



## **Beyond Impact Information Technology**

---

# **Microsoft Endpoint Manager / Intune Implementation**

**Release for Production**

**Document Version 2.0**

## Contents

<b>1 Overview .....</b>	<b>4</b>
1.1 Revision History .....	4
1.2 Applicability .....	4
1.3 Required Software.....	4
<i>Introduction.....</i>	<i>4</i>
<i>Intended Audience .....</i>	<i>4</i>
<i>Overview .....</i>	<i>5</i>
<i>Scope.....</i>	<i>5</i>
<i>Out of scope .....</i>	<i>5</i>
<i>Dependencies.....</i>	<i>5</i>
<i>Time Line .....</i>	<i>5</i>
<i>Known Issues.....</i>	<i>5</i>
<i>Content.....</i>	<i>5</i>
<b>2 Initial Tenant and Microsoft Endpoint Manager Configuration.....</b>	<b>6</b>
2.1 Configure MDM Authority .....	6
2.2 Configure Company Portal .....	6
2.3 Test MDM DNS Records .....	9
2.4 Configure Device Enrollment Restrictions .....	10
2.5 Configure Device Enrollment .....	11
2.6 Dynamic Device Groups .....	16
2.7 Device Cleanup Rules .....	17
2.8 Creating Device Categories .....	18
<b>3 Mobile Device Management (MDM) Configuration.....</b>	<b>20</b>
3.1 Intune Device Profiles – Configuration Profiles .....	20
3.2 Intune Compliance Policies and Conditional Access .....	21
3.3 Create Intune Device Categories.....	22
3.4 Configure Personal or Corporate Identifiers.....	23
<b>4 Application Management and Software Update Policies.....</b>	<b>25</b>
4.1 Deploy Client Apps to Managed Intune Devices.....	25
4.2 App Protection Policies (MAM).....	27
4.3 Software Update Policies .....	29
<b>5 Enroll Devices into Intune .....</b>	<b>32</b>
5.1 Windows 10.....	32
5.2 iOS and Android .....	40



## 1 Overview

### 1.1 Revision History

Version	Change <i>(Topic, Section, Page)</i>	Author(s)	Reviewer(s)	Date
1.0	Initial Draft	Steve Buckner		8/1/22
2.0	Final Draft	Steve Buckner		8/2/22
4.0	Final	Steve Buckner		8/16/22

### 1.2 Applicability

Business/Region affected	Global
Requestor/PIF number	N/A
WTS Entry	N/A
Platform	MEM – Azure, and Microsoft 365
Operating system version	N/A
Security model tier	N/A
CAP	N/A
VTM ID	N/A
Software location/package name	N/A

### 1.3 Required Software

- Web Browser
  - Browser of your choice

#### Introduction

This document provides a general overview of the steps taken to successfully implement Microsoft Endpoint Manager Windows (MEM).

#### Intended Audience

Internal Operations Systems Group



## Overview

Microsoft Intune / Microsoft Endpoint Manager (MEM) is a Microsoft cloud-based management solution that provides for mobile device and operating system management. It aims to provide Unified Endpoint Management of both corporate and BYOD devices in a way that protects corporate data. It extends some of the "on-premises" functionality of Microsoft System Center Configuration Manager to the Windows Azure cloud.

The test tenant used for this document has been configured as follows:

Licenses; Microsoft 365 E5

Domain: BeyondImpactLLC.com

Azure Active Directory Only. On-premises DCs, Azure AD Connect Services being utilized, Hybrid.

Devices; Windows 10, Apple iPhone. Apple iPad Mini, Android 8

Intune as a stand-alone MDM solution

## Scope

All Corporate Environment

### Out of scope

All Production Environment

### Dependencies

None

### Time Line

9/2/2022

### Known Issues

None

### Content


See Below

## 2.1 Download and Install Configure MDM Authority

The mobile device management (MDM) authority setting determines how you manage your devices. As an IT admin, you must set an MDM authority before users can enroll devices for management.

Login to the Microsoft Endpoint Manager Admin Center ( <https://endpoint.microsoft.com> ) and set the MDM authority. Since this is a stand-alone MDM solution, we will want to verify that our MDM Authority is set to Microsoft Intune.

Click Tenant Administration / Tenant Status and verify that Microsoft Intune is set as the MDM authority.

<u>Tenant details</u>	Connector status	Service health and message center	
Tenant name BeyondImpactLLC.com	MDM authority Microsoft Intune 	Service release 2207	Total licensed users 38
Tenant location North America 0501	Account status Active	Total enrolled devices 4	Total Intune licenses 125

**Best Practices:** You should create all management settings and configurations, as well as deployments, shortly after the change to the MDM authority has completed. This helps ensure that devices are protected and actively managed during the interim period.

## 2.2 Configure Company Portal

### Configure Portal Terms and Conditions

As an Intune admin, you can require that users accept your company's terms and conditions before using the Company Portal to enroll devices and access resources like company apps and email.

**Beyond Impact Terms and Conditions | Properties** ...

Terms and conditions

Search (Ctrl+/) <<

Overview

**Manage**

Properties

**Monitor**

Acceptance Reporting

**Basics** [Edit](#)

Name: Beyond Impact Terms and Conditions

Description: Beyond Impact Terms and Conditions

**Terms** [Edit](#)

Title: Beyond Impact Terms and Conditions

Terms and conditions: These terms and conditions apply to all employees, contractors, students, volunteers and consultants of Beyond Impact LLC who use MS Intune to access Beyond Impact LLC - data & applications on their mobile devices.

Summary of terms: These terms and conditions apply to all employees, contractors, students, volunteers and consultants of Beyond Impact LLC who use MS Intune to access Beyond Impact LLC - data & applications on their mobile devices.

**Assignments** [Edit](#)

Included groups: All users

**Scope tags** [Edit](#)

Default



**This needs to be updated.**

**Best Practices:** Be sure to ask for the necessary department for the proper Terms and Conditions verbiage

**Customization and Branding in Azure Active Directory**


## Edit company branding

Azure Active Directory

 Save  Discard

---


Sign-in page background image  
Image size: 1920x1080px  
File size: <300KB  
File type: PNG, JPG, or JPEG ⓘ



[Remove](#)

---

Banner logo  
Image size: 280x60px  
File size: 10KB  
File type: Transparent PNG, JPG, or JPEG ⓘ



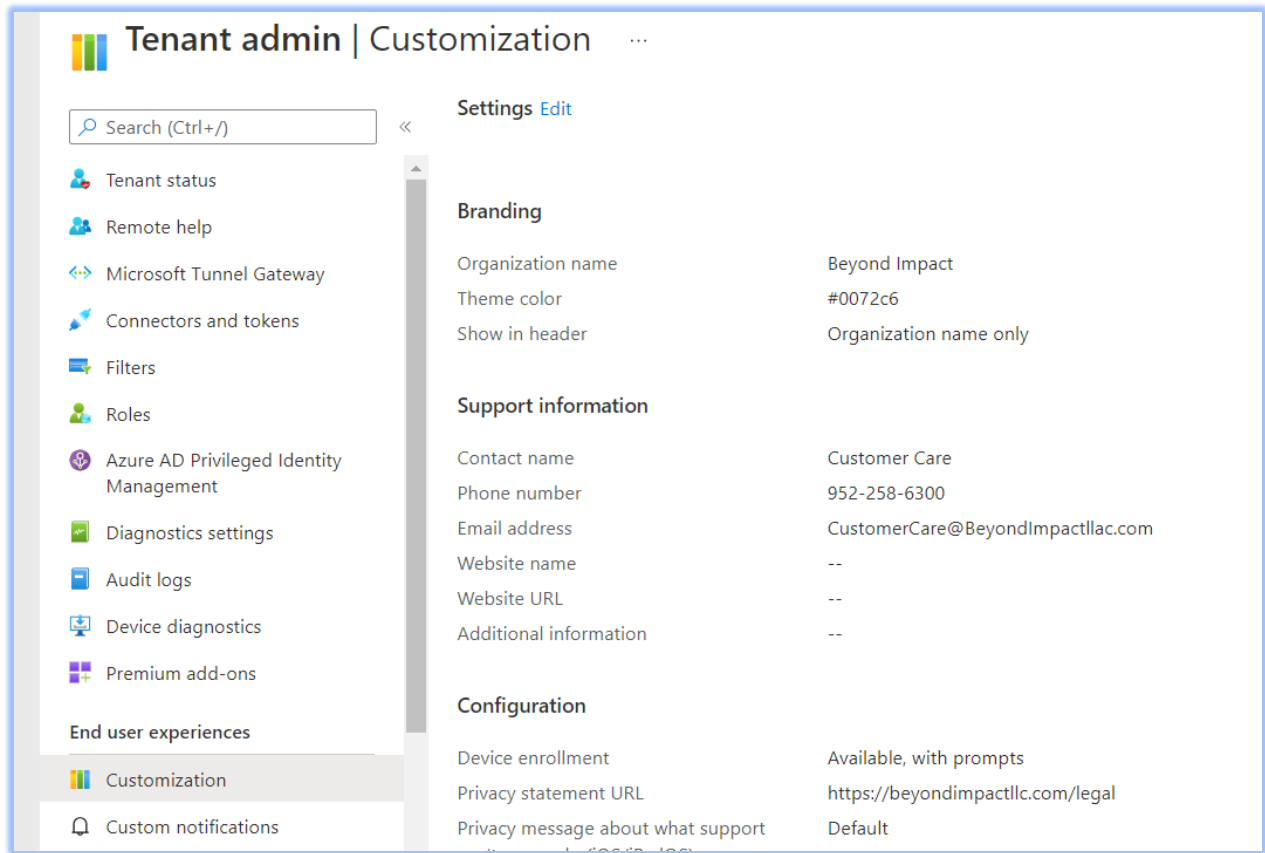
[Remove](#)

---

Username hint ⓘ

### Customization and Branding in the MEM Admin Console





**Best Practices:** Use your organization's logo and custom color schemes to provide a consistent look-and-feel on your Azure Active Directory (Azure AD) sign-in pages. Your sign-in pages appear when users sign into your organization's web-based apps, such as Microsoft 365, which uses Azure AD as your identity provider.

### 2.3 Test MDM DNS Records

To simplify enrollment, create a domain name server (DNS) alias (CNAME record type) that redirects enrollment requests to Intune servers. Otherwise, users trying to connect to Intune must enter the Intune server name during enrollment. You will want to test that the CNAME record is in place.

### CNAME Validation ✕

Windows enrollment

Configuring a CNAME in your DNS saves your users from having to enter the address of the MDM server when enrolling their Windows devices. [Learn more.](#)

After configuring the CNAME resource records in your DNS, enter the corresponding domain here to confirm that it has been configured correctly. Changes to DNS records might take up to 72 hours to propagate.

Domain

 ✓

**Test**

✓ CNAME for beyondimpactllc.com is configured correctly.

**Best Practices:** Intune conditional access requires devices to be registered, also called "workplace joined". If you plan to use conditional access, you should also configure the Enterprise Registration CNAME for each company name you have.

## 2.4 Configure Device Enrollment Restrictions

You should set the types of devices that can enroll, accomplished by simply choosing to Block or Allow a given device type platform like Android or iOS for instance. As for the maximum number of devices restriction option, you define how many devices a single user is allowed to enroll, for instance 7 devices.

### All Users ...

Search (Ctrl+/) « ^ Essentials

**Overview**

Created : 12/31/69, 7:00 PM

Last modified : 08/02/22, 11:23 AM

Device limit : 7

Assigned to : [All devices.](#)

Platform settings 2 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 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
Android Enterprise (work profile)	<input type="radio"/> Allow <input type="radio"/> Block	Allow min/max range: Min <input checked="" type="checkbox"/> Max <input checked="" type="checkbox"/>	<input type="radio"/> Allow <input type="radio"/> Block
Android device administrator	<input type="radio"/> Allow <input checked="" type="radio"/> Block	Allow min/max range: Min <input type="checkbox"/> Max <input type="checkbox"/>	<input type="radio"/> Allow <input type="radio"/> Block
iOS/iPadOS	<input type="radio"/> Allow <input type="radio"/> Block	Allow min/max range: Min <input checked="" type="checkbox"/> Max <input checked="" type="checkbox"/>	<input type="radio"/> Allow <input type="radio"/> Block
macOS	<input type="radio"/> Allow <input type="radio"/> Block	Restriction not supported	<input type="radio"/> Allow <input type="radio"/> Block
Windows (MDM)	<input type="radio"/> Allow <input type="radio"/> Block	Allow min/max range: Min <input checked="" type="checkbox"/> Max <input checked="" type="checkbox"/>	<input type="radio"/> Allow <input type="radio"/> Block

Devices | Enrollment device platform restrictions

Search (Ctrl+F)

- Update settings for Windows 10 and later
- Feature updates for Windows 10 and later (preview)
- Quality updates for Windows 10 and later (preview)
- Update policies for iOS/iPadOS
- Enrollment device limit restrictions
- Enrollment device platform restrictions**
- eSIM cellular profiles (preview)

Android restrictions | **Windows restrictions** | MacOS restrictions | iOS restrictions

+ Create restriction

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restriction may be edited, but not deleted. [Learn more](#).

Device type restrictions

Define which platforms, versions, and management types can enroll.

Priority	Name	Assigned
Default	All Users	Yes

**Best Practices:** Use enrollment restrictions to better control mobile devices Microsoft Intune license holders can enroll up to five devices. It is usually preferable for IT to put some restrictions on those devices. This is a common best practice because organizations often do not support specific device platforms or manufacturers.

## 2.5 Configure Device Enrollment

### Configure policies for device enrollment settings in Azure Active Directory

Next you can users to enroll Windows devices by signing in with their work or school account.

### Configure / Verify Windows Enrollment Settings in MEM

Automatic enrollment lets users enroll their Windows 10 devices in Intune. To enroll, users add their work account to their personally owned devices or join corporate-owned devices to Azure Active Directory. In the background, the device registers and joins Azure Active Directory. Once registered, the device is managed with Intune.

Home > Beyond Impact 2.0 LLC | Mobility (MDM and MAM) >

## Configure

Microsoft Intune

Save Discard Delete

MDM user scope  None  Some  All

Groups 1 group selected

MDM terms of use URL  ✓

MDM discovery URL  ✓

MDM compliance URL  ✓

Restore default MDM URLs

MAM user scope  None  Some  All

Groups 1 group selected

MAM terms of use URL  ✓

MAM discovery URL  ✓

MAM compliance URL  ✓

Restore default MAM URLs

### Select groups

Search

- AI 1:1 Agenda Items  
11AgendaItems@BeyondImpactLLC.com
- SD 2019 SNI DR Failover Test  
2019SNIDRFailoverTest@BeyondImpactLLC.com
- AD ADSyncAdmins

Selected groups

- IM Intune Managed Users

Select

Updated 8/2/22

### Configure ...

Microsoft Intune

Save Discard Delete

MDM user scope ⓘ None Some All

MDM terms of use URL ⓘ  ✓

MDM discovery URL ⓘ  ✓

MDM compliance URL ⓘ  ✓

Restore default MDM URLs

MAM user scope ⓘ None Some All

MAM terms of use URL ⓘ  ✓

MAM discovery URL ⓘ  ✓

MAM compliance URL ⓘ  ✓

**Enrollment status** Enrollment alerts Compliance sta

**Intune enrolled devices** 8/2/22 - 14:10

LAST UPDATED 8/02/22, 2:39 PM

Platform	Devices
Windows	4
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
<b>Total</b>	<b>4</b>

**Best Practices:** For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled.

If your intent is to enable automatic enrollment for Windows BYOD devices to an MDM: configure the MDM user scope to All (or Some, and specify a group) and configure the MAM user scope to None (or Some, and specify a group – ensuring that users are not members of a group targeted by both MDM and MAM user scopes).

For corporate devices, the MDM user scope takes precedence if both MDM and MAM user scopes are enabled. The device will get automatically enrolled in the configured MDM.

### IOS - Configure MDM Push Certificate

Home > Devices > Enroll devices

**Enroll devices | Apple enrollment**

Search (Ctrl+/) <<

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

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple push certificates 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  
Manage Automated Apple Business Manager

**Configure MDM Push Certificate**

Delete

Essentials

Status	Active	Days until expiration	365
Last updated	11/11/2020	Expiration	11/11/2021
Apple ID	steve@microsofttraininglab.com	Subject ID	com.apple.mgmt.Ext
Serial number	2D13FE5BAF708C8E		

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. Mo
  - I agree.

## Apple Push Certificates Portal

**Confirmation**

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

Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Nov 11, 2021

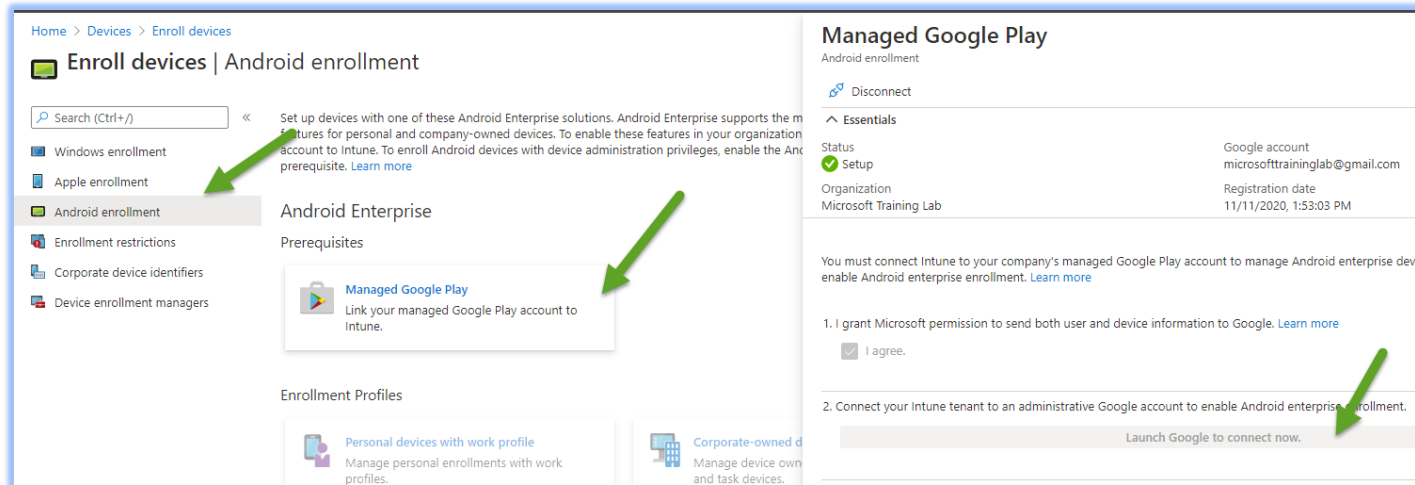
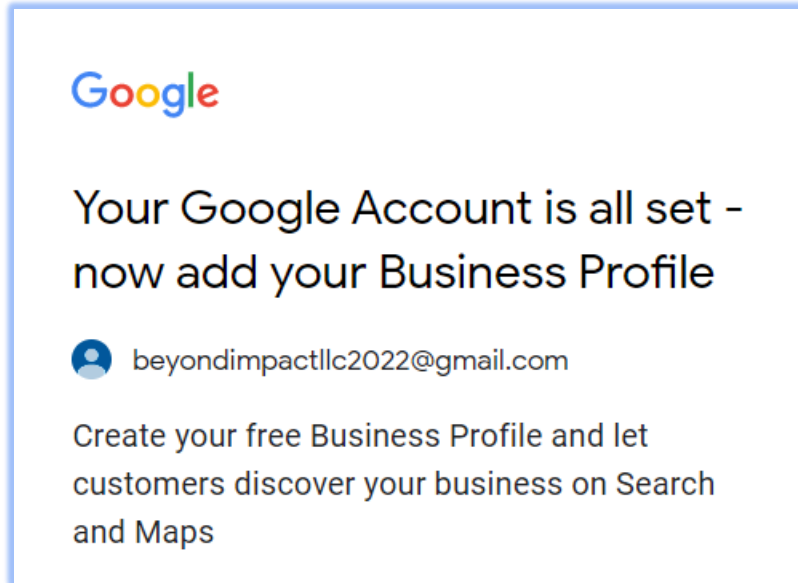
[Manage Certificates](#) [Download](#)

# BEYOND IMPACT

PEOPLE WHO SOLVE

**Best Practices:** Your Apple MDM push certificate appears Active and has 365 days until expiration.

## Android – Google Play Store



**Bring Your Own Device (BYOD)** - Company Managed Work Device - Work Profile totally separate and isolated from personal data

**Device Owned (COD)** - Fully managed by Corp MDM

**Corporate Owned Single User (COSU)** - Kiosk mode - has limited access to underlying OS

**Corporate Owned Personally Enabled (COPE)** - Not supported by Intune

**Best Practices:** There may be an instance where you may want to disable / block the use of Android Device Administrator by configuring an Enrollment Restriction.

## Android Work Profile – BYOD – Android Enterprise

Setting up a Bring Your Own Device (BYOD) - Company Managed Work Device - Work Profile totally separate and isolated from personal information.

### 2.6 Dynamic Device Groups

You can automatically add devices to device groups based on categories that you define. In this example I will create 3 groups based upon the Operating Systems type: one for Windows, IOS, and Android devices. This makes it far easier to administer devices.

#### Create Azure Active Directory Dynamic Device Security Groups – based on OS Type (OST)

Home > Groups >

## New Group

Group type \* ⓘ  
Security

Group name \* ⓘ  
Android Devices

Group description ⓘ  
Android Devices

Azure AD roles can be assigned to the group (Preview) ⓘ  
Yes **No**

Membership type \* ⓘ  
Dynamic Device

Owners  
No owners selected

Dynamic device members \* ⓘ  
Add dynamic query



**Dynamic membership rules**

Save | Discard | Got feedback?

Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or: And | Property: deviceOSType | Operator: Contains | Value: android

+ Add expression

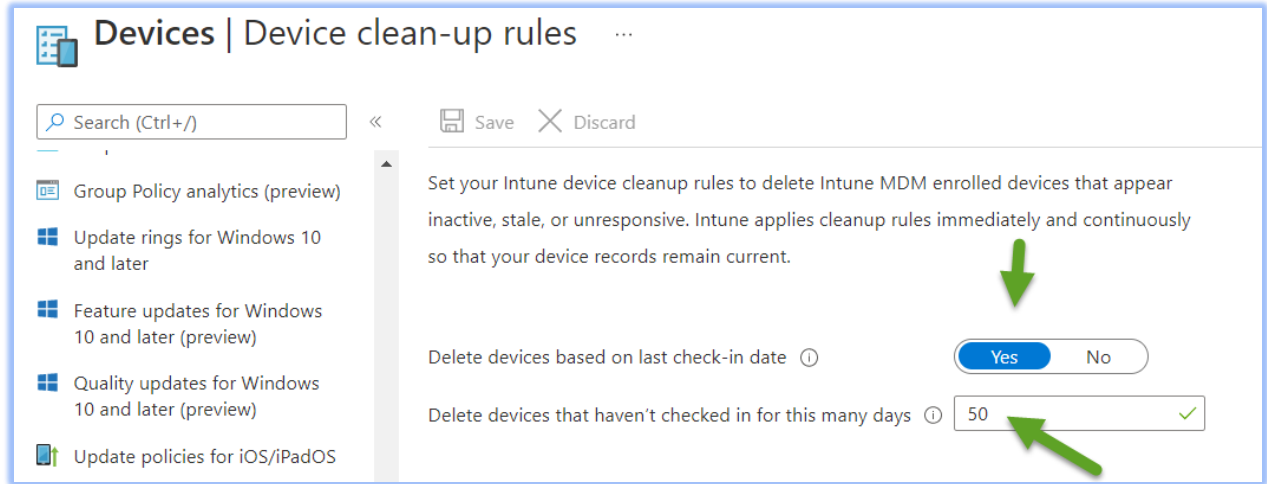
**Rule syntax**  
(device.deviceOSType -contains "android")

Name	Object Id	Group Type	Membership Type
<input type="checkbox"/> AC All Company	3fd0d9d2-4c94-465c-9a46-ce43f46...	Microsoft 365	Assigned
<input type="checkbox"/> AD Android Devices	44029dc7-6ba6-428b-b2ae-2a7236...	Security	Dynamic
<input type="checkbox"/> AD Apple Devices	ee124981-7479-494d-84b5-2196fd...	Security	Dynamic
<input type="checkbox"/> m microsofttraininglab27	6a27e819-2e48-46cc-89aa-ed9ec13...	Microsoft 365	Assigned
<input type="checkbox"/> WD Windows Devices	d2017051-ce72-4a40-b00a-1d2aa9...	Security	Dynamic

Best Practices:

## 2.7 Device Cleanup Rules

We often get a lot of inactive and stale Intune records due to the nature of test device enrollments. We want to keep our Intune environment and reports current by cleaning up these stale devices. With Intune device cleanup, we can configure the automatic cleanup rule which cleans up devices that are inactive, orphaned, or obsolete and have not checked in recently.



**Best Practices:** Once this rule is enabled, Intune will automatically remove devices that haven't checked in for the number of days you set. It is best to check with the client to get the desired "days" setting based on their device check-in behavior.

## 2.8 Creating Device Categories

A device category is used to prompt users to answer what type of device they have during enrollment.

Category	↑↓	Description
Laptop		Windows Laptop
Desktop		Windows Desktop
Apple iPhone		Apple iPhone
Apple iPad		Apple iPad
Android Device		Android Device Phone or Tablet

**Best Practices:** What about already enrolled devices, will they also get this option to select a category? The answer is, Yes (when they open the Company Portal app for the first time after this feature have been enabled in your tenant).



## 3 Mobile Device Management (MDM) Configuration

### 3.1 Intune Device Profiles – Configuration Profiles

A Device Profile is used to add and configure settings then push these settings to devices in your organization. Microsoft Intune includes settings and features you can enable or disable on different devices within your organization. These settings and features are added to "configuration profiles". You can create profiles for different devices and different platforms then, use Intune to apply or "assign" the profile to the devices.

As part of your mobile device management (MDM) solution, use these configuration profiles to complete different tasks. Some profile examples include:

- On Windows 10 devices, use a profile template that blocks ActiveX controls in Internet Explorer.
- On iOS/iPadOS and macOS devices, allow users to use AirPrint printers in your organization.
- Allow or prevent access to bluetooth on the device.
- Create a WiFi or VPN profile that gives different devices access to your corporate network.
- Manage software updates, including when they are installed.
- Run an Android device as dedicated kiosk device that can run one app or run many apps.

#### Windows - Configure a Windows device restriction profile

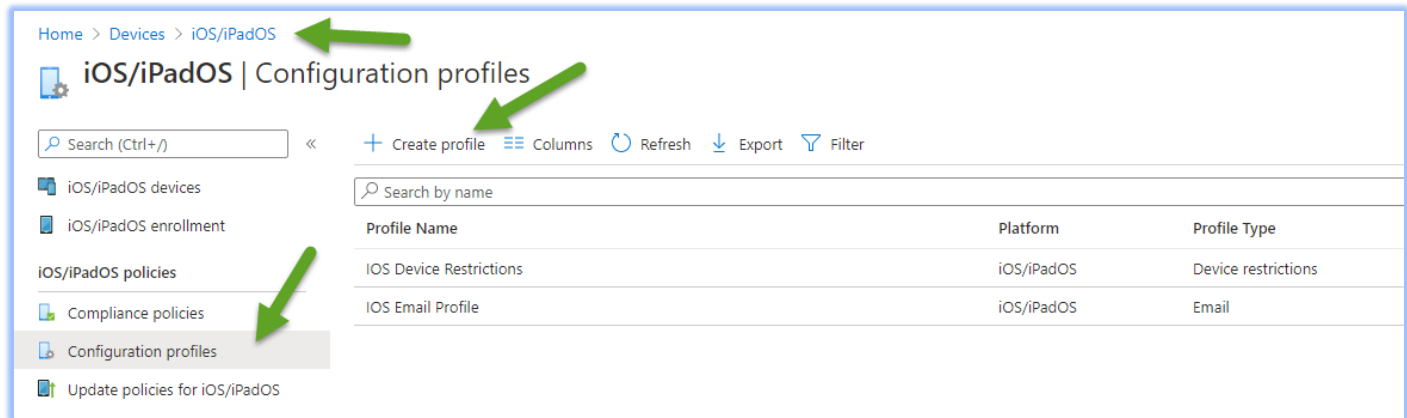
The screenshot shows the Microsoft Intune console interface. The left sidebar is expanded to show 'Configuration profiles'. A green arrow points to this menu item. The main area displays a table of configuration profiles. The table has columns for 'Profile Name', 'Platform', 'Profile Type', and 'Assigned'. One profile is listed: 'Windows 10 Device Restrictions Profile' with a platform of 'Windows 10 and later' and a profile type of 'Device restrictions'. The 'Assigned' column shows 'Yes'.

Profile Name	Platform	Profile Type	Assigned
Windows 10 Device Restrictions Profile	Windows 10 and later	Device restrictions	Yes

Device restriction policy that disables Cortana.

Device Profile for Windows 10 to implement Bitlocker.

IOS – Configure a IOS Device profile to automatically configure Email and to require a password



**Best Practices:** As a best practice, create and assign profiles specifically for your user groups. And, create and assign different profiles specifically for your device groups.

### 3.2 Intune Compliance Policies and Conditional Access

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Intune can help protect organizational data by requiring users and devices to meet some requirements. In Intune, this feature is called compliance policies.

Compliance policies in Intune:

- Define the rules and settings that users and devices must meet to be compliant.
- Include actions that apply to devices that are noncompliant. Actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on noncompliant devices.
- Can be combined with **Conditional Access**, which can then block users and devices that do not meet the rules.

There are two parts to compliance policies in Intune:

- **Compliance policy settings** – Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that have not received any device compliance policies are compliant or noncompliant.
- **Device compliance policy** – Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.

Creating a Windows 10 Compliance Policy to require BitLocker and Windows Defender

## Conditional Access Policy

**Conditional Access | Policies**  
Azure Active Directory

« + New policy | What If | Got feedback?

**What is conditional access?**  
Conditional Access gives you the ability to enforce access requirements when specific conditions occur. Let's take a few examples

Conditions	Controls
When any user is outside the company network	They're required to sign in with multi-factor authentication
When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined device

Want to learn more about conditional access?

**Get started**

- Create your first policy by clicking "+ New policy"
- Specify policy Conditions and Controls
- When you are done, don't forget to Enable policy and Create

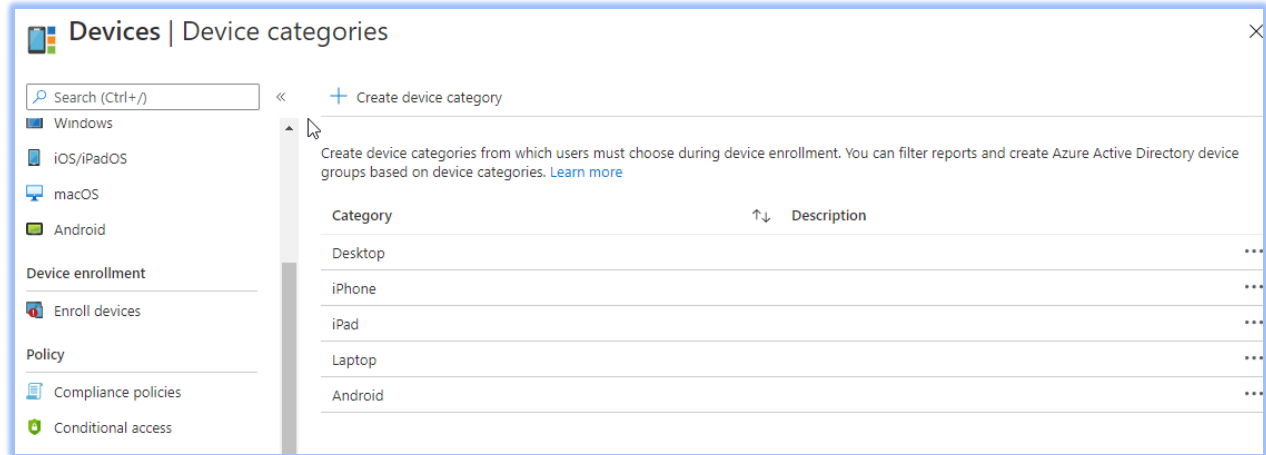
[Interested in common scenarios?](#)

In this example we will require a user that has been detected as a medium security risk to require MFA when accessing Microsoft Teams.

**Best Practices:** Using this feature requires an Azure AD Premium P1 or P2 license. When new policies are ready for your environment, deploy them in phases in the production environment. First apply a policy to a small set of users in a test environment and verify if the policy behaves as expected. This will avoid blocking users in production.

### 3.3 Create Intune Device Categories

A device category is used to prompt users to answer what type of device they have during enrollment. To make managing devices easier, you can use Microsoft Intune device categories to automatically add devices to groups based on categories that you define.



**Best Practices:** Device categories use the following workflow:

- Create categories that users can choose from when they enroll their device.
- When users of iOS/iPadOS and Android devices enroll a device, they must choose a category from the list of categories you configured. To assign a category to a Windows device, users must use the Company Portal website.
- You can then deploy policies and apps to these groups.

### 3.4 Configure Personal or Corporate Identifiers

You can identify devices as corporate-owned to refine management and identification. Intune can perform additional management tasks and collect additional information such as the full phone number and an inventory of apps from corporate-owned devices. You can also set device restrictions to block enrollment by devices that aren't corporate owned.

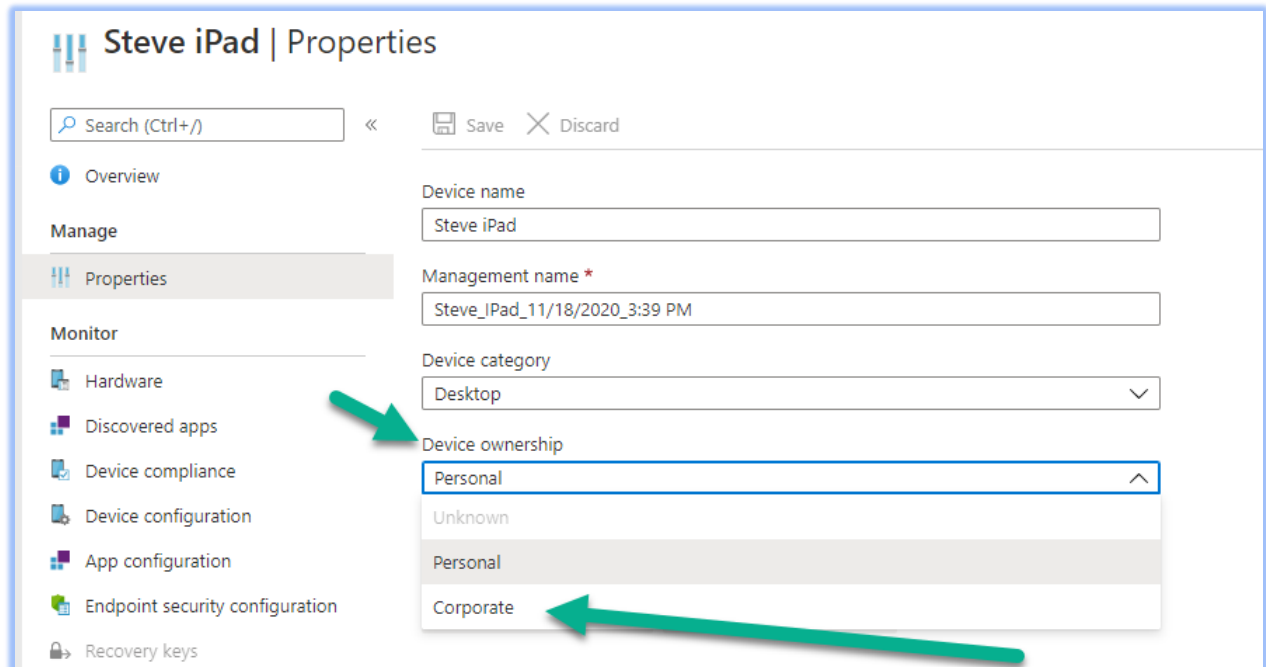
At the time of enrollment, Intune automatically assigns corporate-owned status to devices that are:

- Enrolled with a device enrollment manager account (all platforms)
- Enrolled with the Apple Device Enrollment Program, Apple School Manager, or Apple Configurator (iOS only)
- Identified as corporate-owned before enrollment with an international mobile equipment identifier (IMEI) numbers (all platforms with IMEI numbers) or serial number (iOS and Android)
- Joined to Azure Active Directory with work or school credentials. Devices that are Azure Active Directory registered will be marked as personal.
- Set as corporate in the device's properties list

After enrollment, you can change the ownership setting between Personal and Corporate.

## To change device ownership:

1. Sign into the Microsoft Endpoint Manager admin center, choose Devices > All devices > choose the device.
2. Choose Properties.
3. Specify Device ownership as Personal or Corporate.



**Best Practices:** Be sure to check before marking personally owned device to corporate owned devices. This may be prohibited by the client.



## 4 Application Management and Software Update Policies

### 4.1 Deploy Client Apps to Managed Intune Devices

There are various types of apps that are available for Intune. You must determine app requirements that are needed by the users at your company, such as the platforms and capabilities that your workforce needs.

#### App types in Microsoft Intune

Intune supports a wide range of app types. The available options differ for each app type. Intune lets you add and assign the following app types:

App types	Installation	Updates
Apps from the store (store apps)	Intune installs the app on the device.	App updates are automatic.
Apps written in-house (line-of-business)	Intune installs the app on the device (you supply the installation file).	You must update the app.
Apps that are built-in (built-in apps)	Intune installs the app on the device.	App updates are automatic.
Apps on the web (web link)	Intune creates a shortcut to the web app on the device home screen.	App updates are automatic.
Apps from other Microsoft services	Intune creates a shortcut to the app in the Company Portal. For more information, see <a href="#">App source setting options</a> .	App updates are automatic.

#### Deploy Client Apps to Managed Intune Devices

You can add an app in Microsoft Intune by selecting Apps > All apps > Add. The Select app type pane is displayed and allows you to select the App type.

### Add App

iOS store app

✓ **App information**   2 Assignments   3 Review + create

Select app \* ⓘ   [Search the App Store](#)

Name \* ⓘ   Microsoft Word

Description \* ⓘ   The trusted Word app lets you create, edit, view, and share your files with others quickly and easily. Send, view and edit Office docs attached to emails from your

Publisher \* ⓘ   Microsoft Corporation

Appstore URL   https://apps.apple.com/us/app/microsoft-word/id586447913?uo=4

Minimum operating system \* ⓘ   iOS 8.0

Applicable device type \* ⓘ   2 selected

Category ⓘ   0 selected

Show this as a featured app in the Company Portal ⓘ    Yes    No

Option	Devices enrolled with Intune	Devices not enrolled with Intune
Assign to users	Yes	Yes
Assign to devices	Yes	No

Deploy Microsoft Team to iOS devices.

Deploy a weblink to all devices.

Deploy a Line of Business application to Windows Devices.

**Best Practices:** For each app, you determine the platforms needed, the groups of users that need the app, the configuration policies to apply for those groups, and the protection policies to apply.

Additionally, you must determine whether to focus on Mobile Device Management (MDM) or only on Mobile Application Management (MAM).

## 4.2 App Protection Policies (MAM)

Enrolled devices are fully managed by MDM, meaning all devices settings can be controlled and configured according to a company policy. A device can still have access to company resources and not be enrolled. App protection policies utilizing Intune Mobile Application Management (MAM) can ensure that an organizations data remains safe or remains in a managed app.

Application protection policies can be configured on devices that are Enrolled in Intune (typically corporate owned) or device that are not enrolled (BYOD). You have control over corporate applications on device that are not enrolled.

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it and can be managed by Intune.

The MDM solution adds value by providing the following:

- Enrolls the device
- Deploys the apps to the device
- Provides ongoing device compliance and management

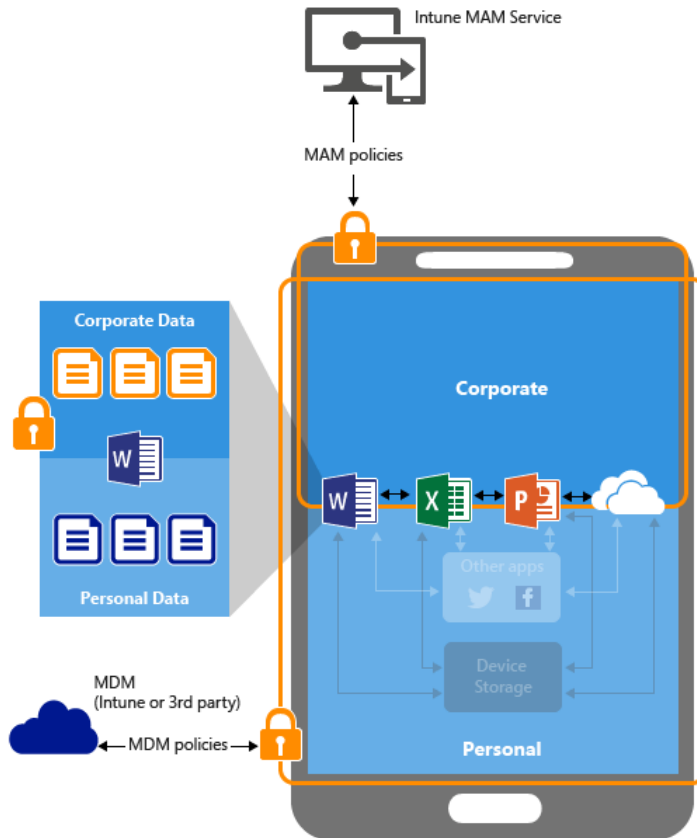
The App protection policies add value by providing the following:

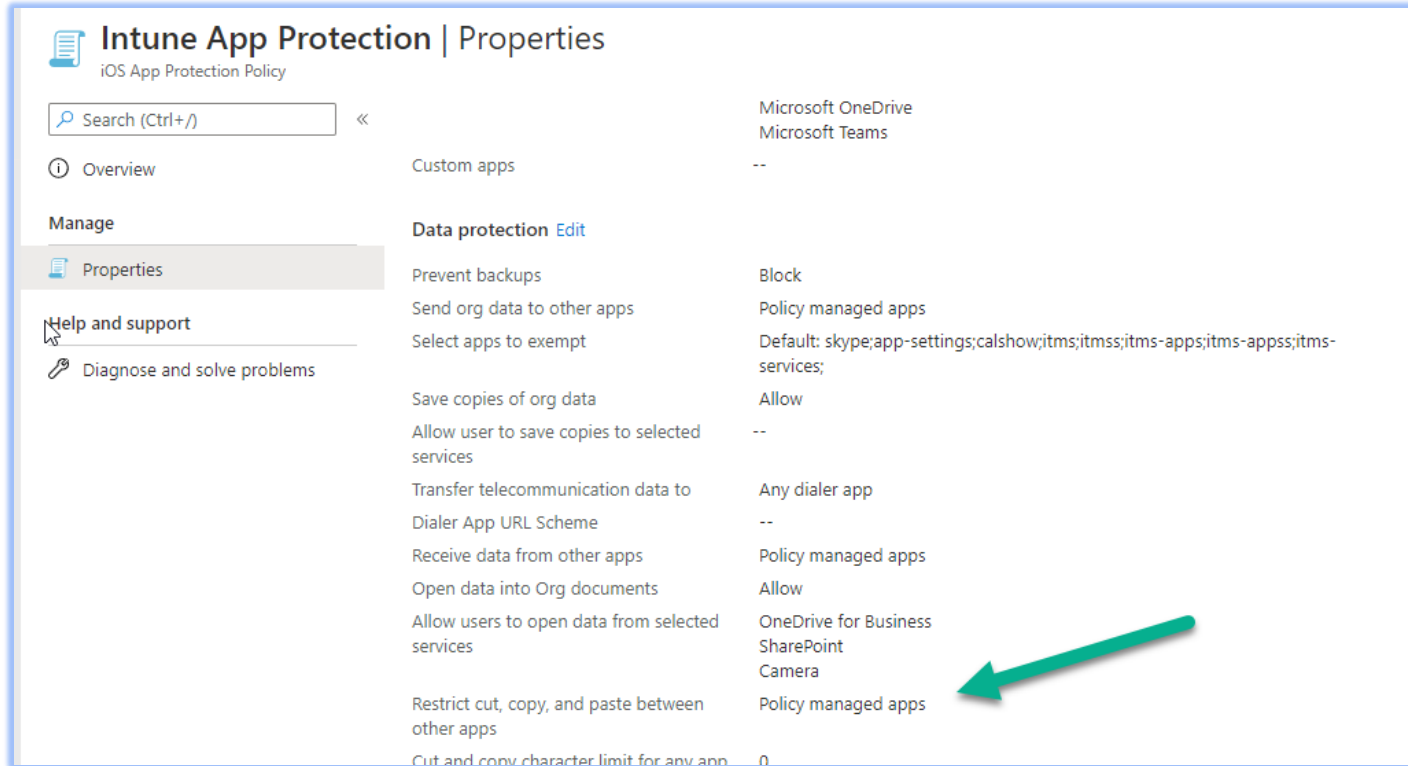
- Help protect company data from leaking to consumer apps and services
- Apply restrictions like *save-as*, *clipboard*, or *PIN*, to client apps
- Wipe company data when needed from apps without removing those apps from the device

In the example below we will create an iOS APP Protection Policy to prohibit copy and paste between non corporate managed apps.

## Data protection with APP on devices managed by an MDM solution

The below illustration shows the layers of protection that MDM and App protection policies offer together.





**Best Practices:** Apply a less strict MAM policy to Intune managed devices and apply a more restrictive MAM policy to non-MDM-enrolled devices. Apply a MAM policy to unenrolled devices only.

### 4.3 Software Update Policies

Software update policies let you force supervised iOS/iPad iOS, Android and Windows devices to automatically install OS updates.

#### Windows 10

Use Intune to manage the install of Windows 10 software updates from Windows Update for Business.

By using Windows Update for Business, you simplify the update management experience. You do not need to approve individual updates for groups of devices and can manage risk in your environments by configuring an update rollout strategy. Intune provides the ability to configure update settings on devices and gives you the ability to defer update installation. You can also prevent devices from installing features from new Windows versions to help keep them stable, while allowing those devices to continue installing updates for quality and security.

Intune stores only the update policy assignments, not the updates themselves. Devices access Windows Update directly for the updates.

Intune provides the following policy types to manage updates:

- Windows 10 update ring: This policy is a collection of settings that configures when Windows 10 updates get installed.
- Update ring policies are supported for devices that run Windows 10 version 1607 or later.
- Windows 10 feature updates: This policy updates devices to the Windows version you specify, and then freezes the feature set version on those devices. This version freeze remains in place until you choose to update them to a later Windows version. While the feature version remains static, devices can continue to install quality and security updates that are available for their feature version.
- You assign policies for Windows 10 update rings and Windows 10 feature updates to groups of devices. Use both policy types in the same Intune environment to manage updates for your Windows 10 devices.

**Windows 10 Updates | Properties**  
Windows 10 update rings

Search (Ctrl+J) «

Overview

**Manage**

Properties

**Monitor**

- Device status
- User status
- End user update status

**Update ring settings** Edit

Update settings	
Servicing channel	Semi-Annual Channel
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	7
Feature update deferral period (days)	30
Set feature update uninstall period (2 - 60 days)	10
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM

**Best Practices:** Minimum of 3 Update rings Test, with a few IT people only. Pilot, with more IT people and users for many department/roles. Production, with everyone else.

## iOS Updates

The update policy for iOS devices will only provide you the choice to prevent the device from installing the updates. However, you can use this option to choose when the update will be applied.

**iOS Update Policy | Properties**  
iOS/iPadOS Updates

Search (Ctrl+/) <<

Overview

Manage

Properties

**Basics Edit**

Name: iOS Update Policy  
Description: Update Policy for all iOS Devices

**Update policy settings Edit**

Update to install: Install iOS/iPadOS Latest update  
Schedule type: Update during scheduled time  
Time zone: UTC-5  
Time window:

Start day	Start time	End day	End time
Sunday	1 AM	Sunday	4 PM

**Assignments Edit**

Included groups: iPad Test, Apple Devices

**Best Practices:** You may decide that it is best to only have the updates installed over a weekend.

## 5 Enroll Devices into Intune

Enrolling your devices into Microsoft Intune allows your Windows 10 devices to get access to your organization's secure data, including email, files, and other resources. This is true for both Windows 10/11 systems, MacOS, and iOS/Android Mobile devices.

### 5.1 Windows 10/11

Enrolling your devices helps secure this access for both you and your organization and helps keep your work data separate from your personal data. To manage devices in Intune, devices must first be enrolled in the Intune service. Both personally owned and corporate-owned devices can be enrolled for Intune management.

There are two ways to get devices enrolled in Intune:

- Users can self-enroll their Windows PCs (BYOD)
- Admins can configure policies to force automatic enrollment without any user involvement (Corporate Owned Devices)

### 5.2 Azure AD Join – Windows 10/11- Corporate Owned Devices Only:

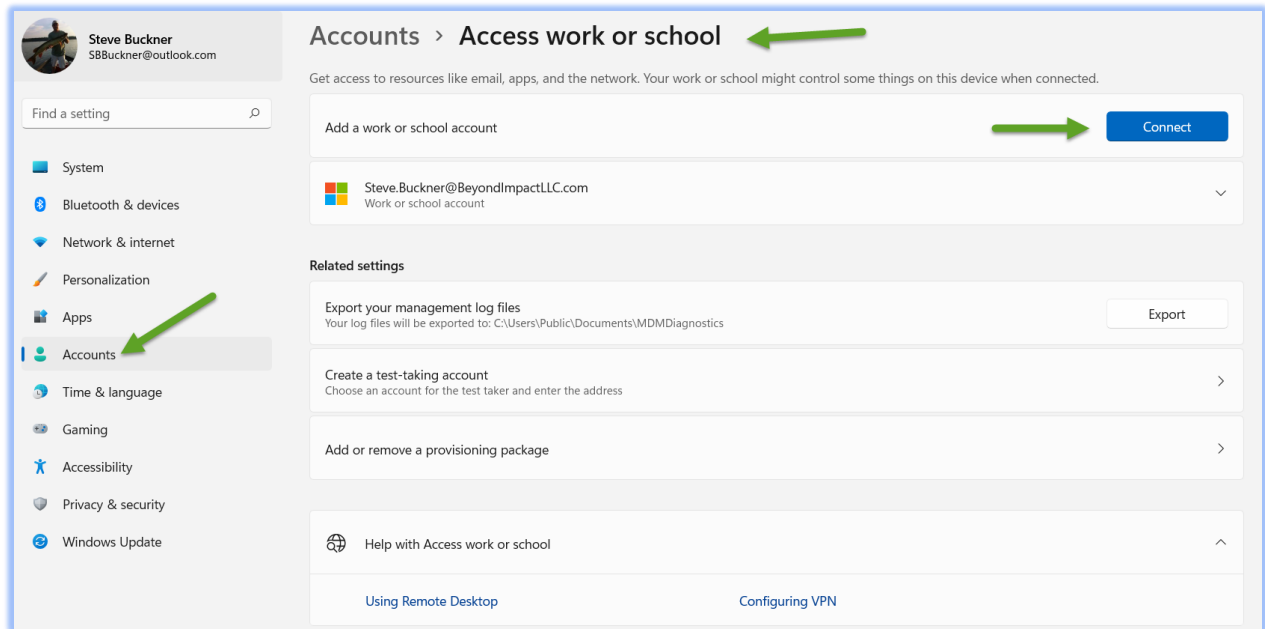
This option is **ONLY** for devices that have **NOT** been Azure AD Joined and that you wish to convert to Azure AD Joined.

What are the benefits of Azure AD join?

Joining devices to Azure AD enables the following benefits

- Single sign-on to cloud resources, which includes the Microsoft 365 suite of apps, SaaS applications and potentially on-premises applications.
- Biometric authentication through Windows Hello for Business
- Self-service password reset which is great for remote workers.
- Full device management via Intune and zero-touch provisioning leveraging Windows Autopilot including automatic device license assignment.
- Self-service enterprise application provisioning through the published enterprise app store.
- Security benefits through leveraging device based Conditional Access policies.





## Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Email address


### Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.


[Join this device to Azure Active Directory](#)

[Join this device to a local Active Directory domain](#)

Next

 Microsoft

## Sign in

steve.buckner@beyondimpactllc.com 


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

**Next**


**BEYOND  
IMPACT**

← steve.buckner@beyondimpactllc.com

## Enter password

..... 


[Forgot my password](#)


**Sign in** 

**BEYOND  
IMPACT**

steve.buckner@beyondimpactllc.com

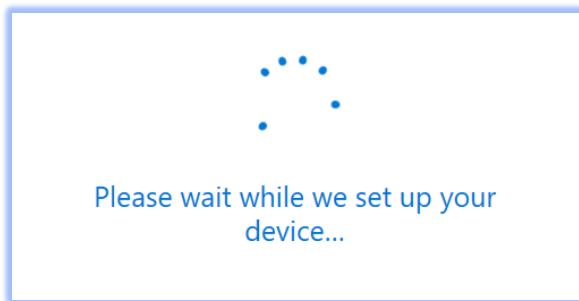
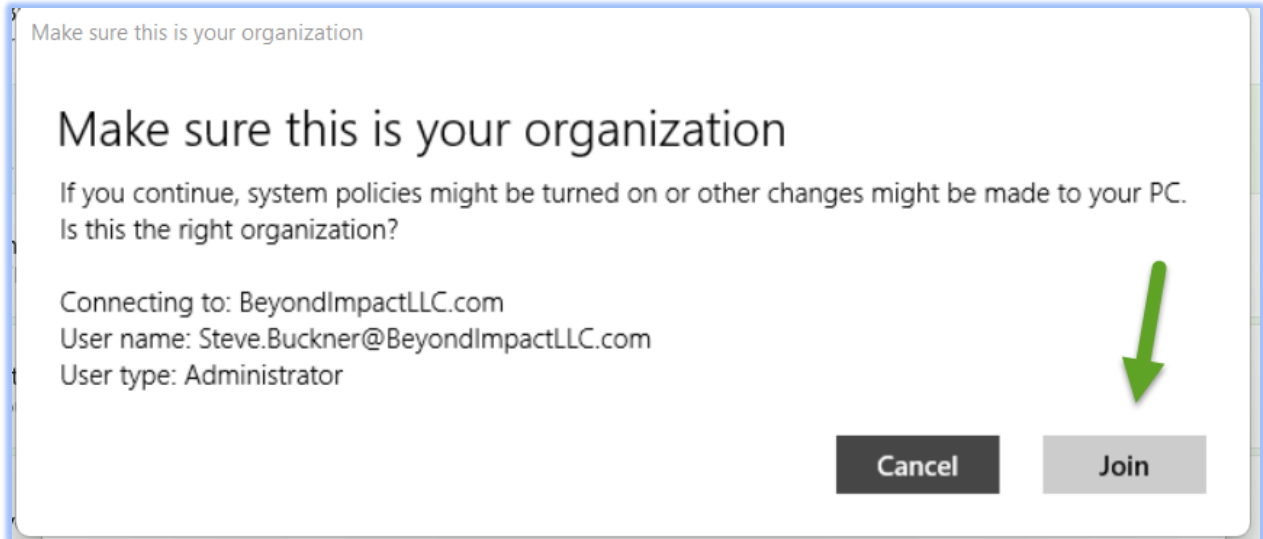
### Verify your identity

 Text +X XXXXXXXX47

 Call +X XXXXXXXX47

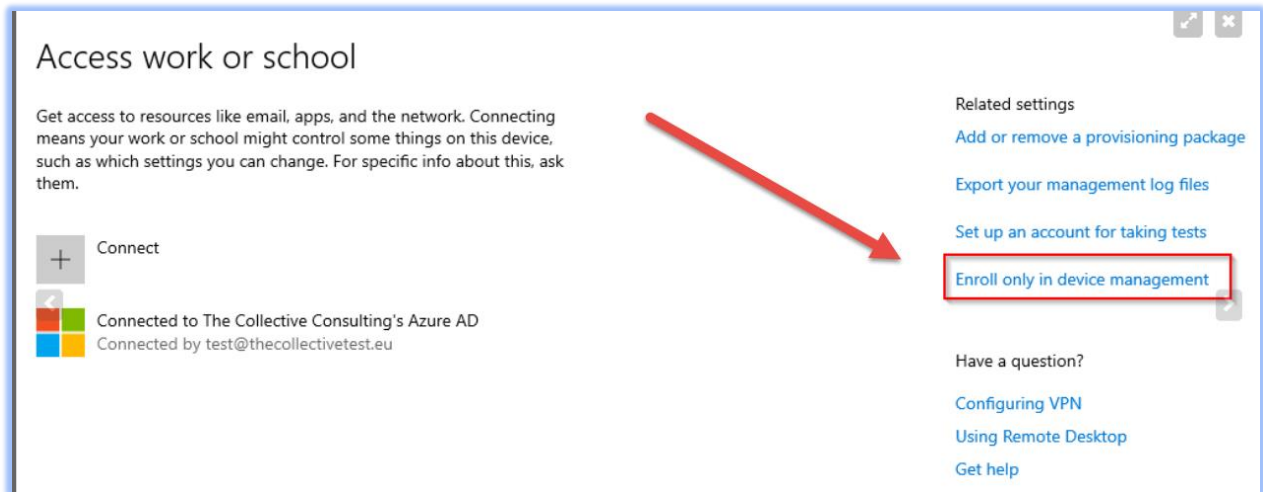
Are your verification methods current? Check at <https://aka.ms/mfasetup>

**Cancel**



### 5.3 Enroll a Windows 10 / 11 Device into Intune that has already been Azure AD Joined (including Hybrid Azure Ad Joined)

The preferred way to enroll existing devices that have already been Azure AD Joined or Hybrid Azure AD Joined is to use the **Enroll only in device management** option located in Settings.



Once enrolled, you can also optionally install the Company Portal App from the Microsoft Store - [Company Portal - Microsoft Store Apps](#).

The Company Portal will allow users to view available applications that have been made available to them for installation. Intune Administrations also have the option to automatically install/push applications to Azure AD Joined systems. If the applications have not been automatically pushed, they will be available to them using the Company Portal App.

## 5.4 Enroll Windows 10/11 - Personally Owned Devices into Intune

For a Windows BYOD (self-enrollment) you can **Azure AD Register** it into enroll into Intune:

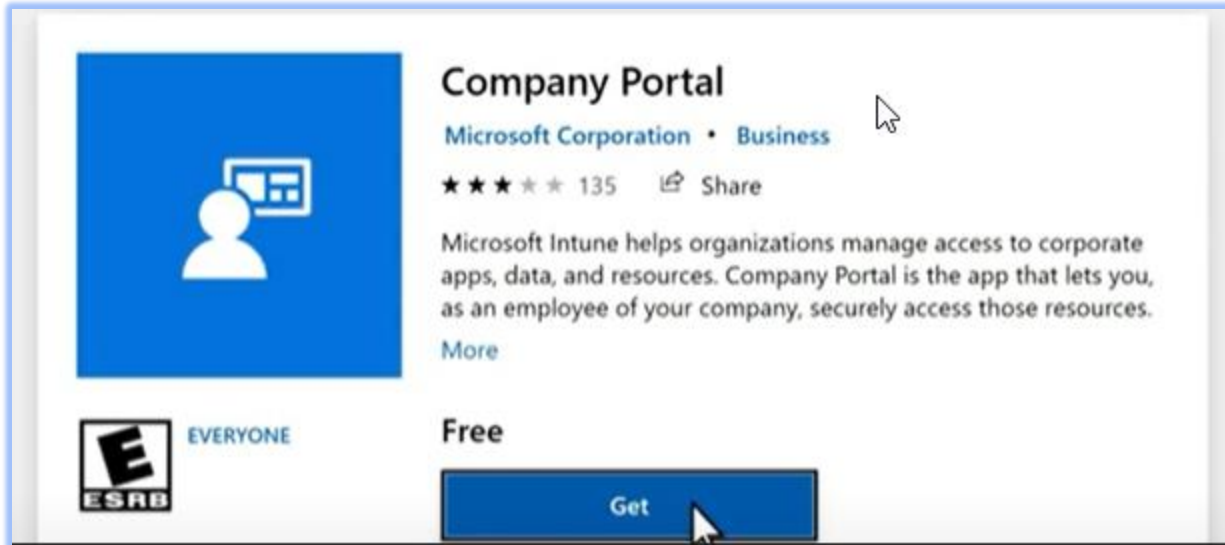
You can install the Company Portal App from the devices app store to enroll into Intune (Azure AD Registered):

Azure AD join is really only for devices that are company owned where the entire device is used for work and only one account is used on the device. With **employee owned or contractor devices**, they will be logging into their device with their own account or personal identity but will use their Azure AD identity to access company resources. For this scenario, Azure AD registration is used.

When a device is Azure AD registered, it is possible to ensure the device meets your compliance requirements before accessing company resources. You can still send security policies to these AAD registered devices (e.g., require a passcode on the device) and will gain visibility of the device in your tenant.

### REGISTERING THROUGH THE COMPANY PORTAL APP

Enrolling existing devices via the Company Portal app from the Microsoft Store is the **easiest** option for employees to Azure AD register their device. They can download the app and enroll using their Azure AD identity. [Company Portal - Microsoft Store Apps](#)



**Company Portal**  
Microsoft Corporation • Business  
★★★★★ 135 Share  
Microsoft Intune helps organizations manage access to corporate apps, data, and resources. Company Portal is the app that lets you, as an employee of your company, securely access those resources.  
More

**Free**

ESRB EVERYONE

Get

Use this account everywhere on your device

Windows will remember your account and make it easier to sign in to apps and websites. You won't have to enter your password each time you access your organization's resources. You may need to allow them to manage certain settings on your device.

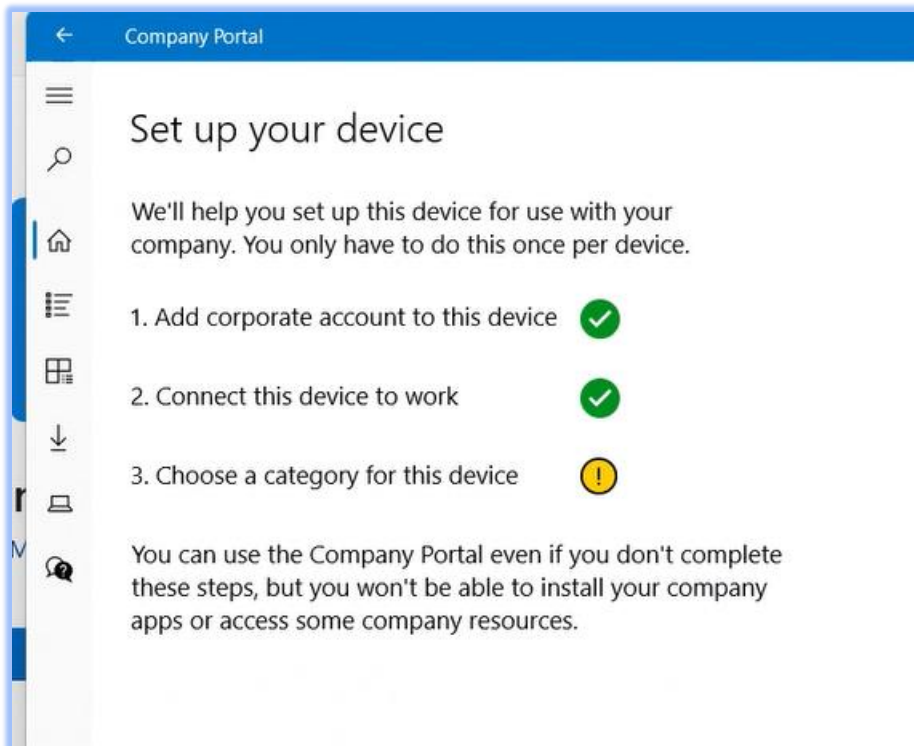
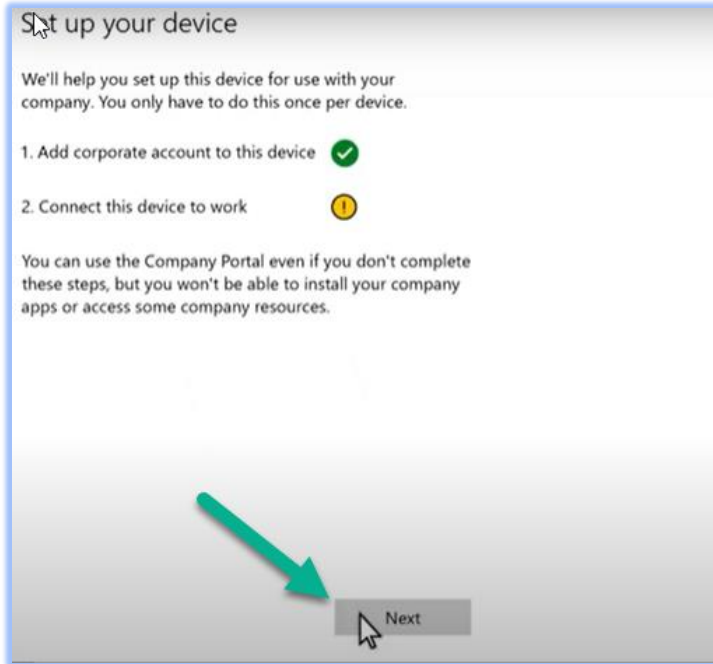
Allow my organization to manage my device

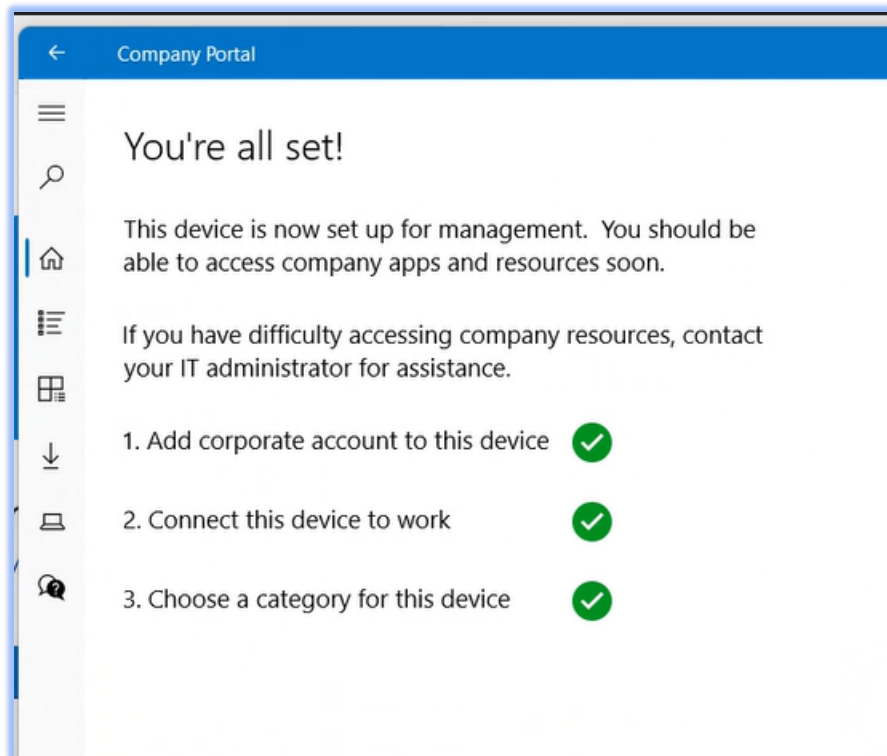
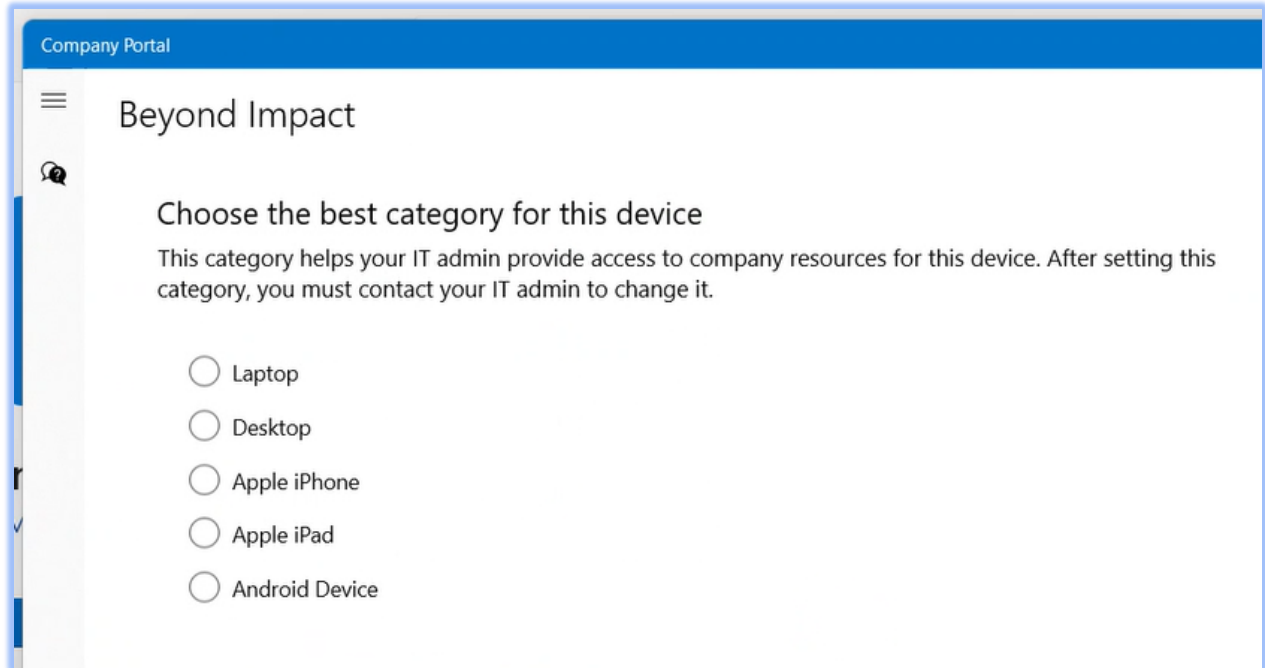
Newest apps

Your IT administrator did not make any apps available to you.

My Devices

**i** This device hasn't been set up for corporate use yet. Select this message to begin setup.





The churchoffice Windows 10 PC below was enrolled using the Company Portal App and is Azure AD Registered.

Name	Enabled	OS	Version	Join Type	Owner	MDM
<input type="checkbox"/> churchoffice	✔ Yes	Windows	10.0.19041.630	Azure AD registered	Kate Buckner	None

The STEVE-OFFICE Account was connected using “Join this device to Azure Active Directory.”

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
<input type="checkbox"/> KATE-DESKTOP	✔ Yes	Windows	10.0.18363.1198	Azure AD joined	Kate Buckner	Microsoft Intune	✔ Yes
<input type="checkbox"/> Steve iPad	✔ Yes	iPad	12.4.8	Azure AD registered	Steve Buckner	Microsoft Intune	✔ Yes
<input type="checkbox"/> STEVE-OFFICE	✔ Yes	Windows	10.0.19042.630	Azure AD joined	Steve Buckner	Microsoft Intune	✔ Yes
<input type="checkbox"/> Joe_AndroidForWor...	✔ Yes	AndroidForWork	9.0	Azure AD registered	Joey	Microsoft Intune	✔ Yes

## 5.5 Enroll iOS and Android Devices into Intune

### ENROLLING THROUGH THE COMPANY PORTAL APP

Enrolling Android or iOS devices via the Company Portal app from the Google Play or Apple Store is the **easiest** option for employees. They can download the app and enroll using their Azure AD identity (see company portal steps above).

**BYOD** - After you have assigned user licenses, users can download the Intune Company Portal app from the App Store, and follow enrollment instructions in the app.

**Company Owned** - For organizations that buy devices for their users, Intune supports the following iOS/iPad iOS company-owned device enrollment methods:

- Apple's Automated Device Enrollment (ADE)
- Apple School Manager
- Apple Configurator Setup Assistant enrollment
- Apple Configurator direct enrollment