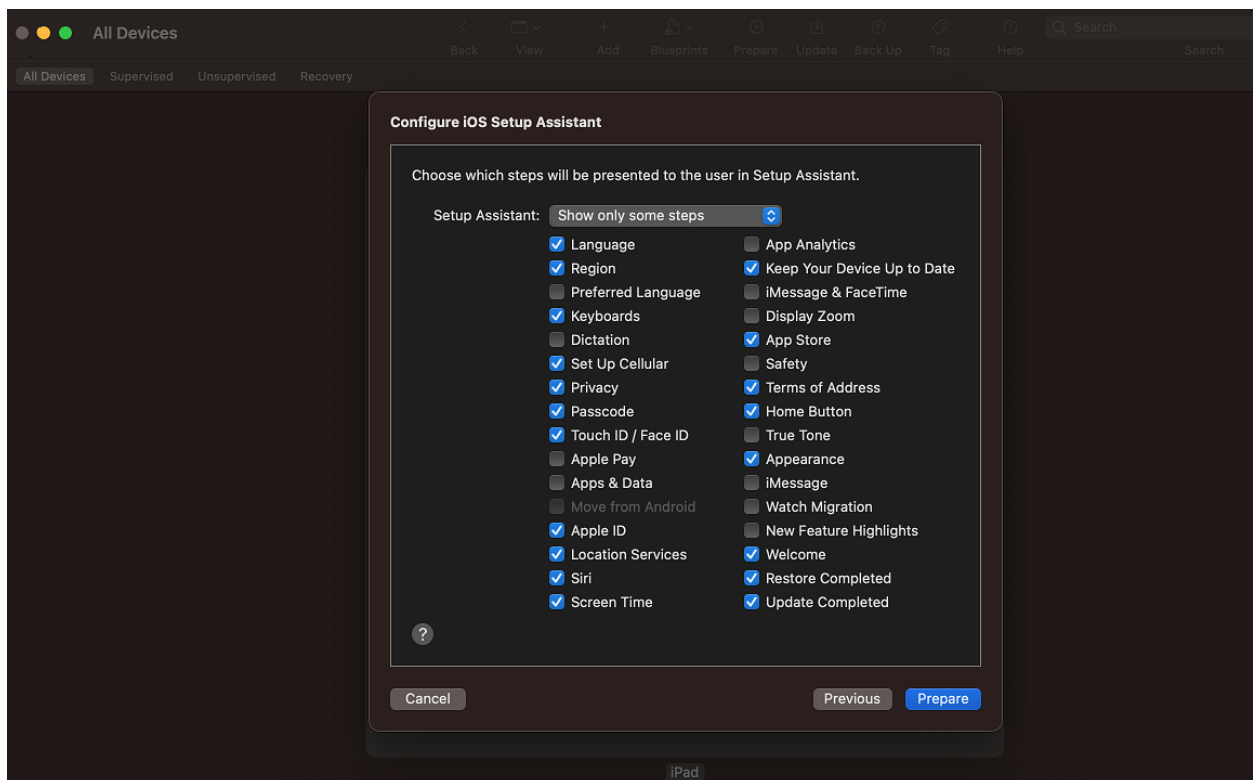


I created the Organization before the setup. You can do the same from Apple Configurator -> Settings -> Organization -> Click +

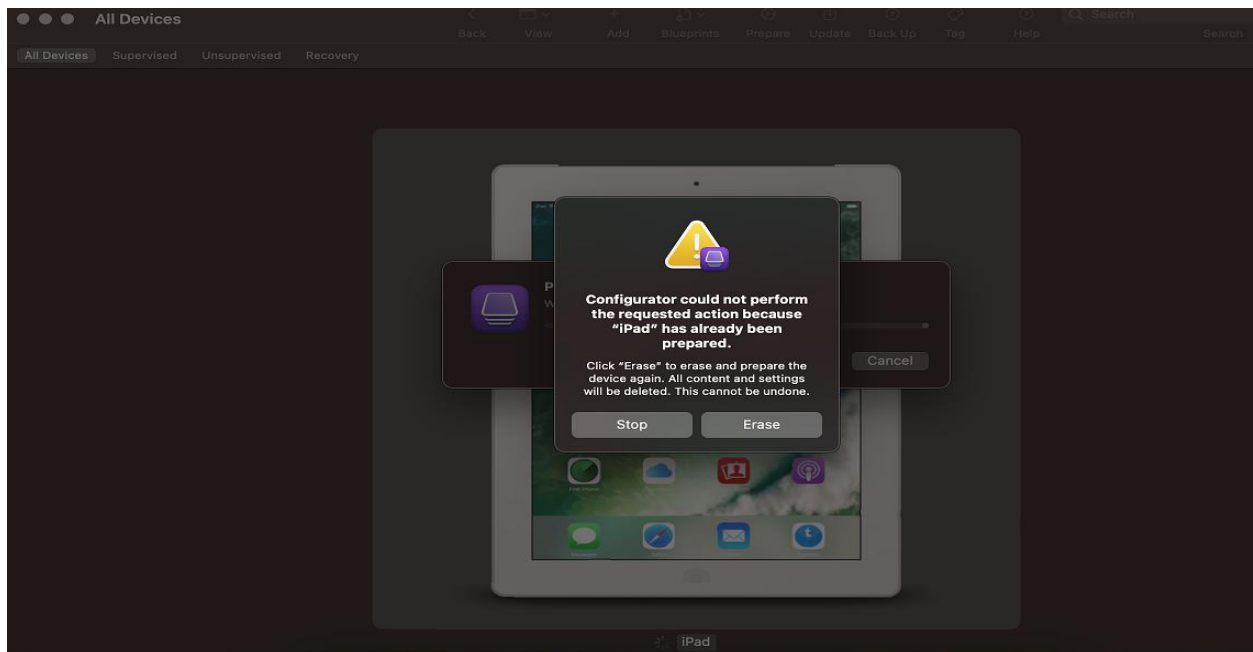




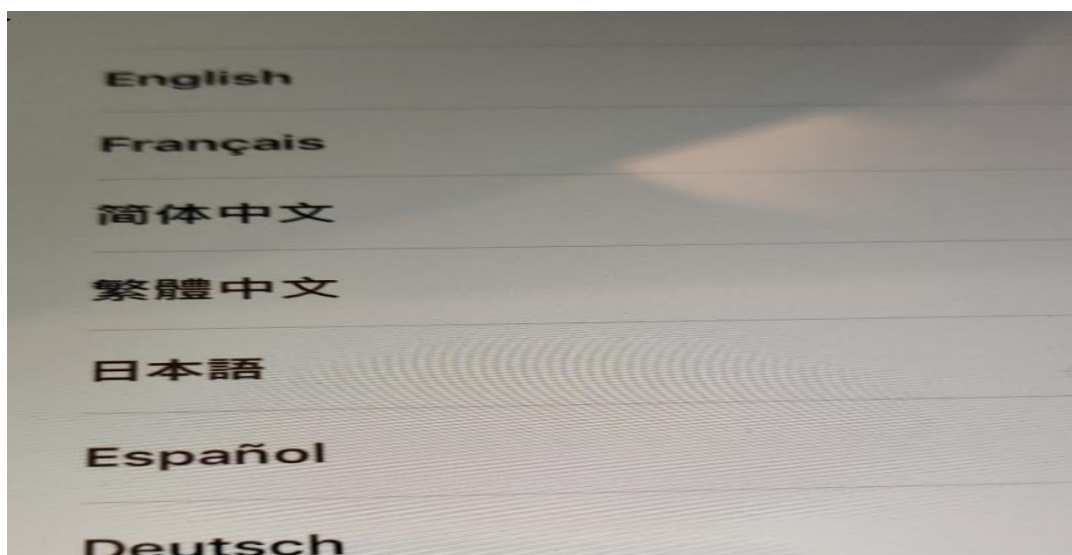
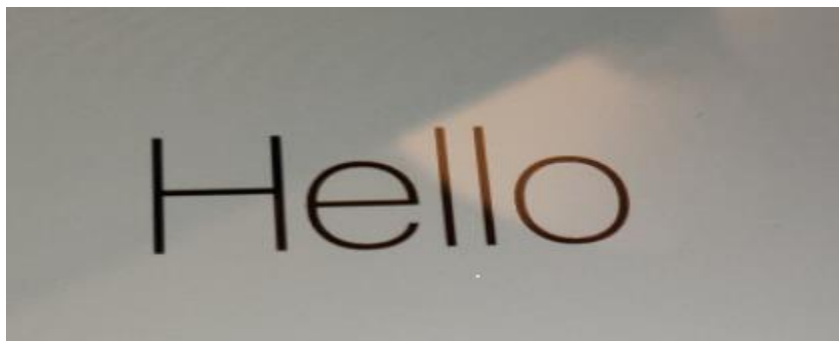
Here you get the option to select what your users should see during initial setup. I just enabled a few for this test run within home lab.



As, I mentioned before iPad being used for this test is already setup. That is why we are getting below message. I did click Erase to start from the scratch.



When the devices finishes preparing disconnect USB cable and distribute the device to end user. When user power on the device they will see these screens.



Select Your Country or Region

Canada

Choose a Wi-Fi Network

✓ 1216

Location Services

Location Services allows Maps and other apps and services like Find My iPad to gather and use data indicating your approximate location.

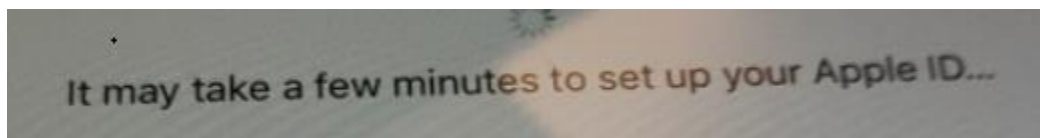
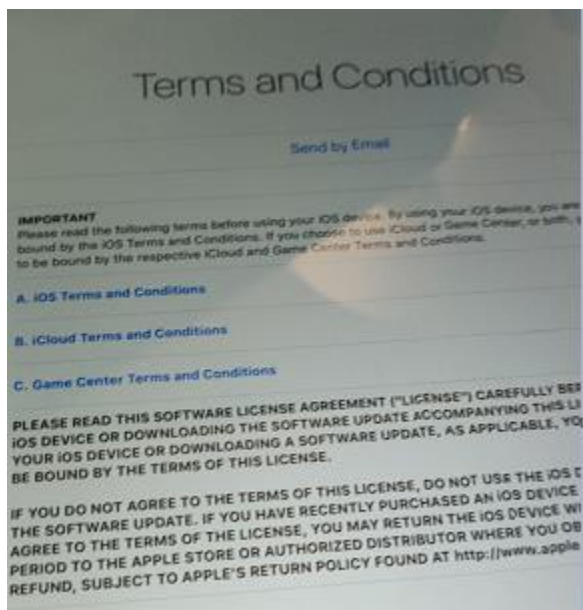
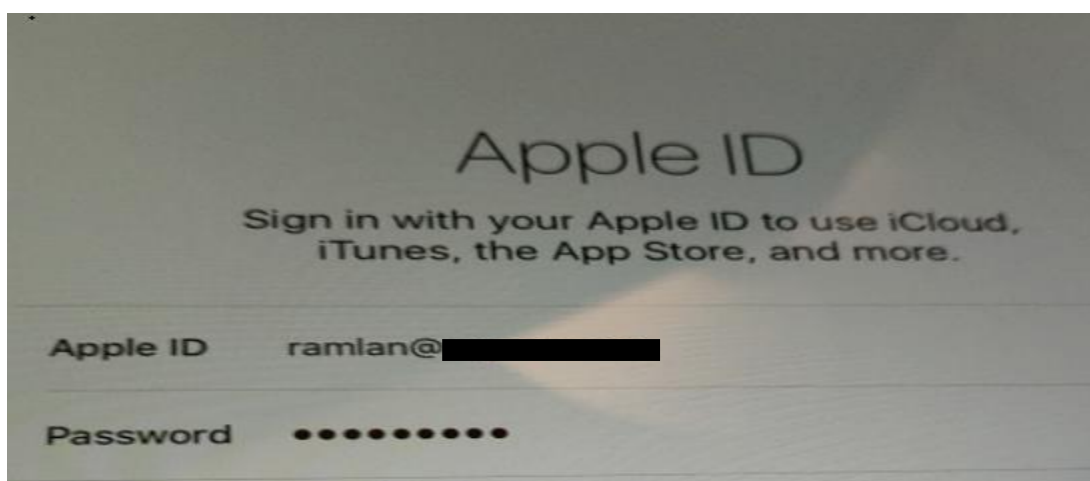
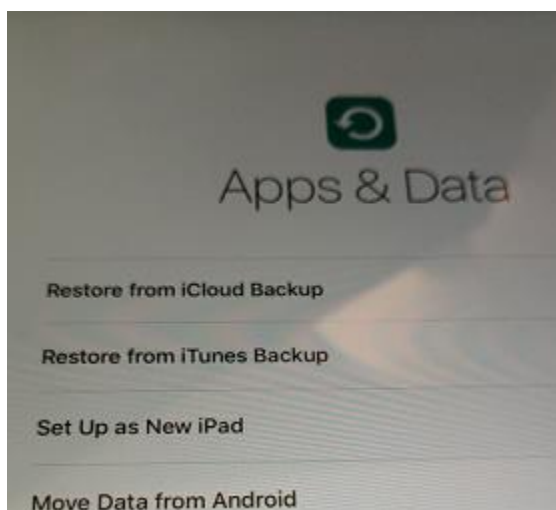
[About Location Services](#)

[Enable Location Services](#)

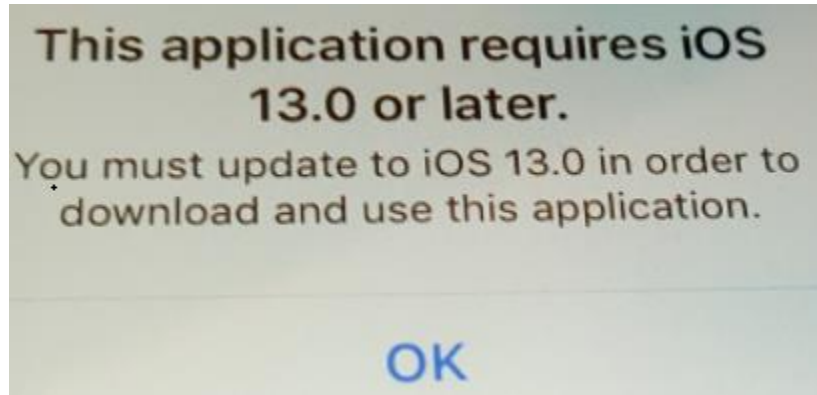
Create a Passcode

A passcode protects your data and is used to unlock iPad.





On the next screen we should see Remote Management to enroll the device to Intune and complete installing Management profile. Unfortunately, the iPad, I am using for this test is running IOS 10. So cannot proceed further. Will have to find a new device that is running IOS 13 or later and perform the exercise again. Now you at least get an idea how Apple Configurator works and how it can be implemented in production.




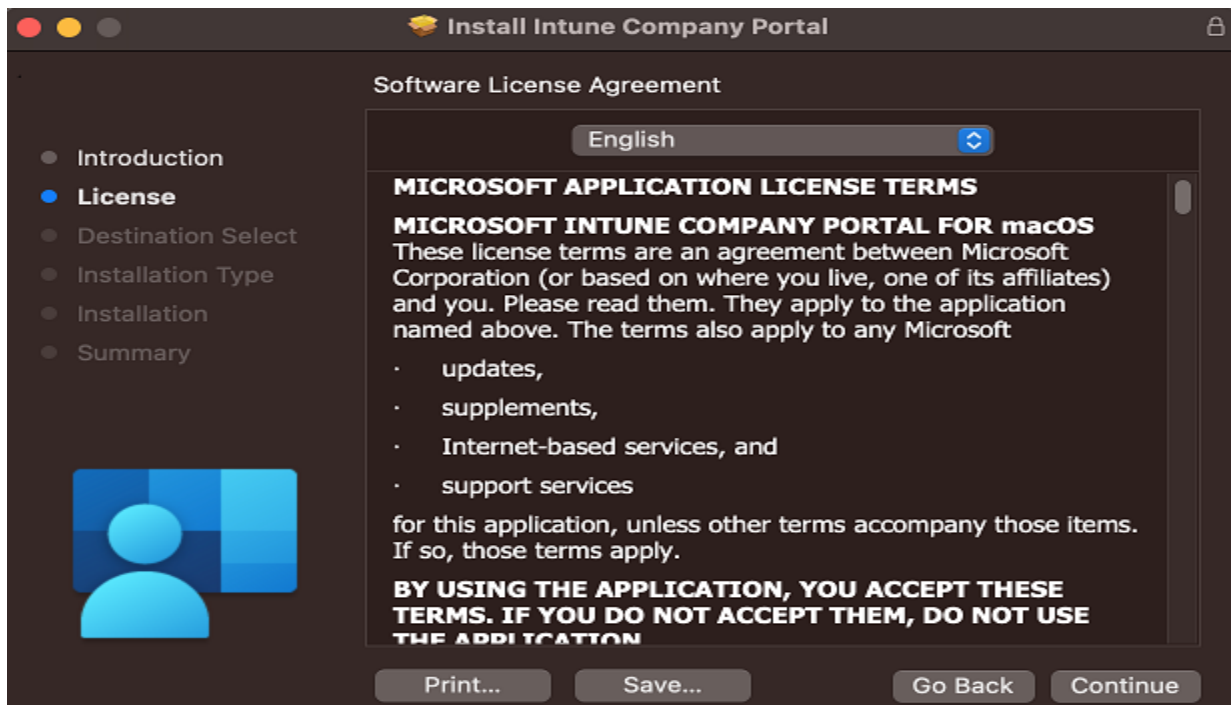
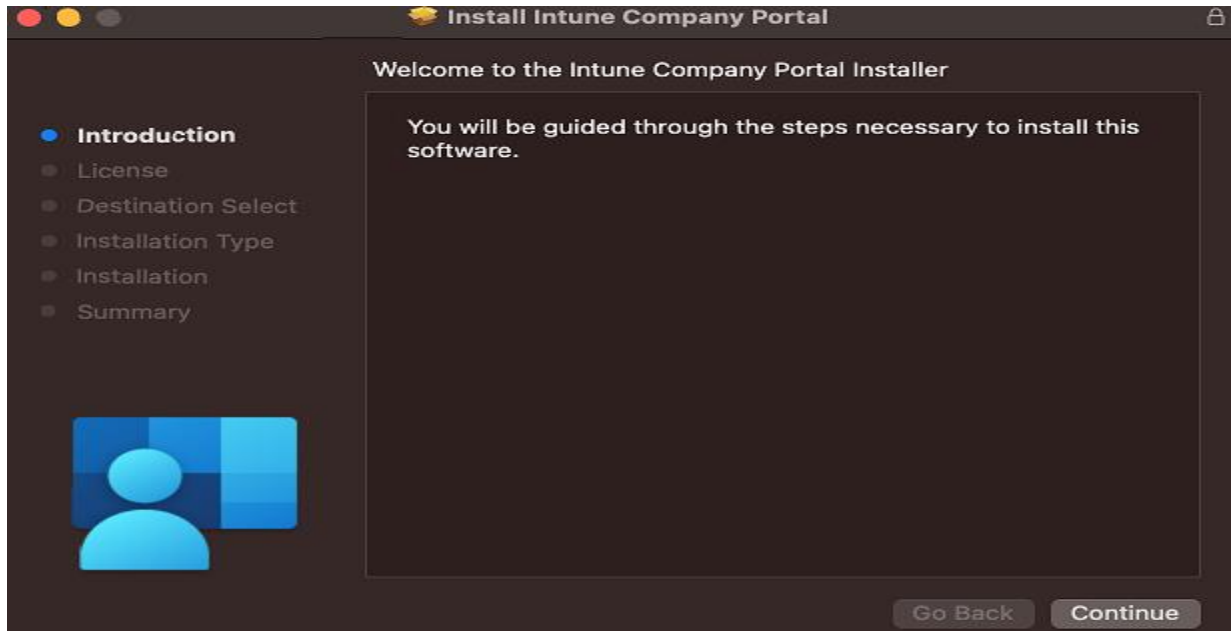
HOW TO ENROLL MACBOOK PRO - Since, I don't have spare iPhone to enroll, I will give it a try using MacBook Pro 2016.

<https://learn.microsoft.com/en-us/mem/intune/user-help/enroll-your-device-in-intune-macos-cp>

Download Enroll My Mac package from here - <https://go.microsoft.com/fwlink/?linkid=853070>

Login to MacBook Pro -> Open the pkg and continue through the steps detailed below

| Name | Date modified | Type | Size |
|---------------------------------------------------------------------------------------------------------------|------------------|----------|-----------|
|  CompanyPortal-Installer.pkg | 28-Dec-2022 5... | PKG File | 26,166 KB |



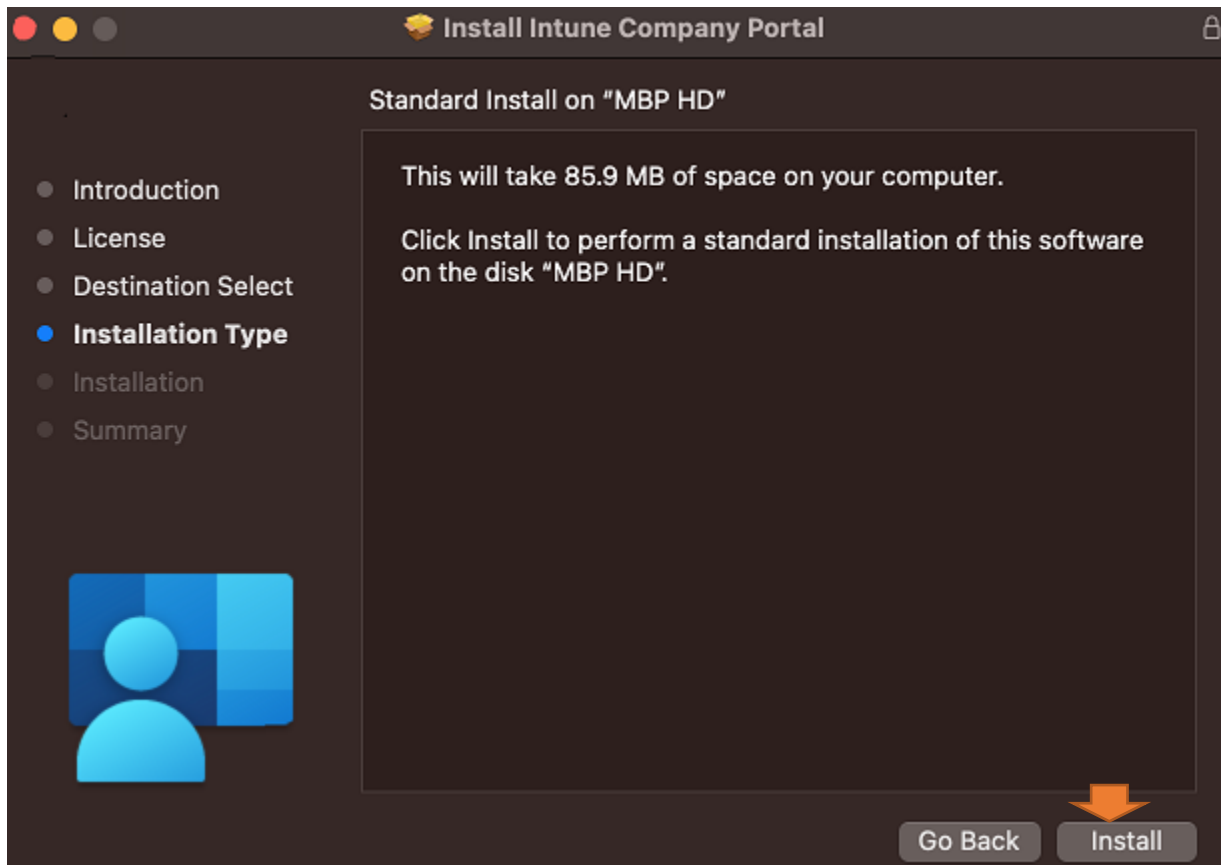
To continue installing the software you must agree to the terms of the software license agreement.

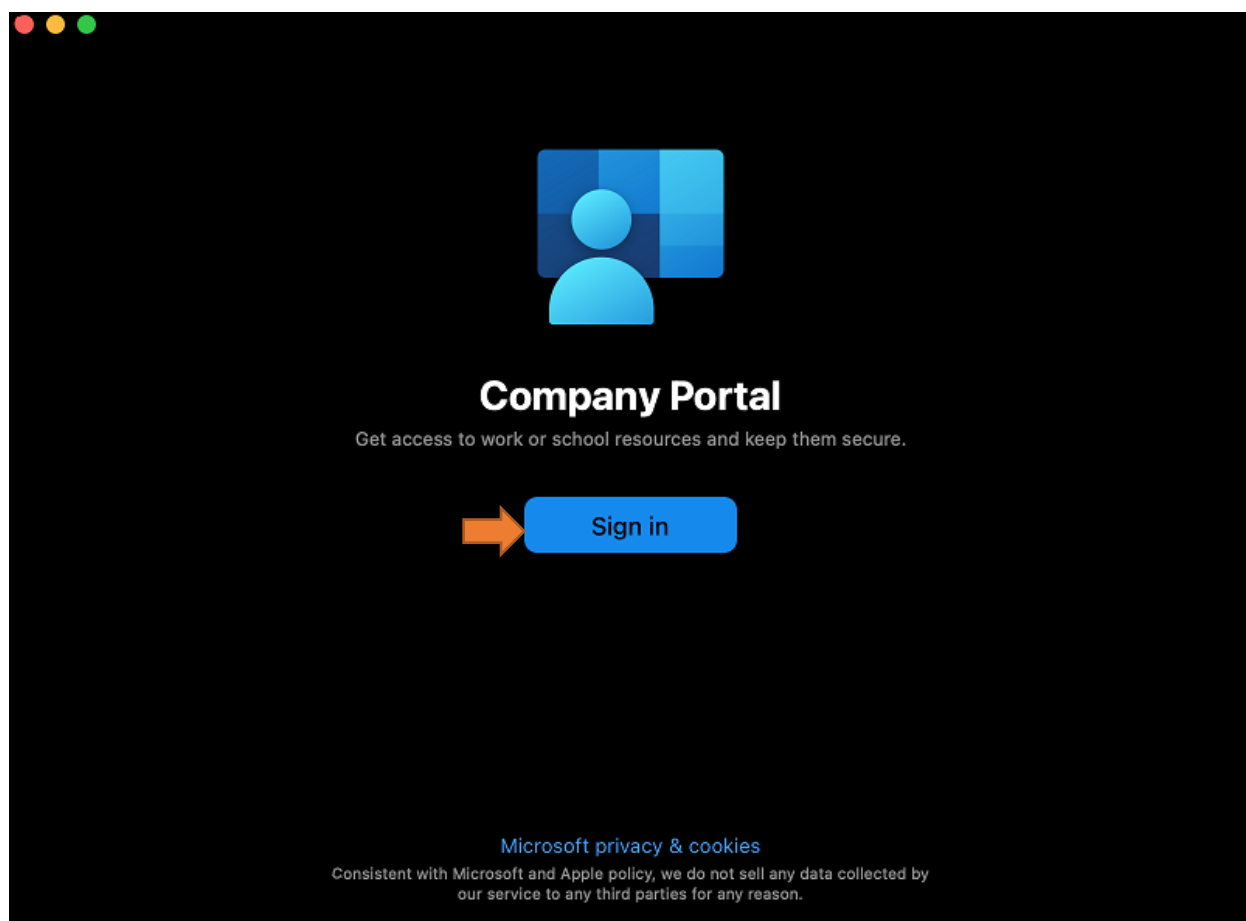
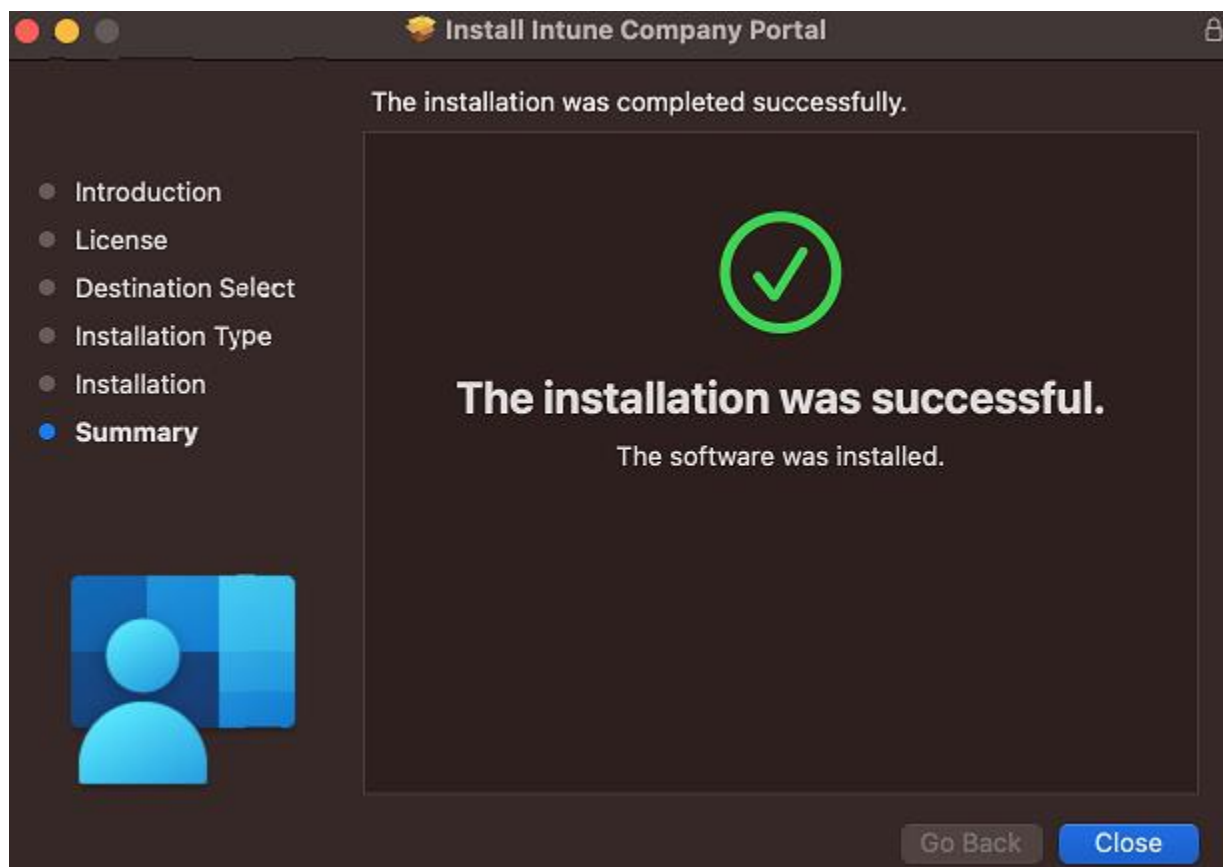
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

Read License

Disagree

Agree





Microsoft Intune



Sign in

ram@ramlan.ca

[Can't access your account?](#)

Next

RAMLAN INC

- ① Review privacy information
- ② Install management profile
- ③ Checking device settings

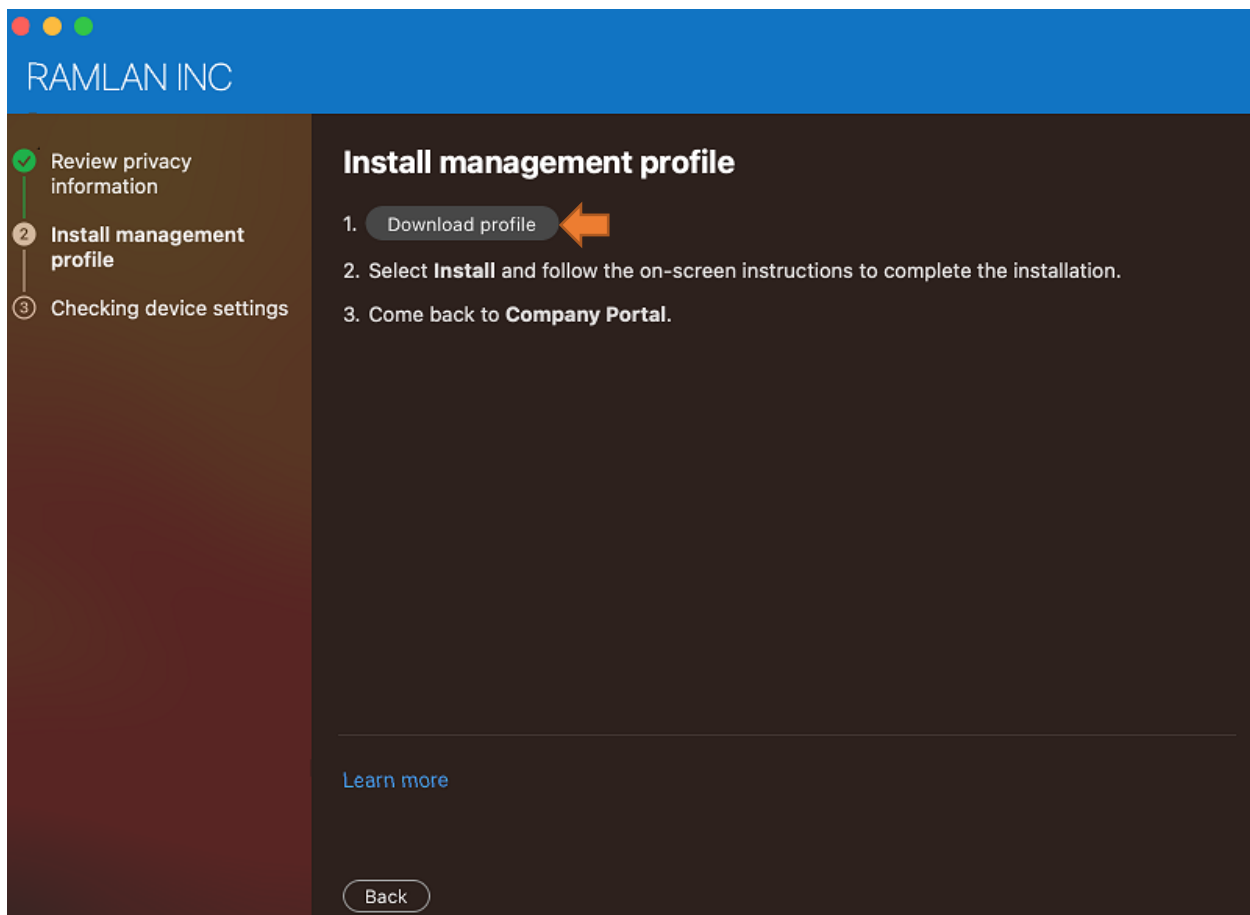
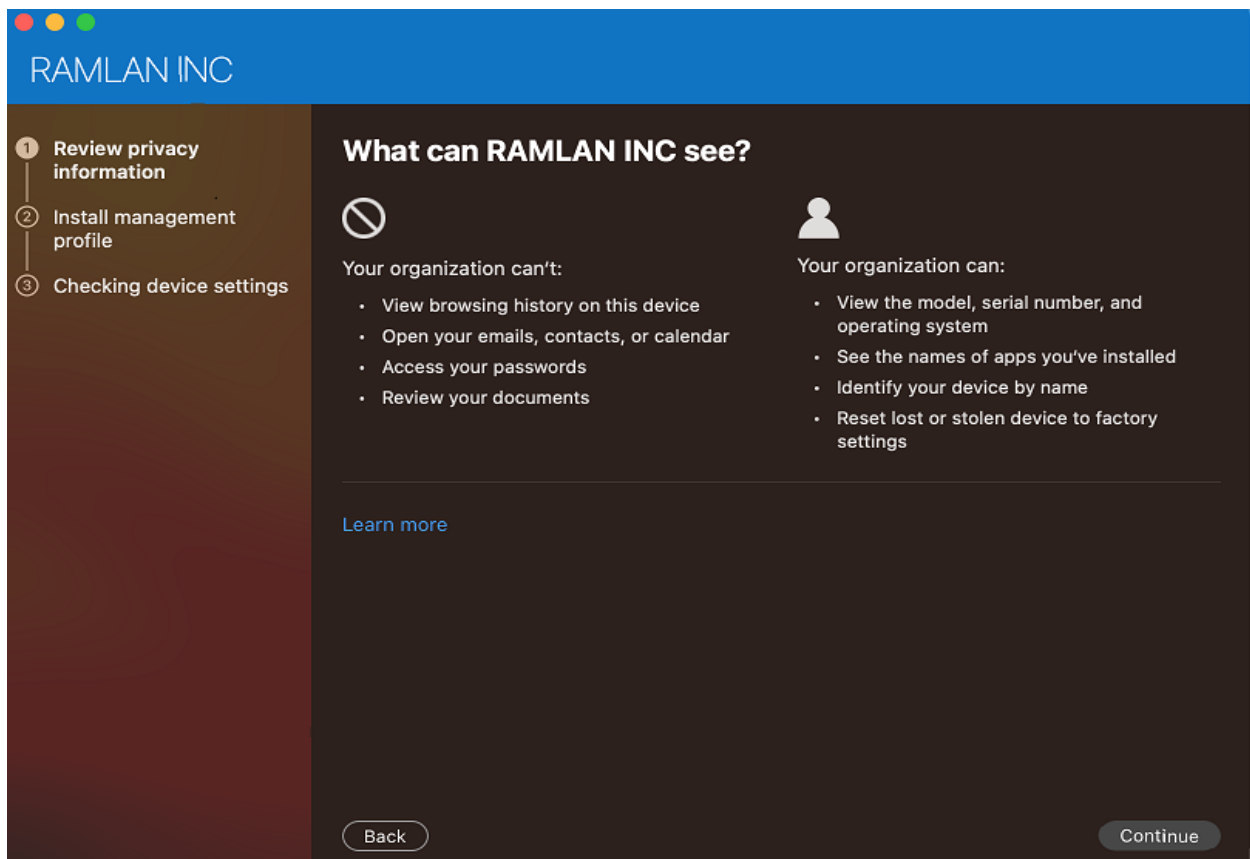
Set up RAMLAN INC access

Set up your device to access your email, devices, Wi-Fi, and apps for work.



Begin


[Postpone](#)




<

Profiles


Downloaded



Management Profile

 1 setting

Are you sure you want to install this profile?



Management Profile

Verified

Description

Install this profile to get access to your company apps

Signed

IOSProfileSigning.manage.microsoft.com

Received

Dec 28, 2022 at 5:28 PM

Settings

Profile Service Enrollment

fef.amsua0102.manage.microsoft.com

Details

Profile Service Enrollment


Description

Encrypted Profile Service

URL

https://fef.amsua0102.manage.microsoft.com/StatelessIOSEnrollmentService/DeviceEnrollment/ReportDeviceInfo2?client-request-id=c6692bef-be2b-4b24-976c-18638c9bc84d&id=925ea719-1580-4bed-b33e-[REDACTED]

Install...



Ignore

Cancel



Profiles

Profiles is trying to enroll you in a remote management (MDM) service.

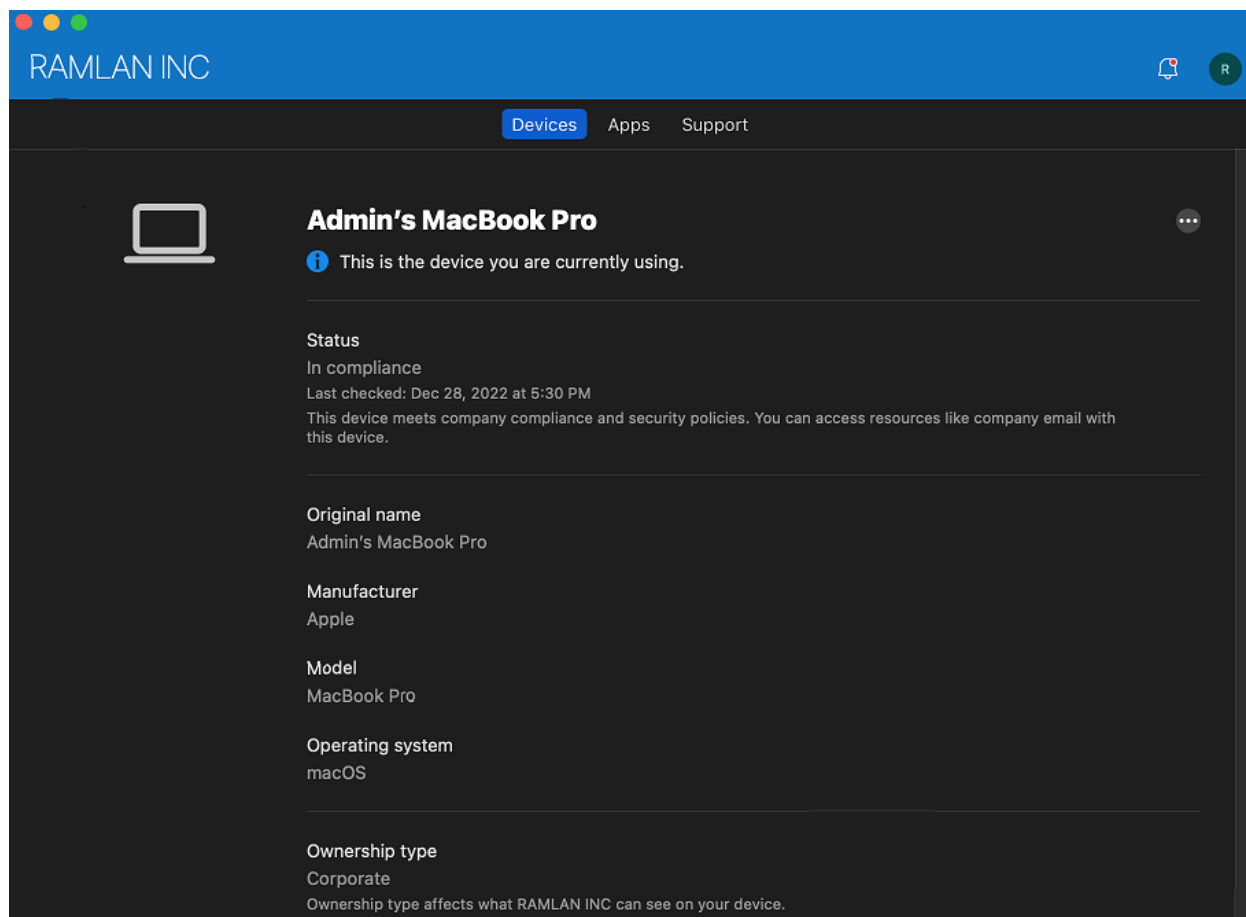
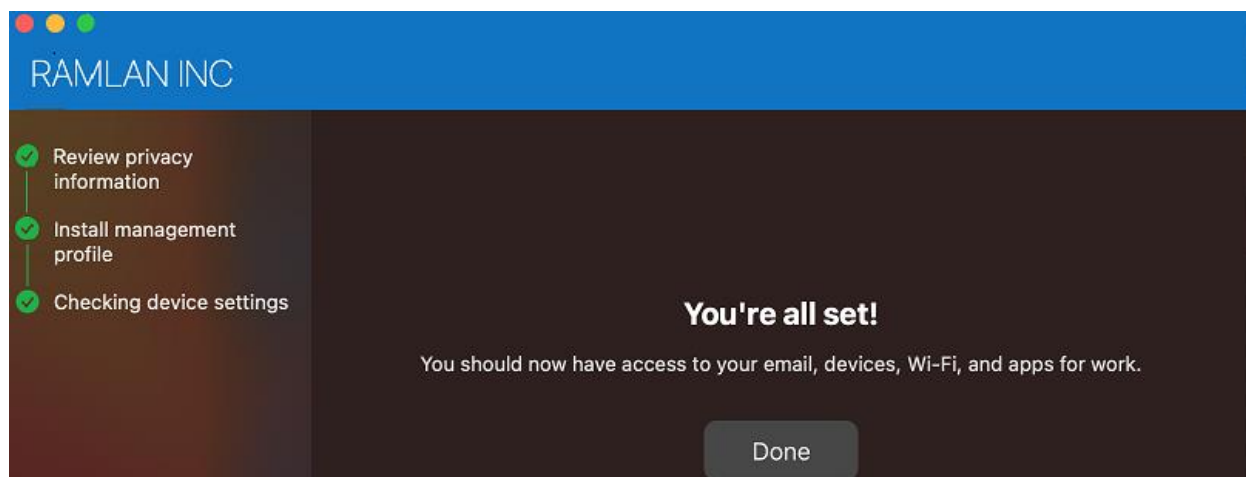
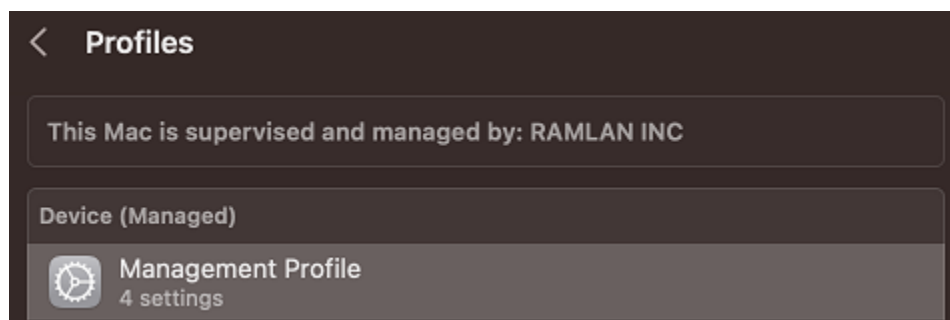
Enter your password to allow this.

Admin

••••••••

Cancel

Enroll



RAMLAN INC

<

R

ram@RAMLAN.CA

Change password

Sign out

i

You are signed in with a device enrollment manager account, which has limited capabilities

[Learn more](#)

Department

IT

Email

ram@ramlan.ca

RAMLAN INC

Devices

Apps

Support

Support

Contact

Ram

Call

647740

Email

ram@ramlan.ca

Website

INFOTECHRAM

Home > Devices | macOS

macOS | macOS devices

Search

Refresh Filter Columns Export Bulk Device Actions

macOS devices

macOS enrollment

macOS policies

Compliance policies

Configuration profiles

Shell scripts

Filters applied: OS

Search

Showing 1 to 1 of 1 records

< Previous

Page 1 of 1

Next >

| Device name | Managed by | Ownership | Compliance | OS | OS version | Last check-in | Primary user UPN |
|---------------------|------------|-----------|------------|-------|---------------|------------------------|------------------|
| Admin's MacBook Pro | Intune | Corporate | Compliant | macOS | 13.0 (22A380) | 12/28/2022, 5:36:27 PM | ram@RAMLAN.CA |

Retire

Wipe

Delete

Remote lock

Sync

Remove passcode

Restart

Shut down

Erase

Rotate FileVault recovery key

Rename device (corporate only)

Essentials

Device name

Management name

Ownership

Serial number

Phone number

Device manufacturer

Primary user

Enrolled by

Compliance

Operating system

Device model

Last check-in time

Remote assistance

See less

System

| | |
|--------------------------|--------------------------------------|
| Name | Admin's MacBook Pro |
| Management name | ram_MacOS_12/28/2022_10:29 PM |
| UDID | CD5BD1A6-BFBF-5C19-AB9D-9316CB8DC478 |
| Intune Device ID | 3d8ec0e7-649c-4094-93ac-[REDACTED] |
| Azure AD Device ID | 3d8ec0e7-649c-4094-93ac-[REDACTED] |
| Serial number | C02M314GFH05 |
| User approved enrollment | Yes |
| Enrollment profile | |

Operating system

| | |
|------------------------------------|---------------|
| Operating system | macOS |
| Operating system and build version | 13.0 (22A380) |
| Operating system language | |
| Operating system edition | |

Storage

| | |
|-----------------------|-----------|
| Total storage space | 500.00 GB |
| Free storage space | 468.00 GB |
| Total physical memory | |

System enclosure

| | |
|------------------------|----------------|
| IMEI | |
| MEID | |
| Manufacturer | Apple |
| Model | MacBook Pro |
| Product name | MacBookPro11,1 |
| Processor Architecture | x64 |
| Phone number | |
| Battery level | |



Device Enrollment

You have successfully enrolled Macbook Pro

[View details >](#)

RAMLAN INC
Ram
647740 [REDACTED]
ram@ramlan.ca

ENROLLMENT PROGRAM TOKENS – Let's continue with this one - <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios>

Enrollment program tokens ...

Apple Enrollment pipe

+ Add Columns

^ Essentials

Oldest sync : None

⚠ On iOS/iPadOS 14.5.x and 14.6.x, the Passcode and Touch ID Setup Assistant screens during device setup aren't working. If you use these settings in your policy, the settings aren't enforced. [Learn more.](#)

Apple enrollment programs help businesses and educational institutions remotely enroll Apple devices. Enrollment program tokens let Intune enroll devices registered with these programs. [Learn more about iOS/iPadOS.](#) [Learn more about MacOS.](#)

Home > Devices | Enroll devices > Enroll devices | Apple enrollment > Enrollment program tokens >

Add enrollment program token ...

Enrollment program tokens

1 Basics 2 Review + create

* I grant Microsoft permission to send both user and device information to Apple. [Learn more.](#)

☒ I agree.

* Download the Intune public key certificate required to create the token.

[Download your public key](#) ↓

I am going to use Apple Business Manager for lab use. First we have to enroll our business and get DUNS # from Dun&Bradstreet. Below is the request, I made today..

Here is the link to visit <https://www.dnb.com/ca-en/duns-number/lookup.html>

To use Apple Business Manager, use your key to download a token from the link below.

[Create a token via Apple Business Manager](#) ↗

Or

To use Apple School Manager, use your key to download a token from the link below. Microsoft School Data Sync will be required for some features. [Learn more.](#)

[Create a token via Apple School Manager](#) ↗

⊗

This Apple ID can't be used with Apple Business Manager.

Apple Business Manager can be used by Managers and Administrators with organizationally managed accounts. Sign in with your Managed Apple ID, or enroll your organization.

[Forgot Managed Apple ID or password?](#)

Not yet an Apple Business? [Enroll now.](#) ←

Receive a D&B D-U-N-S® Number

Please fill out the following form to have the requested D&B D-U-N-S Number emailed to you.

Infotechram Incorporated

[Redacted]

CA

Registration No: 8337527

Ram

Lan

ramlan@infotechram.cc

Submit

After we get DUNS # we can complete Apple Business Manager Organization Enrollment.

Enroll Your Organization

Enroll your organization to buy content, configure automatic device enrollment in your mobile device management (MDM) solution, create accounts for your employees, or sign up for Apple Business Essentials. Already enrolled? [Sign In](#)

Organization Info ⓘ

Infotechram Incorporated

202091555

+1 (647) 740-

www.infotechram.com

☒ I'm interested in Apple Business Essentials.

Time Zone & Language ⓘ

US/Eastern (GMT -05:00)



English (US) - English (US)



Your Details

Admin Strator

administrator@ramlan.ca

I T Admin

Verification Contact ⓘ

Ram Lan

ramlan@rogers.com

Director (Technology)

Cancel Continue

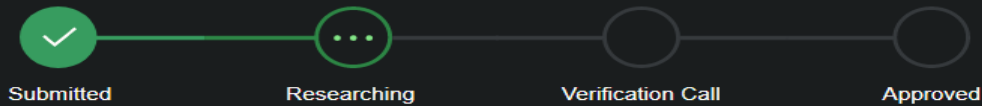
Enroll Your Organization

| | |
|------------------------------------------|-----------------------------------|
| Your Organization | Infotechram Incorporated |
| D-U-N-S Number ⓘ | 202091555 |
| Address ⓘ | 275 [REDACTED] Onta [REDACTED] |
| Phone Number | +1 (647) 740-[REDACTED] |
| Website | www.infotechram.com |
| Time Zone | US/Eastern (GMT -05:00) |
| Language | English (US) - English (US) |
| Interested in Apple Business Essentials? | Yes |
| Your Name | Admin Strator |
| Work Email Address | administrator@ramlan.ca |
| Role / Job Title | I T Admin |
| Verification Contact | Ram Lan |
| Work Email Address | ramlan@rogers.com |
| Role / Job Title | Director (Technology) |

Go Back Cancel Submit

Your Enrollment is in Review

We will notify you when your enrollment is approved. The review of your enrollment may take up to 5 days.

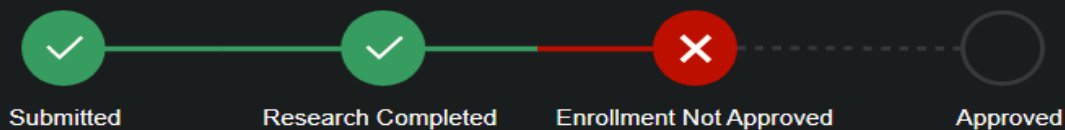


An AppleCare agent has been assigned to your enrollment request, and is researching your organization.

[Print Enrollment Details](#)

Your Enrollment is in Review

We will notify you when your enrollment is approved. The review of your enrollment may take up to 5 days.



Your enrollment could not be approved.

Thank you for your interest in Apple Business Manager. Unfortunately, we were unable to approve your request for enrollment.

Your enrollment contained invalid information.

As a result, we cannot use Apple Business Manager for home lab purpose. So, I am going to ignore this and use Apple Configurator for device enrollment (See above for more details).

ANDROID DEVICE SETUP

Login to Endpoint.microsoft.com -> Devices -> Android -> Android Enrollment

The screenshot shows the 'Android | Android enrollment' page in the Microsoft Endpoint Manager console. The breadcrumb trail is 'Home > Devices | Android > Android'. The left sidebar contains links for 'Overview', 'Android devices', 'Android enrollment' (selected), and 'Android policies' (with sub-links for 'Compliance policies' and 'Configuration profiles'). The main content area is titled 'General' and includes a search bar, a descriptive paragraph about selecting a management solution, and a 'Managed Google Play' section highlighted with a red box. This section contains a 'Managed Google Play' icon and the text 'Link your managed Google Play account to Intune.' Below this is an 'Android Enterprise' section with a 'Prerequisites' heading.

The screenshot shows the 'Managed Google Play' setup window. At the top, it says 'Managed Google Play' with a close button. Below is a 'Disconnect' link. The 'Essentials' section shows the status as 'Not Setup' with a red 'X' icon, and both 'Google account' and 'Organization' are listed as 'Not Available'. A message states: 'You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the steps below to enable Android enterprise enrollment. [Learn more.](#)' The first step is '1. I grant Microsoft permission to send both user and device information to Google. [Learn more.](#)' with a checked 'I agree.' checkbox. The second step is '2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.' At the bottom, a blue button with an orange arrow icon says 'Launch Google to connect now.'

I created a new Gmail account for the business and sign in. After that entered domain name for business registration.

The screenshot shows a promotional banner with a teal background. The main text reads 'Bring Android to Work' in large white font. Below it, in smaller white font, is 'Work smarter and faster with Android'. At the bottom left, there is a blue button with the text 'SIGN IN' in white capital letters.

Contact details

We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer data protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available right now.

Data Protection Officer

Name

Ram Lan

Email

ramlan@rogers.com

Phone

6477401956

Set up complete

Thanks for choosing Android enterprise.

[Complete Registration](#)

Managed Google Play

Android enrollment

 Disconnect

^ Essentials

Status

✓ Setup

Organization

RAMLAN.CA

Google account


rmlnndrd@gmail.com


Registration date


12/30/2022, 11:58:16 AM


Now we have various other options for enrollment

Enrollment Profiles

**Personally-owned devices with work profile**
Manage personal enrollments with work profiles.

**Corporate-owned dedicated devices**
Manage device owner enrollments for kiosk and task devices.

**Corporate-owned, fully managed user devices**
Manage device owner enrollments for user devices.

**Corporate-owned devices with work profile**
Manage enrollments for corporate devices with work profiles.

Android Open Source Project (AOSP)

Enrollment Profiles

**Corporate-owned, user-associated devices**
Manage corporate-owned user devices that were built from the Android open source code (AOSP) without Managed Google Services (GMS).


**Corporate-owned, userless devices**
Manage corporate-owned, userless devices that were built from the Android open source code (AOSP) without Google Mobile Services (GMS).

Android device administrator

Prerequisites

**Personal and corporate-owned devices with device administrator privileges**
Manage personal and corporate-owned devices using Android device administrator.

Personally Owned devices with work profile:

**Personally-owned devices with work profile**
Manage personal enrollments with work profiles.

Personally-owned devices with work profile

Android enrollment

Use personally-owned devices with work profiles to manage corporate data and apps on user-owned Android devices. By default, enrollment of personally-owned work profile devices is enabled, so no further action is needed. To configure platform restrictions and assign them to specific user groups, go to Enrollment restrictions.


ⓘ Block Android device administrator enrollment in Enrollment restrictions if you only want users to enroll with Android Enterprise personally-owned devices with work profiles. [Learn more about Enrollment restrictions.](#)

[Platform settings](#) [Review + save](#)

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more.](#)

| Type | Platform | versions | Personally owned | Device manufacturer |
|-----------------------------------|---------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------|----------------------------------------|
| Android Enterprise (work profile) | Allow Block | Allow min/max range: <input type="text"/> Min <input type="text"/> Max | Allow Block | <input type="text"/> Manufacturer name |
| Android device administrator | Allow Block | Allow min/max range: <input type="text"/> Min <input type="text"/> Max | Allow Block | <input type="text"/> Manufacturer name |
| iOS/iPadOS | Allow Block | Allow min/max range: <input type="text"/> Min <input type="text"/> Max | Allow Block | Restriction not supported |
| macOS | Allow Block | Restriction not supported | Allow Block | Restriction not supported |
| Windows (MDM) ⓘ | Allow Block | Allow min/max range: <input type="text"/> Min <input type="text"/> Max | Allow Block | Restriction not supported |

Corporate owned fully manager user devices:



Corporate-owned, fully managed user devices

Manage device owner enrollments for user devices.


Corporate-owned, fully managed user device...

✕

Android enrollment

Enable your end users to enroll corporate-owned devices. Copy the enrollment token provided to send to end users for enrolling user devices. [Learn more.](#)

Alternatively, you can configure auto provisioning for Android devices using Zero Touch. Configuration of this feature is not currently available in the Intune admin console but will be in the future.

[Configure an auto provisioning deployment on the Zero Touch portal.](#) 

Allow users to enroll corporate-owned user devices

☒ Yes ☐ No


Enrollment token

Highlight and copy the enrollment token below to send to your end users, or post it to your helpdesk site to enable end-users to enroll their devices. This single token is valid for all your users and will not expire. [Learn more.](#)


Corporate Device Enrollment Token

Scan the token below with your corporate device to enroll the device with your company. [Learn more.](#)

Token
RYTKWJSM



Corporate owned device with work profile:



Corporate-owned devices with work profile
Manage enrollments for corporate devices with work profiles.

Corporate-owned devices with work profile ...

Android enrollment

[+ Create profile](#) [Filter](#) [Columns](#) [Export](#)

Create and assign enrollment profiles and tokens for corporate-owned devices with work profiles. [Learn more.](#)

| Name |
|--------------------|
| No profiles found. |

Create profile ...

1 Basics **2 Review + create**

Name * ⓘ ✓

Description

Create profile ...


✓ Basics **2 Review + create**



Summary

Basics

| | |
|-------------|----------------------|
| Name | Android Devices Work |
| Description | -- |


[Previous](#) [Create](#)


 **Android Devices Work | Token** ...
Android enrollment

<<  Revoke token  Export

① Overview

Manage

 Properties

 **Token**


Android Devices Work

Use this token or QR code to enroll devices. [Learn more.](#)


Token creation date
12/30/22, 12:17 PM

Token
LMDRHUBY

Token as QR code



Corporate owned dedicated devices Kiosk:



Corporate-owned dedicated devices
Manage device owner enrollments for kiosk and task devices.

Home > Devices | Android > Android | Android enrollment > Corporate-owned dedicated devices >

Create profile ...

① Basics

② Review + create

Name * ⓘ

Android Device Kios ✓


Description

Optional

Token type * ⓘ

Corporate-owned dedicated device (default) ▼

Token expiration date * ⓘ

12/31/2023 | 

Create profile ...

✓ Basics

2 Review + create

Summary


Basics

| | |
|-----------------------|--------------------------------------------|
| Name | Android Device Kiosk |
| Description | -- |
| Token type | Corporate-owned dedicated device (default) |
| Token expiration date | 12/31/23 |

Previous

Create

Enrollment notifications:



Enrollment notifications (preview)

Send email or push notifications to devices after they enroll.

Android Enterprise Notifications

Android device administrator Notifications

Configure email and push notifications to be sent to users after they enroll. Notifications improve security by notifying users if someone enrolls a device with their credentials. IT admins can also use enrollment notifications to send users a welcome email or onboarding information following enrollment. [Learn more about enrollment notifications](#)

+

Create notifications

Create an enrollment notification ...

Enrollment Notifications

1 Basics

2 Notification settings

3 Scope tags

4 Assignments

5 Review + create

| | |
|-------------|------------------------------|
| Name * | Device Enrollment ✓ |
| Description | <div>Enter description</div> |
| Platform | Android Enterprise ▼ |

Configure the enrollment notifications you want to send to Android Enterprise devices. [Learn more about enrollment notifications](#)

^ Push Notification

Send Push Notification ☒ On

Subject * Device Enrollment ✓

Message * ⓘ

You have successfully enrolled work device

^ Email Notification

Send Email Notification ☒ On

Subject * Device Enrollment ✓

Raw HTML editor ⓘ

☒ On

Message * ⓘ

1 You have successfully enrolled work device

Email Header

Email header and footer settings for email notifications rely on Customization settings within the Tenant admin node in Endpoint manager. [Configure Customization settings](#)

Show company logo ☒ On

Tenant value

Email Footer

Show device details ☒ On

Tenant value

Device details:
OS Family: xxyyzz
OS version: XX.YY.ZZZ
Model: Model name
Serial number: aa11BBcC
Device name : John's PC

ⓘ This setting is turned off by default, as retrieving device details can cause a delay in email notifications being received.

[Learn more about configuring enrollment notifications](#)

| | |
|----------------------------------|-------------------------------------------------------------------------------------|
| Show company name | <input checked="" type="checkbox"/> On |
| Tenant value | <input type="text" value="RAMLAN INC"/> |
| Show contact information | <input checked="" type="checkbox"/> On |
| Tenant value | <div>Ram 6477401956 ram@ramlan.ca</div> |
| Show company portal website link | <input checked="" type="checkbox"/> On |
| Tenant value | <input type="text" value="https://portal.manage.microsoft.com/devices/{deviceId}"/> |

[Previous](#) [Next](#)

✓ Basics

✓ Notification settings

✓ Scope tags

4 **Assignments**

5 Review + create

Included groups

Add groups

Add all users

Groups

All users

Remove

Create an enrollment notification

Enrollment Notifications

✓ Basics

✓ Notification settings

✓ Scope tags

✓ Assignments

5 **Review + create**

Summary

Basics

Name

Device Enrollment

Description

--

Platform

androidForWork

Notification settings

Push Notification

Send Push Notification

On

Subject

Device Enrollment

Message

You have successfully enrolled work device

Email Notification

Send Email Notification

On

Subject

Device Enrollment

Message

You have successfully enrolled work device

Email Header

Show company logo

On

Email Footer

| | |
|----------------------------------|----|
| Show device details | On |
| Show company name | On |
| Show contact information | On |
| Show company portal website link | On |

Scope tags

Default

Assignments

Included groups All users

Previous

Create

| Priority | Name | Notification Type | Assigned | Date Modified |
|----------|-------------------|-------------------|----------|--------------------|
| 1 | Device Enrollment | Email, Push | Yes | 12/30/22, 12:36 PM |

Enrollment notifications (preview) ...

Android enrollment

Android Enterprise Notifications

Android device administrator Notifications

Configure email and push notifications to be sent to users after they enroll. Notifications improve security by notifying users if someone enrolls a device with their credentials. IT admins can also use enrollment notifications to send users a welcome email or onboarding information following enrollment. [Learn more about enrollment notifications](#)

+ Create notifications

Create an enrollment notification ...

Enrollment Notifications

1 Basics 2 Notification settings 3 Scope tags 4 Assignments 5 Review + create

Name *

User Enrolled Android Device ✓

Description

Enter description

Platform

Android device administrator

✓ Basics 2 Notification settings 3 Scope tags 4 Assignments 5 Review + create

Configure the enrollment notifications you want to send to Android device administrator devices. [Learn more about enrollment notifications](#)

Push Notification

Send Push Notification

Off

Email Notification

Send Email Notification

On

Subject *

Device Enrolled ✓

Raw HTML editor ⓘ

On

Message * ⓘ

1 just completed enrolling a device to corporate

Email Header

Email header and footer settings for email notifications rely on Customization settings within the Tenant admin node in Endpoint manager. [Configure Customization settings](#)

Show company logo ☐ Off

Tenant value

Email Footer

Show device details ☒ On

Tenant value

Device details:
OS Family: xyyzz
OS version: XX.YY.ZZZ
Model: Model name
Serial number: aa11BBcC
Device name : John's PC

i This setting is turned off by default, as retrieving device details can cause a delay in email notifications being received.

[Learn more about configuring enrollment notifications](#)

Show company name ☒ On

Tenant value

RAMLAN INC

Show contact information ☒ On

Tenant value

Ram
6477401956
ram@ramlan.ca

Show company portal website link ☐ Off

Tenant value

<https://portal.manage.microsoft.com/devices/{deviceId}>

[Previous](#)

[Next](#)

Create an enrollment notification

Enrollment Notifications

☒ Basics ☒ Notification settings ☒ Scope tags **☒ 4 Assignments** ☐ 5 Review + create

Included groups

 Add groups  Add all users

Groups

All users [Remove](#)

Create an enrollment notification ...

Enrollment Notifications

✓ Basics ✓ Notification settings ✓ Scope tags ✓ Assignments 5 Review + create

Summary

Basics

| | |
|-------------|------------------------------|
| Name | User Enrolled Android Device |
| Description | -- |
| Platform | android |

Notification settings

Push Notification

| | |
|------------------------|-----|
| Send Push Notification | Off |
|------------------------|-----|

Email Notification

| | |
|-------------------------|-----------------------------------------------------|
| Send Email Notification | On |
| Subject | Device Enrolled |
| Message | User just completed enrolling a device to corporate |

Email Header

| | |
|-------------------|-----|
| Show company logo | Off |
|-------------------|-----|

Email Footer

| | |
|---------------------|----|
| Show device details | On |
|---------------------|----|

Email Footer

| | |
|----------------------------------|-----|
| Show device details | On |
| Show company name | On |
| Show contact information | On |
| Show company portal website link | Off |

Scope tags

Default

Assignments

| | |
|-----------------|-----------|
| Included groups | All users |
|-----------------|-----------|

[Previous](#)

[Create](#)

| Priority | Name | Notification Type | Assigned | Date Modified |
|----------|------------------------------|-------------------|----------|--------------------|
| 1 | User Enrolled Android Device | Email | Yes | 12/30/22, 12:40 PM |

Android device administrator

Prerequisites



Personal and corporate-owned devices with device administrator privileges

Manage personal and corporate-owned devices using Android device administrator.

Personal and corporate-owned devices with device administrator privileges

⚠️ Android's device administrator capabilities have been superseded by Android Enterprise. As a result, we recommend using Android Enterprise if it's supported in your country/region. [Learn more.](#) →

This setting enables Android's older management method, device administrator, to manage corporate data and apps. You can still manage your devices with device administrator, but we recommend that you switch to Android Enterprise for the most up-to-date and secure features. [Learn more.](#)

You can further configure platform settings and assign them to specific user groups in [Enrollment Restrictions](#). For example, you can use Enrollment Restrictions to force devices to enroll with device administrator in regions that do not support Android Enterprise.

☐ Use device administrator to manage devices. By enabling this feature, you grant Microsoft permission to send both user and device information to Google. [Learn more.](#)

Are you sure want to enable device administrator management?

Android's device administrator capabilities have been superseded by Android Enterprise. For continuous device management and security, Intune recommends using Android Enterprise for all new enrollments.

Use anyway?

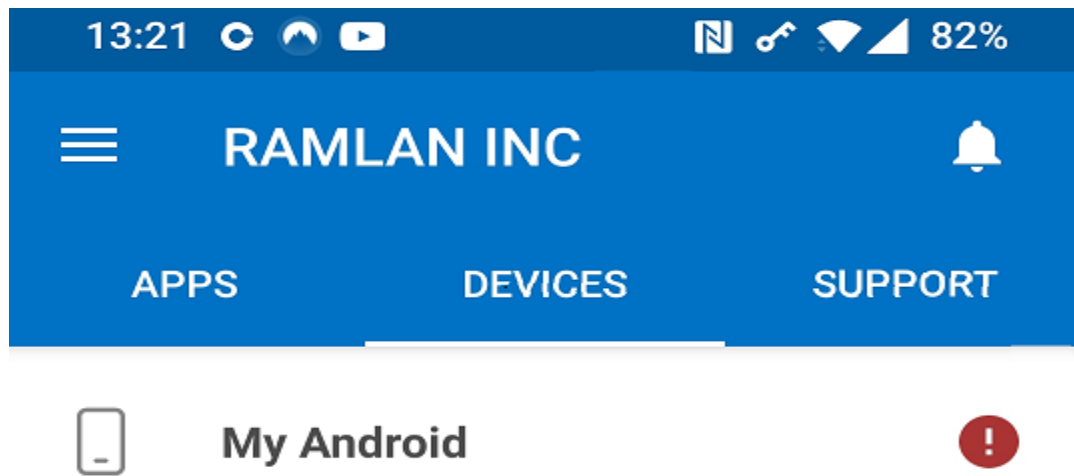
Yes

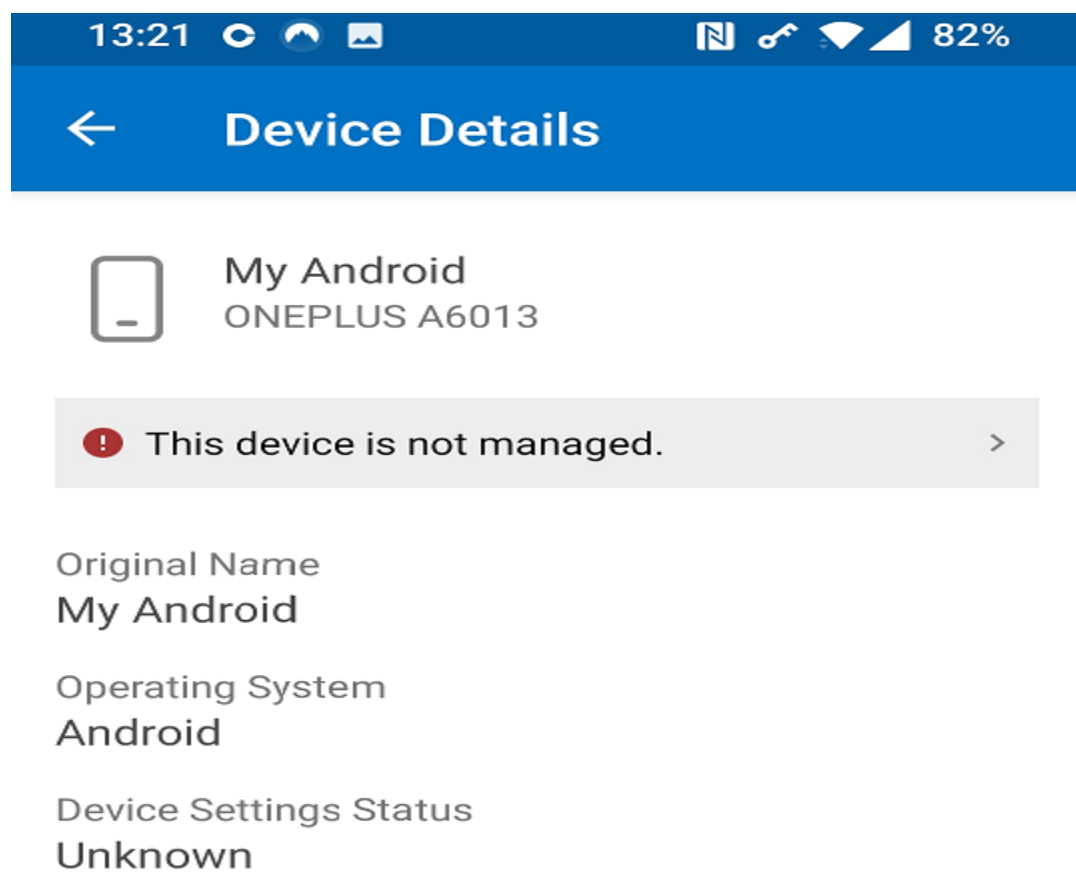
No

We have completed most of the configuration for Android device enrollment. Now it is time to test. I am using personal OnePlus 6 Android phone.

ENROLLING ANDROID DEVICE - <https://learn.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-company-portal>

Open Company Portal -> Login with corporate credentials -> Click Devices -> Select the device to enroll





RAMLAN INC Access Setup

Let's set up your device to access your email, Wi-Fi, and apps for work. You'll also be able to manage your devices.

- 1 Get your device managed
- 2 Update device settings

[Learn more about device setup](#)

RAMLAN INC



RAMLAN INC cares about your privacy.

While setting up your device, you will see some Android system screens requesting permissions to help your company secure your device.

**RAMLAN INC can never see:**

- Call and Web history
- Location
- Email and text messages
- Contacts
- Passwords
- Calendar
- Camera roll

**RAMLAN INC may see:**

- Model
- Serial number
- Operating system
- App names
- Owner

13:22



81%

RAMLAN INC



What's next?

1. **Allow** permission to make and manage phone calls

Your Android device needs this permission to report your device's serial number and a cellular antenna ID. RAMLAN INC and the Company Portal app cannot make phone calls with this information.

2. **Activate** Android device administrator

Android device administrator allows RAMLAN INC to apply required settings to your device.

[Learn more about permissions](#)



**Allow Company Portal to
make and manage phone
calls?**

ALLOW

DON'T ALLOW

13:22



81%

< **Company Portal**



Company Portal

Company Portal

Activating this admin app will allow the app Company Portal to perform the following operations:

Erase all data

Erase the phone's data without warning by performing a factory data reset.

Change the screen lock

Change the screen lock.

Set password rules

Control the length and the characters allowed in screen lock passwords and PINs.

13:23



81%

RAMLAN INC



Registering your device...

This may take a few minutes... You can use other apps but you might not have access to RAMLAN INC resources yet.

13:24



81%

RAMLAN INC



You're all set!

You should have access to your email, Wi-Fi, and apps for work within a couple of minutes.



Get your device managed



Update device settings

[Learn more about device setup](#)

13:24

81%

RAMLAN INC

1

APPS

DEVICES

SUPPORT

ram_Android_12/30/2022_6:23 PM

13:24

81%

Device Details

ram_Android_12/30/2022_6:23 PM

ONEPLUS A6013

This is the device you're currently using.

Original Name

ram_Android_12/30/2022_6:23 PM

Operating System

Android

Ownership Type

Corporate

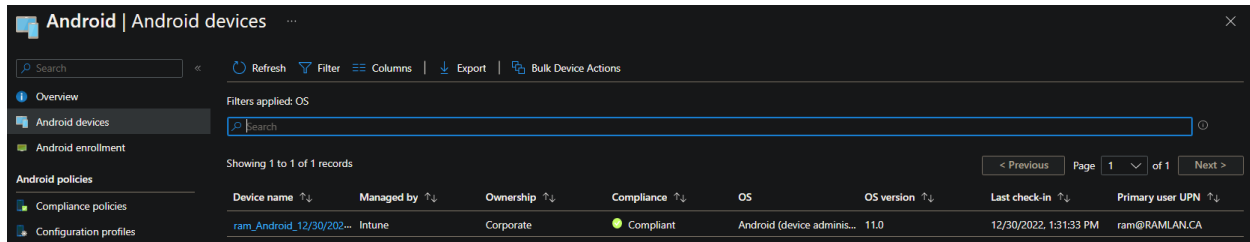
[Learn More](#)

Device Settings Status

In Compliance

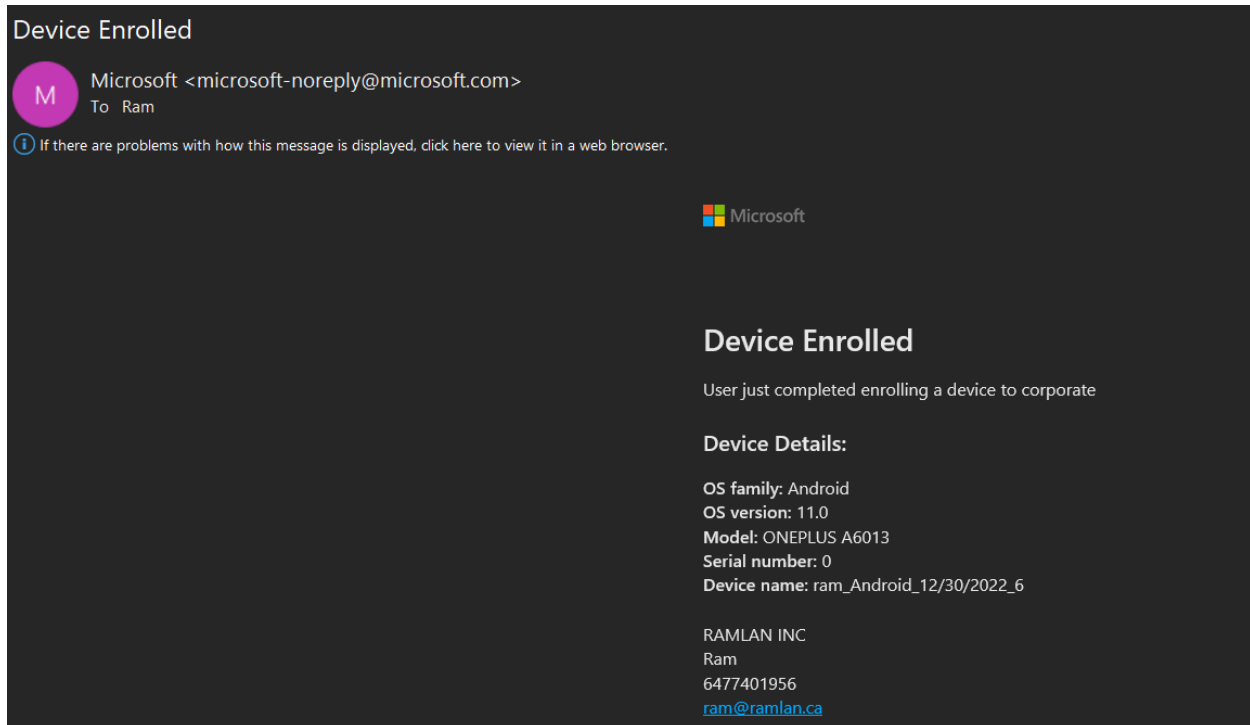
Last checked: December 30, 13:23

We can see it is enrolled within Intune.



| Device name | Managed by | Ownership | Compliance | OS | OS version | Last check-in | Primary user UPN |
|--------------------------|------------|-----------|------------|----------------------------|------------|------------------------|------------------|
| ram_Android_12/30/2022_6 | Intune | Corporate | Compliant | Android (device adminis... | 11.0 | 12/30/2022, 1:31:33 PM | ram@RAMLAN.CA |

Received email confirmation addressed to Android Device Administrator



Device Enrolled

Microsoft <microsoft-noreply@microsoft.com>
To: Ram

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft

Device Enrolled

User just completed enrolling a device to corporate

Device Details:

OS family: Android
OS version: 11.0
Model: ONEPLUS A6013
Serial number: 0
Device name: ram_Android_12/30/2022_6

RAMLAN INC
Ram
6477401956
ram@ramlan.ca

Now we have a fully functioning MDM for Windows, iPhone, iPad, MacOS and Android devices.

Thanks

Ram

30th Dec 2022