

Intune Implementation Guide



Guide Description

The purpose of this guide is to lay out the steps for implementing Intune. This guide is assuming you have the **M365 Business** License. It can apply to EMS licenses but some features will not be covered such as Conditional Access and Windows Autopilot. After you complete this guide you will have:

- Created different Device Groups
- Configured Autoenrollment of devices
- Configured Policies and Profiles for devices
- Added Applications
- Setup Enrollment for Apple, Windows, and Android Devices
- Enrolled a device to Intune

Disclaimer

This guide is meant to provide best practices for policy creation and implementation of Intune. It is meant to be used as a template, but the policies defined will not be the same in all use cases. You must access to policies and configuration you will need for your customers environment and make changes as needed. As a best practice, test all configurations with a pilot group before moving to broad deployment across an entire organization



Pre-Flight Checklist



- a. Determine Platforms that you will support
 - i. IOS/Android
 - ii. MAC/Windows
- b. Have baseline security requirements complied that you want to implement
 - i. Min/Max OS versions
 - ii. Password Requirements
 - iii. Encryption Enabled
- c. Determine if there will be separate groups for separate security policies
 - i. Ex1. I have one group I want to assign IOS policies to and I have another I want to assign Android policies to.
 - ii. Ex2. I have more granular security policies I want to apply to on group over another.
 - iii. I encourage you to create a test group for piloting everything you are looking to implement in your organization
- d. Access if there are any apps beyond 365 that you want users to have access to
- e. Choose 3 pilot devices you want to enroll into Intune



Table of Contents



Phase 1: Groups and Licensing

•Ensure that all users have appropraite Licensing •Add Necessary Groups for Policy Assignment •Configure Device Autoenrollment



Phase 2: Polciy and Profile Creatation

•Configure Device Polcies

Android

•Windows

•Create Device Profile





Phase 4: Configuring Enrollment

•Setting Apple Enrollment •Setting Android Enrollment •Setting Terms and Conditions •Adding Company Branding



Phase 5: Enroll Devices

•Enroll Devices: Windwos •Enroll Devices: iOS and Android



Phase 6: Testing and Broad Deployment

• Pilot Testing and Remediation •Broad Deployment



Table of Contents Continued (Links to sections of Document):

Phase 1: Groups and Licensing

- Ensure that all users have appropriate Licensing
- Add Necessary Groups for Policy Assignment
- <u>Configure Device Autoenrollment</u>
- Phase 2: Policy and Profile Creation
 - <u>Configure Device Policies</u>
 - o <u>iOS</u>
 - o <u>Android</u>
 - o <u>Windows</u>
 - <u>Create Device Profiles</u>

Phase 3: Add Apps

- Adding Applications
- Adding Microsoft Authenticator App

Phase 4: Configuring Enrollment

- <u>Setting Apple Enrollment</u>
- <u>Setting Android Enrollment</u>
- <u>Setting Terms and Conditions</u>
- Adding Company Branding

Phase 5: Enrolling Devices

- Enroll Devices: Windows
- Enroll Devices: iOS and Android

Phase 6: Testing and Broad Deployment

• Pilot Testing and Remediation



Licensing Users

1. Ensure All appropriate Users are Licensed

•

a. Login to 365 Admin Center> Go to Active User

	Microsoft 365 admin cen	nter	
≡		<u>^</u>	wraj records!
ŵ	Home		Ferentiale
8	Users	^	Essentials
	Active users		User management
	Contacts 🖑		
	Guest users		User management
	Deleted users		
₽	Devices	\sim	Add, edit, and remove user accounts, and reset passwords.
RR	Groups	\sim	
侵	Resources	\sim	Add user Edit user \vee
	Billing	\sim	
			Azura Activa Diractory

b. Select a User>Click Licenses and Apps>Ensure an M365 License is Assigned

Ü	Refresh 🔍 Reset password 🛱 Assign	n to group	📋 Manage product licenses 🤌 Manage role	es @ Manage email aliases	
	Display name ↑		Username	Licenses	Blake Closper
	Adams Aliasing Test		alongmire1@wrajrecords.com	Unlicensed	BC S S
	admin		$admin_marcusfor the winand stuff.on microsoft.com \# EXT$	Unlicensed	Sign in allowed Change photo
	Administrator		administrator@wrajrecords.com	Unlicensed	
	Andy Green		agreen@wrajrecords.com	Unlicensed	Account Devices Licenses and Apps Mail OneDrive
	Anthony Tonetti		atonetti@wrajrecords.com	Microsoft Flow Free, Power BI (free)	
	Anthony Tonetti		anthonytonetti@wrajrecords.com	Unlicensed	United States
	Austin Lieber		alieber@wrajrecords.com	Unlicensed	
	Axel Morlotte		amorlotte@wrajrecords.com	Unlicensed	Licenses (17)
	Betty Joe		bettyjoe@wrajrecords.onmicrosoft.com	Unlicensed	Audio Conferencing You don't have any licenses available. To purchase additional licenses, please contact your partner(s).
	Billy Prejean		bprejean@wrajrecords.com	Unlicensed	Azure Information Protection Plan 1 1 of 1 licenses available
•	Blake Closner		bclosner@wrajrecords.com	Microsoft 365 Business	Domestic Calling Plan 1 of 2 licenses available
	Brandon Smith		bsmith@wrajrecords.com	Unlicensed	Dynamics 365 P1 Trial for Information Workers 9999 of 10000 licenses available
	Bruce Wayne		bwayne@wrajrecords.com	Unlicensed	Enterprise Mobility + Security E3 1 of 2 licenses available
	Carla Diffee		cdiffee@wrajrecords.com	Unlicensed	Exchange Online (Plan 1) You don't have any licenses available. To purchase additional licenses, please contact where neutraneous
	cdeacon		cdeacon_gflclan.com#EXT#@wrajrecords.onmicrosoft.c	Unlicensed	Ord Elements mailable
	Chad Day		cday@wrajrecords.com	Unlicensed	Microsoft 365 E5



Create Groups

Create different groups if you want to separate out different people into different Intune Polices.

a. Scroll Down in the 365 Admin Portal and Go to the **Device Management Portal**

↔ Health	User management
Admin centers	Add, edit, and remove user accounts, and reset passw
◯ Security	
Compliance	
🖨 Device Management	Add user Edit user \lor
Azure Active Directory	Azure Active Directory
Exchange	

b. Click on Groups and click New Group

Microsoft 365 Device Manageme	ent		
«	Dashboard > Groups - All groups		
🗔 Dashboard	Groups - All groups		
i∃ All services	«	+ New group C) Refresh	umns
– 🛨 FAVORITES ————————————————————————————————————	🗳 All groups	New group	annis
Device compliance	🗳 Deleted groups	Search groups	
듉 Device enrollment	Settings	NAME	GROUP TYPE
Conditional Access	🔅 General	AD AAD DC Administrators	Security
Gecurity baselines	Expiration	AU AD Users	Office
L Device configuration	A stilling		0///
🖵 Devices	Activity	AD Adam2TestAgain	Office
🧔 Software updates	E Access reviews	AD adamstest	Office
Client apps	Audit logs	AD AdminAgents	Security
🛓 Users 🧹	Troubleshooting + Support	AD ADSyncAdmins	Security
Groups	🗙 Troubleshoot	AD ADSyncAdmins	Security
	· · · ·		



c. Group Type can be 365 or security. You can add whatever users you would like for this group. This is my test group, so I am going to add my pilot user

Group	×	Select members
* Group type		Select member or invite an external user ()
Office 365	~	nros
* Group name		Nick Days
Test	~	NR nross@wrajrecords.com
Group description 0		Nick Ross
Intune Pilot Group	~	
* Membership type 🛛		
Assigned	~	
Members 0		Selected members:
	>	NIR Nick Ross
		nross@wrajrecords.com
		L ₂ 2
Create		Select

d. Click **Create** when finished

Group type Office 365 Group name • Test Group description • Intune Pilot Group Membership type • 	- All grou	ps > Group	> Selec	t members	5
 ★ Group type Office 365 ★ Group name ● Test ✓ Group description ● Intune Pilot Group ✓ ★ Membership type ● Assigned ✓ 	Grou	D			>
Group type Office 365 Group name Test Group description Intune Pilot Group Membership type Assigned Members					
Office 365 Group name • Test Group description • Intune Pilot Group Membership type • Assigned Members • 	* Group	type			
 ★ Group name ● Test ✓ Group description ● Intune Pilot Group ✓ ★ Membership type ● Assigned ✓ Members ● 	Office	365			\sim
Test ✓ Group description ① Intune Pilot Group * Membership type ① Assigned Members ① >	* Group	name 🚯			
Group description () Intune Pilot Group Membership type () Members ()	Test				~
Intune Pilot Group	Group o	lescription (
Membership type Assigned Members	Intune	Pilot Group			~
Assigned	* Memi	ership type	0		
Members ()	Assign	ed			\sim
	Memb	ers			>
	0				
	Crea	te			



Device Autoenrollment

Ensure Device Autoenrollment is Turned On. Autoenrollment allows devices that join to Azure AD to automatically be enrolled in Intune and have policies push down to them:

a. Go to Device Enrollment and click Windows Enrollment



b. Select Automatic Enrollment





c. Choose **All** if it is not already preselected. You can choose autoenrollment for only subsets of your users by clicking **Some.** Click **Save** when finished

Dashboard > Device enrollment - Windows enrollment > Configure			
Configure			
Rave X Discard 🟛 Delete			
MDM user scope 🚯 None Some All			
MDM terms of use URL (https://portal.manage.microsoft.com/TermsofUse.aspx			
MDM discovery URL			
MDM compliance URL 🚯 https://portal.manage.microsoft.com/?portalAction=Compliance			
Restore default MDM URLs			
MAM User scope None Some All			
MAM Terms of use URL 🚯			
MAM Discovery URL 🚯 https://wip.mam.manage.microsoft.com/Enroll			
MAM Compliance URL 🚯			
Restore default MAM URLs			



Configure Device Policies

Device Policies designate which devices are compliant and non-compliant. When we join devices to Intune after configuring these policies, we will be able to see why the devices are not compliant. You will want to create a device policy for every platform you wish to support in your organization

IOS

a. In the Device Management admin portal, go to Device Compliance>Policies>Create Policy





b. The first policy we will create is for iOS. Select a **Name** and **Description** (if applicable) and choose **iOS** from the **Platform** dropdown list

Name		4
iOS Policy		~
Description		
Enter a descrip	otion	~
iOS		^
Platform		
Select a platfo	rm	
Android		
Android enter	prise	
iOS	0	
macOS	J.	
Windows Pho	ne 8.1	
Windows 8.1 a	and later	
	nd later	

c. Under the Device Health Section for settings, block Jailbroken Devices

iOS compliance policy	×	Device Health	
Select a category to configure settings.		Jailbroken devices 👔	Block Not configured
Email 🔀 1 setting available	>	Require the device to be at or under the Device Threat Level $oldsymbol{0}$	Not configured
Device Health ① 2 settings available	>		
Device Properties () 4 settings available	>		
System Security 1 System Security 1	>	2	



d. Under **Device Properties**, configure **Min/Max OS versions** if applicable. If you do not what to define these settings leave them blank

iOS compliance policy	×	Device Properties	
Select a category to configure settings	i.	Operating System Version	
Email 🕦 1 setting available	>	Minimum OS version 👩	Not configured
Device Health 🚯		Maximum OS version 🚯	Not configured
2 settings available	>	Minimum OS build version 🚯	Not configured
Device Properties 🕦 4 settings available	>	Maximum OS build version 🚯	Not configured
System Security () 10 settings available	>	\$	
OK		or	

e. Under System Security, enter the values as follows:

iOS compliance policy	×	System Security		
Select a category to configure settings.		Require a password to unlock mobile devices. 🗿	Require Not con	nfigured
Email 1 setting available	>	Simple passwords 🛛	Block Not con	figured
Davice Health	-	Minimum password length 👩	4	~
2 settings available	>	Required password type 🚯	Numeric	~
Device Properties 6 4 settings available	>	Number of non-alphanumeric characters in password	Not configured	~
System Security 🔴	>	Maximum minutes after screen lock before password is required $oldsymbol{ heta}$	15 Minutes	~
		Maximum minutes of inactivity until screen locks $oldsymbol{ ilde{ extbf{0}}}$	15 Minutes	~
		Password expiration (days) 🚯	90	~
		Number of previous passwords to prevent Yeuse 🗿	3	~
ОК		ок		



f. Click **ok** and then **Create**

Dashboard > Device compliance - Policies >	Create Policy > iOS compliance policy	Dashboard > Device compliance - Policies > Create Policy
Create Policy	× iOS compliance policy \Box ×	Create Policy \Box \times
* Name iOS Policy	Select a category to configure settings.	* Name
Description Enter a description	Email	Description
* Platform	Device Health 2 settings available	Enter a description
iOS 🗸	Device Properties ① > 4 settings available	* Platform iOS V
Settings > Configure	System Security 7 of 10 settings configured	Settings > 7 configured
Actions for noncompliance > 1 configured		Actions for noncompliance > 1 configured
Scope (Tags) > 0 scope(s) selected		Scope (Tags) > 0 scope(s) selected
Create	OK LINE	 Create

g. Select Assignments and select the group of users you want this policy applied to:

	🕞 Save 🗙 Discard 🗸 Evaluate	Select 🕤 Search by name or email address
(i) Overview	Include Exclude	AD DC Administrators
Manage	Assign to	
Properties	Selected Groups	AU AD Users 47c1496a-3ae3-4b5d-a8b5-74d80d140021@wrajreco
🏠 Assignments	Select groups to include	Adam2TestAgain
Monitor		
Device status	No assignments	selected members.
User status		No members selected
Per-setting status		
	_	
		Select



Android

a. Click Create Policy

,⊃ Search (Ctrl+/)	«	+ Create Policy == Column	is 📍	Filter 💍	Refresh
0 Overview	^	One or more compliance po an active Mobile Threat Defe and Android.	licies fo ense co	r iOS and And nnector. Click	droid have a co here to setup
Manage	10				
Policies					
📮 Notifications		POLICY NAME	τţ	PLATF 🔍	POLICY TYPE
Locations		Android Compliance Policy		Android	Android cor
Monitor		IOS		iOS	iOS complia
Device compliance		iOS Compliance Policy		iOS	iOS complia
		Windows		Windows	Windows 10

b. Select the Name, enter description (if applicable), and choose Android from Platform dropdown

Dashboard > Device compliance - Policies	> Cre
Create Policy	×
* Name	
Android Policy 🗸	
Description	
* Platform	
Android ^	
Select a platform	
Android	
Android enterprise	
iOS	
macOS	
Windows Phone 8.1	
Windows 8.1 and later	
Windows 10 and later	
Scope (Tags)	•



Þ

c. Under Settings>Device Health, configure the following:

Android compliance policy $\qquad \times \qquad $	Device Health	
Select a category to configure settings. Device Health • 6 settings available Device Properties • 2 settings available	Rooted devices ① Require the device to be at or under the Device Threat Level ① Google Play Protect	Block Not configured ✓
System Security 10 settings available	Google Play Services is configured 🕢 🖟 Up-to-date security provider 🕣 Threat scan on apps 🚯	RequireNot configuredRequireNot configuredRequireNot configured
	SafetyNet device attestation	Not configured V
ОК	ОК	

d. Under Device Properties, configure the Min/Max OS version if applicable. If you do not want to configure, leave blank

board > Device compliance - Policies > Cre	ate Policy	> Android compliance policy > Device Propertie	25
Android compliance policy	×	Device Properties	□ ×
Select a category to configure settings. Device Health 3 of 6 settings configured Device Properties 2 settings available System Security 10 settings available	> >	Operating System Version Minimum OS version () Maximum OS version ()	Not configured Not configured
ОК		ОК	



e. Under System Security, configure as follows:

Android compliance policy	×	System Security	
Select a category to configure settings.		Require a password to unlock the device. If not confi	gured, the use of passwords
Device Health 0	>	optional, and left up to the user to configure.	
	-	Pequire a password to uplack mobile devices	De suites - Net see Course
2 settings available	>	Require a password to unlock mobile devices.	Require Not configure
System Security 🚯		Required password type 🕒	Numeric complex
10 settings available		Minimum password length 🚯	4
		Maximum minutes of inactivity before password is required 🕢	15 Minutes
		Password expiration (days) 🚯	90
		Number of previous passwords to prevent reuse 🗿	3

board > Device compliance - Policies > Create Policy > Android compliance policy > System Security

Android compliance policy	×	System Security			
Select a category to configure settings.		Encryption			
Device Health 6 3 of 6 settings configured	>	Encryption of data storage	on device.	Require	Not configured
Device Properties 🚯	>	Device Security			
2 settings available	_	Block apps from unknown s	sources 🚯	Block	Not configured
System Security 🕦 10 settings available	>	Company Portal app runtim	ne integrity 🚯	Require	Not configured
	-	Block USB debugging on de	evice 🚯	Block	Not configured
		Minimum security patch lev	rel 🚯	Not configu	red
		Restricted apps 🚯			Export
		App name	App Bundle ID		
		Not configured I	Not configured		Add
		Vou have not restricted any a	3000		,

OK



f. Click **OK** and **Create**

Create Policy	×	Android compliance policy $\Box \times$	Dashboard 7 Device compliance	rolicies	, cica
ereate roney		Android	Create Policy		×
Description	*	Select a category to configure settings.	Description		•
		Device Health	Enter a description	~	
* Platform		3 of 6 settings configured	* Platform		
Android	~	Device Properties	Android	\checkmark	
Settings 11 configured	>	System Security	Settings 11 configured	>	I
Locations Configure	>	6 of 10 settings configured	Locations Configure	>	I
Actions for noncompliance 1 configured	>		Actions for noncompliance 1 configured	>	I
Scope (Tags) 0 scope(s) selected	>		Scope (Tags) 0 scope(s) selected	>	I
	•		Create		¥

g. Select Assignments and select the group of users you want this to apply to:

«		Select 🚯
	Save 🔨 Discard 🗸 Evaluate	Search by name or email address
() Overview	Include Exclude	AD DC Administrators
Manage	Assign to	
Properties	Selected Groups	AU AD Users 47c1496a-3ae3-4b5d-a8b5-74d80d140021@wrajreco
Assignments	Select groups to include	Adam2TestAgain
Monitor		Selected members:
Device status	No assignments	
User status		No members selected
Per-setting status		
	_	
		Select



Windows

a. Click Create Policy

Device compliance - Policies			
	+ Create Policy == Columns	T Filter 👌	Refresh 🚽
Overview	One or more compliance policie an active Mobile Threat Defense and Android.	s for iOS and And connector. Click	droid have a cou here to setup a
Manage			
Policies	♀ Search by name		
💄 Notifications	POLICY NAME	PLATF ↑↓	POLICY TYPE
Locations	Android Compliance Policy	Android	Android com
Monitor	IOS	iOS	iOS compliar
Device compliance	iOS Compliance Policy	iOS	iOS compliar
Devices without compliance	Windows	Windows	Windows 10
Setting compliance			

b. Select a **Name**, **Description** (if applicable), and Choose **Windows 10 or later** from the Platform dropdown

Dashboard > Device compliance	- Policies >	Create P
Create Policy		×
* Name		
Windows Policy	 	
Description		
Enter a description	~	
* Platform		1
	^	
Select a platform		
Android		
Android enterprise		
iOS		
macOS		
Windows Phone 8.1		
4		
Windows 8.1 and later		



Select a category to configure settings. Device Health • 3 settings available Device Properties • S settings available Configuration Manager Compliance • System Security • 1 setting available Windows Defender ATP • 1 setting available	
Device Health ① 3 settings available Device Properties ① 5 settings available Configuration Manager Compliance ① System Security ① System Security ① 16 settings available Windows Defender ATP ① 1 setting available Windows Defender ATP ①	
Device Properties 5 settings available Configuration Manager Compliance 1 setting available System Security Not certain available Windows Defender ATP Not certain available	configure
S settings available Configuration Manager Compliance 1 setting available System Security 16 settings available Windows Defender ATP 1 setting available	configure
Configuration Manager Compliance 1 setting available System Security 16 settings available Windows Defender ATP 1 setting available	configure
System Security System	
Windows Defender ATP	
Windows Defender ATP	

c. Under Settings>Device Health, configure the following

d. Under Device Properties, configure the Min/Max OS version if applicable. If you do not want to configure, leave blank

Windows 10 compliance policy Windows 10 and later	×	Device Propert Windows 10 and later	ties		
Select a category to configure settings.	_	Operating System \	/ersion 👩		
Device Health 1 3 of 3 settings configured	>	Minimum OS versior	• •	Not configured	
Davice Properties	-	Maximum OS versior	n 0	Not configured	
5 settings available	>	Minimum OS versior	for mobile devices 🚯	Not configured	
Configuration Manager Compliance 🚯 1 setting available	>	Maximum OS version	n for mobile devices 🚯	Not configured	
5	-	Valid operating syste	em builds 🚯		
System Security 1 16 settings available	>	Description	Minimum	Maximum	Export
	-	Not configured	Not configured	Not configured	A
1 setting available	>	No operating system	build ranges		
ОК		ОК			



e.	Under System	Security,	configure	the following:
----	--------------	-----------	-----------	----------------

Windows 10 and I	10 compliance polic	y ×	System Security Windows 10 and later		l
Select a categ	ory to configure settings.		Password		
Device Health 3 of 3 settir	n O ngs configured	>	Require a password to unlock mobile devices. 🕤	Require	Not configured
Device Prope	rties 🚯	_	Simple passwords 🚯	Block	Not configured
5 settings a	vailable	>	Password type 🚯	Device defau	ılt 🗸
Configuratior 1 setting av	n Manager Compliance 🕦 railable	>	Minimum password length 👩	8	`
System Secur	ity	>	Maximum minutes of inactivity before password is required $oldsymbol{6}$	15 Minutes	~
16 settings	available		Password expiration (days) 🚯	90	
Windows Def 1 setting av	ender ATP 🚯	>	Number of previous passwords to prevent reuse $oldsymbol{ extsf{0}}$	3	
		_	Require password when device returns from idle state (Mobile and Holographic) 🕢	Require	Not configured

<	Windows 10 compliance policy Windows 10 and later	×	System Security Windows 10 and later] >
•	Select a category to configure settings.		Encryption of data storage on device. 🚯	Require	Not configured	
	Device Health ① 3 of 3 settings configured	>	Device Security			
	Device Properties 0 5 settings available	>	Firewall 🕜	Require Require	Not configured]
	Configuration Manager Compliance 🛛 🕺	- >	Antispyware 🕦	Require	Not configured]
	System Security 1 16 settings available	- >	Defender			
	Windows Defender ATP 🚯	_ >	Windows Defender Antimalware 🕦 Windows Defender Antimalware minimum version 🔀	Require Not configur	Not configured]
		-	Windows Defender Antimalware signature up-to-date	Require	Not configured]
-			Real-time protection ()	Require	Not configured	



f. Click Ok and Create

Dashboard > Device compliand	ce - Policies > Creat	e Policy > Windows 10 compliance policy		Dashboard > Device compliance -	Policies >
Create Policy	×	Windows 10 compliance p Windows 10 and later	\Box ×	Create Policy	
* Name	·	Select a category to configure settings.		* Name Windows Policy	~
Description		Device Health	>	Description Enter a description	~
Platform		Device Properties ① 5 settings available	>	* Platform	
Windows 10 and later	~	Configuration Manager Compliance 🚯	>	Windows 10 and later	~
Settings Configure	>	1 setting available System Security ①	> 	Settings 13 configured	>
Actions for noncompliance	>	10 of 16 settings configured		Actions for noncompliance 1 configured	>
1 configured Scope (Tags) 0 scope(s) selected	>	Windows Defender ATP () 1 setting available	>	Scope (Tags) 0 scor e(s) selected	>

g. Select Assignments and select the group of users you want this to apply to:

	≪ R Save X Discard ✓ Evaluate	Select 🕤
Overview	Include Exclude	AD AAD DC Administrators
Manage	Assign to	
Properties	Selected Groups	AU AD Users 47c1496a-3ae3-4b5d-a8b5-74d80d140021@wraireco
Assignments	Select groups to include	Adam2TectAgain
Monitor		
Device status	No assignments	Selected members:
User status		No members selected
Per-setting status		
	_	
		Select



Create Device Profile

Device profiles allow you to have uniform settings for all devices across your organization. Examples:

- You create a wifi profile that automatically configures the wifi on device that are enrolled with Intune
- Assume that you want to provision all iOS devices with the settings required to connect to a file share on the corporate network. You create a VPN profile that contains the settings to connect to the corporate network. Then you assign this profile to all users who have iOS devices. The users see the VPN connection in the list of available networks, and can connect with minimal effort.
- You want to have a uniform start menu and settings for all of your Windows 10 Devices. You can create this with a Device Restriction Profile
- Here is a list of the profiles that you can create:
 - o <u>Administrative templates</u>
 - o <u>Custom</u>
 - o <u>Delivery optimization</u>
 - o <u>Device features</u>
 - o <u>Device restrictions</u>
 - Edition upgrade and mode switch
 - o <u>Education</u>
 - o <u>Email</u>
 - o <u>Endpoint protection</u>
 - o <u>Identity protection</u>
 - o <u>Kiosk</u>
 - o <u>PKCS certificate</u>
 - o <u>SCEP certificate</u>
 - o <u>Trusted certificate</u>
 - o <u>Update policies</u>
 - o <u>VPN</u>
 - o <u>Wi-Fi</u>
 - Windows Defender ATP
 - o <u>Windows Information Protection</u>

Since we configured a policy in the previous section to Require Bitlocker, we are going to set up a profile for Bitlocker so that users are immediately prompted to configure if they do not have it already.



a. Go to the Device Management Admin Portal>Device Configuration>Profiles>Create Profile

Microsoft 365 Device Managem	ent	
«	Dashboard > Device configuration - Profile	5
료 Dashboard	Device configuration - Profiles	
i∃ All services	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	
- 🛨 FAVORITES	○ Search (Ctrl+/)	
🛃 Device compliance	Overview	✓ Search by name
듉 Device enrollment	Manage	PROFILE NAME
Conditional Access	Profiles	ATP
🚡 Security baselines	PowerShell scripts	BitLocker
Levice configuration	🚝 eSIM cellular profiles (Preview)	BitLocker Profile
🖵 Devices	Monitor	Device policy for Windows

b. Enter a Name, Description (if applicable), choose Windows 10 or later from the platform, and

* Name	
BitLocker Configuration	~
Description	
Enter a description	~
* Platform	
Windows 10 and later	~
Profile type	
Custom	~
Settings	`
Configure	/
Scope (Tags)	```
0 scope(s) selected	/

from Profile Type



c. Click Add

Custom (Windows 10 and	OMA-URI Settin	gs		
OMA-URI Se	ttings 🚯		Jn Add	Export
NAME		N 🔨 OMA-URI	↑↓ Add VALUE	î↓
No settings				

d. Enter the following, including: ./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption

Add OMA-UI	ROW RI Settings		
* N	lame 🚯	BitLocker	· · · · · · · · · · · · · · · · · · ·
De	scription 🚯	Enable BitLocker	· · · · · · · · · · · · · · · · · · ·
* 0	DMA-URI 🚯	./Device/Vendor/MSFT/BitLocker/	RequireDeviceEncr 💊
* 0	Data type 🚯	Integer	~
	* Value	1	
	ок		



e. Click Ok and Create

Dashboard > Device configuration - Profiles >	eate profile > Custom OMA-URI Settings		Dashboard > Device configuration - Profiles >
Create profile >	Custom OMA-URI Settings Windows 10 and later	\Box ×	Create profile
* Name BitLocker Configuration	OMA-URI Settings 🛛	Export	 ★ Name BitLocker Configuration
Description Enter a description	NAME ¹ DESCRIPTION ¹ OMA-URI ¹ VALUE		Description Enter a description
* Platform Windows 10 and later			* Platform Windows 10 and later ✓
* Profile type Custom ¥			* Profile type Custom
Settings > Configure			Settings >
0 scope(s) selected			Scope (Tags) > 0 scope(s) selected
Create			Create

f. Select Assignments and select the group of users you want this profile to apply to:

	🕞 Save 🗙 Discard 🗸 Evaluate	Select 🚯
(i) Overview	Include Exclude	AD AAD DC Administrators
Manage	Assign to	
Properties	Selected Groups	AU AD Users 47c1496a-3ae3-4b5d-a8b5-74d80d140021@wrajreco
🏜 Assignments	Select groups to include	AD Adam2TestAgain
Monitor		
Device status	No assignments	Selected members:
User status		No members selected
Per-setting status		
	_	
		Select



- ► Encryption needed Your work or school requires this device to be encrypted. Select this notification to encrypt this device.
- g. End users enrolled in Intune will get a notification to set up BitLocker

Are you ready to start encryption?

Disk encryption software other than BitLocker or Windows device encryption will prevent Windows from starting after you encrypt your device. If this happens, you'll need to reinstall Windows, and all data on your device will be lost.

I don't have any other disk encryption software installed.

Don't ask me again.

Learn more



Add an Application

Intune allows you to add application so that when users enroll they immediately have access to those applications via the Microsoft Store for Business, Company Portal App, or this apps can be required and automatically installed without end user interaction. The most common of these if the office Suite of which we will be configuring below:

a. In the Device Management Admin center go to Client Apps>Apps>Add

Microsoft 365 Device Manageme	ent			?
«	Dashboard > Client apps - Apps			
🛄 Dashboard	Client apps - Apps			
All services	Search (Ctrl+/) ≪	Add 🖸 Refresh 🝸 i	Filter 🞍 Export 🗮 Columns	
Device compliance	Overview	Search by name or publishe	<i>r</i>	
👼 Device enrollment	Manage	NAME T ₊	TYPE STATUS	
Conditional Access	Apps	Microsoft Authenticator	iOS store app	
Get Security baselines	App protection policies	Office Desktop Suite	Office 365 ProPlus Suite (Wi	
Levice configuration	R App configuration policies			
🖵 Devices	App selective wipe			
🔜 Software updates	💼 iOS app provisioning profiles			
Client apps	Monitor			
🔓 Users	App licenses			
📲 Groups	Discovered apps			
🍰 Roles	App install status			

b. Select Windows 10 under Office 365 Suite from the dropdown list:

Microsoft 365 Device Managem	ent
×	Dashboard > Client apps - Apps > Add app
료 Dashboard	Add app
i∃ All services	
+ FAVORITES	* App type
🛃 Device compliance	Store app
	Android
	iOS
Conditional Access	Windows Phone 8.1
늘 Security baselines	Windows
Device configuration	Managed Google Play
—	Office 365 Suite
Devices	Windows 10 Jm
Software updates	macOS
	Other
Client apps	Web link
よ Users	Built-In app
Croups	Line-of-business app
M Groups	Windows app (Win32)
🚣 Roles	



c. Under **Settings Format** select **Enter XML data** *Note* We are making this selection because we have M365 Business Plan. If we have a plan that comes with Proplus (E3,E5, M365 E3, M365 E5) we would select Configuration Designer:

Dashboard > Client apps - Apps > Add app	
Add app	
* App type	
Windows 10 V	
Use this type to assign Office 365 ProPlus apps to Windows 10 devices with Intune. This suite of applications will appear as one app in your apps list. Learn more.	
Settings format Configuration designer	
Configuration designer Enter XML data Configure the p suite information	
* Configure App Suite Select Office apps to be assigned	
* App Suite Settings Configure installation options for the a	

d. Under App Suite Information, configure the following and click ok:



Add app	«	×	App Suite Information
* App type Windows 10	~	•	 ★ Suite Name Office Business Suite ✓
Use this type to assign Office 365 ProPlu apps to Windows 10 devices with Intune This suite of applications will appear as one app in your apps list.	15 2.	l	 * Suite Description Office Business Suite ✓
Settings format Enter XML data	~	l	* Publisher Microsoft Category
* App Suite Information ① Configure the app suite inform	>	I	Productivity ✓ Display this as a featured app in the Company Portal 🗊
★ Enter XML data Enter XML data	>	I	Yes No
Scope (Tags) 0 scope(s) selected	>	•	Information URL
Add			ок



e. Go to https://config.office.com/ and sign in with your admin credentials

	\leftrightarrow \rightarrow C $($ https://	<mark>ss://config.office.com/</mark> officeSettings/configure#		☆ .	•
	Hicrosoft	Office Client	(ONICK RC	oss out
-	A Home DEPLOYMENT	Office Customization Tool Import Ex Learn more about the Office Customization Tool IC* Import Ex	port	Reset	
	Deployment config POLICY MANAGEMENT	Deployment settings			
	環 Policy configuration	Products and releases	~	c	01
		Architecture		Ge	ne
		Which architecture do you want to deploy?		Prov Con	vid np
				P	÷.

f. Select your appropriate architecture and select **Office 365 Business** from the dropdown:

Deploy	vment settings
	Architecture
	Which architecture do you want to deploy?
	🔿 32-bit
	● 64-bit



Office Customization Tool Learn more about the Office Customization Tool		Import Expo
Deployment settings		
Which products and apps do you want to deploy?		
Office Suites		
Office 365 Business		~
None		
Office 365 ProPlus		
Office 365 Business	վել	
Office Professional Plus 2019 - Volume License	Office 365 Business	
Office Standard 2019 - Volume License		
Additional Products		
Select Additional product		\sim

g. De-select any apps you do not want to deploy and choose **Monthly** for the update channel and **Latest** for the version

Access	On	Excel	On On	
OneDrive (Groove) 💽 Off	Skype for Business	On On	
OneDrive D	Desktop 🚺 On	OneNote 2016	Off Off	
Outlook	On On	PowerPoint	On On	
Publisher	On On	Teams	On On	
Word	On On			
Lindate char	anel			
opuate cha				
Select the u	update channel, which cont	rols the timing of feature	updates Learn more 🖃	
Select the u	update channel, which cont	rols the timing of feature	updates Learn more 🖃	~
Select the u	update channel, which cont Channel	rols the timing of feature	updates Learn more ㄷ	~
Select the u	update channel, which cont Channel	rols the timing of feature	updates Learn more ㄷî	~
Select the Monthly	update channel, which cont Channel	rols the timing of feature	updates Learn more 🗂	~
Select the Monthly	update channel, which cont Channel which controls the timi	rols the timing of feature	updates Learn more ⊏	~
Select the Monthly	update channel, which cont Channel which controls the tim	rols the timing of feature	updates Learn more 더 Learn more 더	~
Select the Monthly odate channel elect the update channel Monthly Channel	update channel, which cont Channel which controls the tim	rols the timing of feature	updates Learn more 🖂	
Control Select the Under Channel Select the Update channel Monthly Channel	update channel, which cont Channel which controls the tim	rols the timing of feature	updates Learn more 😅	~
Select the Monthly date channel elect the update channel Monthly Channel /hich version do you wan	update channel, which cont Channel which controls the tim t to deploy? Learn more	ing of feature updates	Learn more 🚅	~



h. Under Language select English or your primary language

Office Customization Tool Learn more about the Office Customization Tool 다	Import	Export
Deployment settings		
 Products and releases 		
← Language		
Languages Select primary language*		
English (United States)		\sim
Select additional languages		
Select additional languages	Upda	te
Next		

i. Under the Licensing and Activation section turn the Automatically Accept the EULA to On

Product key		
Product key settings only apply to vol	ume licensed products and suites	
KMS Client Key		
Product key entry is not required for Key	y Management Service (KMS) activation.	
Multiple Activation Key (MAK)		
Multiple activation key (MAK). Type a va	lid 25 character volume license key with no $\widehat{\mathfrak{sp}}$ aces.	
	ff.	



j. Leave all other settings defaulted and click Export

Hicrosoft	Office Client		\odot
Home DEPLOYMENT	Office Customization Tool Learn more about the Office Customization Tool	Imp	ort Export Re
區 Deployment config	Deployment settings		
POLICY MANAGEMENT	Deployment settings		
Policy configuration	∨ Language		
	\checkmark Installation		~
	\checkmark Update and upgrade		\checkmark
			\checkmark
	∨ General	ſm	\checkmark
	✓ Application preferences		\checkmark

k. Agree to the terms, name your file, and click export

Export configuration to XML	×
To export the file, you must accept the terms of the End User License Agreement (EULA).	
MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT OFFICE CUSTOMIZATION TOOL FOR CLICK-TO-RUN (PRE-RELEASE VERSION)	
These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to the software named above and any Microsoft services or software updates (except to the extent such services or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated software or services). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE PIGHTS BELOW, BY USING THE SOFTWARE YOU ACCEPT THESE TERMS.	-
File Name *	nent
Configuration	
L ₃ Export Cance	I



I. Open the XML file and copy the text:



m. Back in the Microsoft portal, click Enter XML Data, paste the text, and click ok

Add app	w X	Configuration File
Add app * App type Windows 10 Use this type to assign Office 1 apps to Windows 10 devices w this suite of applications will a one app in your apps list. Learn more. * Settings format Enter XML data * App Suite Information App suite information is co * Enter XML data Scope (Tags) O composite calcuted	 × 365 ProPlus vith Intune. appear as > ><	Configuration File Use the Office Customization tool to create the configuration files that are used to deploy Oflarge organizations. Learn more. <

n. Click Add



Add app	
Windows 10	~
Use this type to assign C Windows 10 devices with applications will appear list. Learn more.	Office 365 ProPlus apps to n Intune. This suite of as one app in your apps
* Settings format	
Enter XML data	~
* App Suite Information (App suite information	▶ n is configured
* Enter XML data 🕦 XML Data Entered	······································
Scope (Tags) 0 scope(s) selected	

o. Click on Assignments>Add Group, select your group and under Assignment type, select Required

Office Desktop Suite - Assigner Client Apps	ments « ×	Add g	roup	
	🛱 Save 🗙 Discard			F2
0 Overview	Add group	i	when excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn	
Manage			more.	
III Properties	GROUP ASSIGNME MODE	Calastan		
Assignments		this app.	oups where you want to assigr	I
Monitor	AVAILABLE FOR ENROLLED DEVICES	Assianme	nt type	
	No assignments, select 'Add group' to add a	Select a	ssignment type	
Device install status		Availabl	e for enrolled devices	
🏜 User install status	REQUIRED	Require	d 🜉	\ \
	Nicks Required Included	Uninsta	I Im	
	UNINSTALL	No grou Exclude	ups selected ed Groups	>
	No assignments select 'Add group' to add a			

p. When a user enrolls into Intune the xml file will be pushed and they will get office installed without any interaction:





Adding the Microsoft Authenticator App

The Microsoft Authenticator app is widely using for MFA that comes with M365 Business. You can add this app in Intune so that it is immediately available for download for your clients.

iOS

a. In the Device Management Admin center go to Client Apps>Apps>Add





b. Under App Type select **iOS**, then click **Select App**, then search for **Microsoft Authenticator** *NOTE* You will have to search for this text in its entirety for it to find this app:

. . .

Add app	« ×	Search the App Store			
* App type iOS	~	Microsoft Authenticator Found 3 apps			United States (defau
* Search the App Store Select app	>	NAME	↑↓	PUBLIS	HER
* App information Configure	>	Microsoft Authenticator		Micros	oft Corporation
Scope (Tags) 0 scope(s) selected	>	SAASPASS Authenticator 2FA MF/	A	SAASP	ASS
	\searrow	TOTP Authenticator – Fast 2FA		Арруға	actor

c. Select the app and click **Configure** under App Information. Say **Yes** for displaying app in Company Portal. Leave all other settings defaulted:

Add app	« ×	App information		\times
* App type		* Appstore URL	6	•
iOS	\checkmark	https://itunes.apple.com/us/app/micros	iot	
		* Minimum operating system		
 Search the App Store Microsoft Authenticator 	>	iOS 8.0	\sim	
		* Applicable device type		
* App information 🦰	>	2 selected	\sim	
Configure		Category		
Scope (Tags)	、 、	0 selected	\sim	
0 scope(s) selected		Display this as a featured app in the Company Portal 🕦		ł
		Yes No		
	2	Information URL		
		Enter a valid url	~	
		Privacy URL		
		Enter a valid url	1	•
Add		OK		



d. Click Add

Dashboard > Client apps - Apps > Add app	
Add app	
* App type iOS ~	
* Search the App Store > Microsoft Authenticator	
* App information > Configure	
Scope (Tags) > 0 scope(s) selected	



e. Click Assignments>Add Group>Select Required for Assignment Type. Save when complete





Android

a. In the Device Management Admin center>Client Apps>Apps>Add

Microsoft 365 Device Manageme	ent	¢ ¹ @ ?
«	Dashboard > Client apps - Apps	
🛄 Dashboard	Client apps - Apps	
E All services	○ Search (Ctrl+/)	≪ + Add ひ Refresh ▼ Filter ↓ Export ≡ Columns
- 🛨 FAVORITES	/*(//	- In the second se
🛃 Device compliance	1 Overview	> Search by name or publisher
👼 Device enrollment	Manage	NAME ¹ J TYPE STATUS
Conditional Access	Apps	Microsoft Authenticator iOS store app
💼 Security baselines	App protection policies	Office Desktop Suite Office 365 ProPlus Suite (Wi
Levice configuration	App configuration policies	
Cevices	App selective wipe	
🤜 Software updates	📲 iOS app provisioning profiles	
Client apps	Monitor	
🎍 Users	App licenses	
📲 Groups	Discovered apps	
Sector Roles	App install status	
🗙 Troubleshoot		

b. For App Type, select **Android** and fill out the fields as follows, including the following for AppStore URL:

https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US

Add app	« ×	App information		>
* App type		* Name		
Android	\sim	Microsoft Authenticator Android	~	
* App information		* Description		
Configure	>	Microsoft Authenticator Android	~	
Scope (Tags)	>	* Publisher		
0 scope(s) selected		Microsoft	~	
		* Appstore URL		
		s?id=com.azure.authenticator&hl=en_US	~	
\searrow		* Minimum operating system		
		Android 4.0 (Ice Cream Sandwich)	~	
		Category		
		0 selected	~	
		Display this as a featured app in the Company Portal 🚯		
		OK		



c. Click Add

d. Click Assignments>Add Group>Select Required for Assignment Type. Save when complete





Set up Apple MDM Push Certificate

The Apple MDM Push Certificate allows us to start enrolling iOS devices. You can think of this cert as a shell account in which you can put all over your customers under. The certificate is associated with the Apple ID used to create it. As a best practice, use a company Apple ID for management tasks and make sure the mailbox is monitored by more than one person like a distribution list. Never use a personal Apple ID.

a. In the Device Management Admin Center go to **Device Enrollment>Apple Enrollment>Apple MDM Push Certificate**



b. Agree to the terms and conditions, Download you CSR (save to another location or keep in downloads. The file is used to request a trust relationship certificate from the Apple Push Certificates Portal.), and click **Create your MDM Push Certificate** to open the Apple center

	HIPAABusinessAssociateAgr(WW)(ENG)(Februar	9/30/2018 1:54 PM	Microsoft Word Doc	51 KB
	☑ IMG_1436	10/28/2018 8:18 PM	JPG File	53 KB
7	IntuneCSR.csr	11/2/2018 12:43 PM	CSR File	10 KB
×	🔋 invoice-48365	10/24/2018 4:32 PM	PDF File	59 KB
OCE	invoice-51422	10/4/2018 1:19 PM	PDF File	42 KB
าร	🔋 invoice-51913	10/4/2018 1:18 PM	PDF File	62 KB
	🔋 invoice-55188	10/22/2018 12:23 PM	PDF File	64 KB



🔟 Del	ete
t eps:	I grant Micrusoft permission to send both user and device information to Apple. More information.
_	✓ * I agree.
2.	Download the Intune certificate signin request required to create an Apple MDM push certificate.
3.	Create an Apple MDM push certificate. More information
4.	Enter the Apple ID used to create your Apple MDM push certificate.

c. Sign in with your Business Apple ID or create a new Apple account for your business if you do not have one already. (takes 5 min and no financial commitment)

Sig	ın In.				N			
Apple	e ID				43°			
Forg	got your Apple IC	??				-	1	
Pass	sword					6 . 9		
Forg	got your passwor	rd?	Sign	In				

d. After you sign in click Create Certificate





Apple Push Certificates Portal	nross@wra
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 Choose File IntuneCSR.csr	
Cancel Upload	JHP







Delete	
4.	Enter the Apple ID used to create your Apple MDM push certificate.
	* Apple ID
	nross@wrajrecords.com
	\sim
5.	Browse to your Apple MDM push certificate to upload
	* Apple MDM push certificate
	"MDM_Microsoft Corporation_Certificate.pem"

e. Back in Microsoft enter you Apple ID and upload the MDM Cert you just downloaded

🤊 🍸 T 🏴	> 1 ni:	s PC > Downloads				↓ 0	Search Downloads
nize • New	/ folde	r					-
Juick access		Name	Date modified	Туре	Size		
Desktop	*	MDM_ Microsoft Corporation_Certificate.pem	11/2/2018 1:09 PM	PEM File	2 KB		
Downloads	*						
Documents	*						
Pictures	*						
Azure Transfer	Proce						
BitTitan Migrat	ions						
NickRoss							
OneDrive - PA	X8						
neDrive - PAX	В						
his PC							
letwork							
					N		
					3		



f. You will see the status as active

Configure MDM Push C	Configure MDM Push Certificate						
🔟 Delete							
Status: Active		Days Until Expiration: 217					
Last Updated: 12/3/2018		Expiration: 11/2/2019					
Apple ID: nross@wrajrecords.com	\searrow	Subject ID com.apple.mgmt.External.5931b72a-83a1-4f12-8829-c93e4d9d2					
		*					

Setting Up Android Enrollment

Setting up Android enrollment requires that you link Intune to an existing Google Play account. If you do not have one you can create one for your business. You can think of this cert as a shell account in which you can put all over your customers under. As a best practice, use a company Google Account for management tasks and make sure the mailbox is monitored by more than one person like a distribution list. Never use a personal Google Account.

a. In the Device Management Admin Portal, go to **Device Enrollment>Android** Enrollment>Managed Google Play

Microsoft 365 Device Managem	nent	c ^e ج nross
«	Dashboard > Device enrollment - And	ndroid enrollment
🖪 Dashboard	Device enrollment - Androi Microsoft Intune	oid enrollment
All services FAVORITES	, ≶earch (Ctrl+/)	By default, all Android devices, including those that support Android Enterprise, can b conventional Android devices. To enable management of the Work Profile and other <i>i</i>
Device compliance	1 Overview	 functionality, configure Managed Google Play below. Learn More.
5 Device enrollment	🝊 Quick start	Prerequisites
Conditional Access	Manage	Managed Google Play
🗣 Security baselines	Apple enrollment	Link your managed Google Play account to Intune.
L Device configuration	Android enrollment	
🖵 Devices	Windows enrollment	Android Enterprise
🧔 Software updates	Terms and conditions	Personal devices with work profile
Client apps	Enrollment restrictions	
🛓 Users	Device categories	Corporate-owned dedicated devices
Groups	La Corporate device identifiers	Manage device owner enrollments for klosk and task devices.



b. Agree to the terms and conditions and click Launch Google to Connect now

Managed Google Play	
🕪 Disconnect	
Status:	Google Account: Not Available
Organization: Not Available	Registration Date: Not Available
	*
You must connect Intune to your company's n to enable Android enterprise enrollment. Lear	nanaged Google Play account to manage Android enterp n More.
You must connect Intune to your company's n to enable Android enterprise enrollment. Lear 1. I grant Microsoft permission to send both u I agree.	nanaged Google Play account to manage Android enterp n More. user and device information to Google. Learn More.

c. Sign in to your business Google Account. If you do not have one Create one now. Click Get Started:





d. Enter your Business Name and click Next

Business We need some detai	NAME Is about your business		
Business name			
Your answer			
Enterprise mobility m	anagement (EMM) provider		
Microsoft Intune	2	Previous	Next

e. If you are in the EU, you can enter the contact of an EU representative. If not, simply agree to the terms and click confirm:

Phone	_	
EU Representative		
Name		
Email		
Phone	_	
✓ I have read and agree to the	Managed Google Play agreement.	
	Previous	Confirm



f. Click Complete Registration and you will be redirected back to Microsoft



g. You will get a green check for the status. Registration is complete.



You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the s to enable Android enterprise enrollment. Learn More.

1. I grant Microsoft permission to send both user and device information to Google. Learn More.



2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

Launch Google to connect now.



Setting Up 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
- Access resources like company apps and email.
- a. In the Device Management Admin Portal, go to **Device Enrollment>Terms and Conditions>Create**





b. Name your company terms and then define them in the **Define Terms of Use** tab:

Create Terms and Condition	\times s	Terms and Conditions		×
* Display name: 🚯		Enter a title, brief summary of what it means to accept your terms and conditions, and the	2	
Company Terms	✓	terms that the user must agree to. See how this displays to users.		
Description: 🚯		* Tiller •		
Optional		Company X Terms and Conditions	~]
		* Summary of Terms: 👩		
		By enrolling your device, you agree to Company X terms and conditons	~	
Define term of use Not Defined	>			
		* Terms and Conditions: 👩		
Create	6	I acknoledge that by enrolling my device, Company X Administrators have certain types of control. This includes visibility into coporate app inventory, email usage, and device risk. I further agree to keep company resources safe to the best of my ability and inform Company X administrators as soon as I believe my device is lost or stolen.	~	
		Ok]

Ex. Summary of Terms

By enrolling your device, you agree to <Company X> terms and conditions

Ex. Terms and Conditions

I acknowledge that by enrolling my device, <Company X> Administrators have certain types of control. This includes visibility into corporate app inventory, email usage, and device risk. I further agree to keep company resources safe to the best of my ability and inform <Company X> administrators as soon as I believe my device is lost or stolen.

c. Click Ok and then **Create**

Dashboard > Device enrollment - Term	s and	cond	liti
Create Terms and Conditi		\times	
* Display name: 🚯			
Company Terms	~		
Description: 🚯		_	
Optional]	
		-	
★ Define term of use 🚯	、		
Defined	/		
_ 0			
Creeling			



d. Click on the Policy after creation and click **Assignments** to assign the Terms to All Users or a select group:

Dashboard > Device enrollment - Terms Company Terms - Assignmen	Select groups to include Azure AD groups	
Terms and conditions		
	R Save X Discard	Select o Search by name or email address
() Overview	Assign to	AAD DC Administrators
Manage	Selected Groups	
III Properties	All Users	AD AdminAgents
🝰 Assignments		
Monitor	No assignments	AD ADSyncAdmins
Acceptance Reporting		Selected members:
		No members selected

Add Company Branding

Company Branding allows you to white label the end user experience when they are enrolling their device to Intune. This applies to both existing devices that are just now enrolling and OOBE for new devices.



a. In the Device Management Admin portal, go to Client Apps>Branding and customization



b. Enter Company name and all other information you want to include. Notice there is a preview button so you can view your changes in real-time

📙 Save 🛛 Preview 💍 F	Refresh
Enter your company's support information, along with the cus Learn more	information to provide your employee with a contact for Intune-related c tom settings you configure, will be visible throughout the Intune user ex
Company information	
* Company name: 🚯	(max 40 characters)
Privacy statement URL: 🕦	https://www.example.com (max 79 characters)
Support information	
Contact name:	(max 40 characters)
Phone number: 🔀	(max 20 characters)
Email address:	someone@example.com (max 40 characters)
Website name: 🚯 🛛 🍃	(max 40 characters)
Website URL:	https://www.example.com (max 150 characters)
Additional information: 🛭	(max 120 characters)

c. Choose your Theme and upload your logo. When done, click Save

соптрану шеницу втанинну

^	Theme color and logo in the Company Portal	
	Select a standard color or enter a six-digit hex code for a custom color.	Standard Custom
	Choose theme color	Blue
	Display	Company name only
	Ν	Text color: White 🚯
^	Logo to use on white or light background	
	Upload your logo	Select a file



Enroll Devices: Windows

Recycle	Bin		
≡	All Apps Documents Settings V	Web	More 🔻 Feedback …
ŵ	Best match		
0	Access work or school System settings	\rightarrow	
Į.	Settings		Access work or school
	Ease of Access keyboard settings	>	System settings
	Ease of Access brightness setting	>	
	d ・ Ease of Access audio settings	>	다 Open
	- 染 Ease of Access high contrast settings	>	
	Use Sticky Keys to press one key at a time for keyboard shortcuts	>	
	Use Toggle Keys to hear a tone when	>	

a. On the Windows 10 Device, click Start and type Access Work or School

b. Click Connect





c. Click Join this device to Azure Active Directory

You'll get access to re work or school might	sources like emai control some thi	l, apps, and tł ngs on this de	ne networ evice, such	k. Conne 1 as whic	ecting means y h settings vou
change. For specific in	fo about this, asl	k them.	,		5-7
Email address					
		2			
Alternate actions:					
Alternate actions: These actions will set full control over this d	up the device as evice.	your organiza	tion's and	d give yo	ur organizatic
Alternate actions: These actions will set full control over this d Join this device to Azu	up the device as evice. rre Active Directo	your organiza	tion's and	d give yo	ur organizatic
Alternate actions: These actions will set full control over this d Join this device to Azu Join this device to a lo	up the device as evice. rre Active Directo cal Active Directo	your organiza ry ory domain	tion's and	d give yo	ur organizatic

d. Sign-In with the Users Azure AD credentials

Let's get you signed in

Work or school account

someone@example.com

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

Privacy statement

Next



e. When prompted, click Join

Make sure this is your organization

Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC. Is this the right organization? Connecting to: wrajrecords.com User name: nross@wrajrecords.com User type: Administrator

f. You will get a success message when complete. If this is the first device the user is enrolling, you will be first given Terms and Conditions to accept

You're all set!							
This device is connected to wraj records!.							
When you're ready to use this new account, select the Start button, select your current account picture, and then select 'Switch account'. Sign in using your nross@wrajrecords.com email and password.							
l∂							
	Done						



g. Back in the Intune Portal, you can go to **Device Compliance>Policies>Click on your Windows Policy** (we created earlier in this document)

Micr	flicrosoft 365 Device Management									
		×	Dashboard > Device	complianc	oliance - Policies					
Dashboard Device compliance -			nce - Po	olicies						
;≡, -★	W Devi	indows - Dev	ice status							
ا 🜄 ا	0	Search (Ctrl+/)		«	🔳 Columns 🚽 Exp	port				
0 0 0	0	Overview			i Data in this view is live.					
	Manage				✓ Filter items					
- -	111	Properties			DEVICE	↑↓	USER PRINCIPAL NAME	↑↓	COMPL	IANCE STATUS
		Assignments			DESKTOP-MEO0NQ6		None		Not e	valuated
	Мо	nitor			DESKTOP-TRBCT6F		jsonnier@wrajrecords.	com	😣 No	t Compliant
* i *		Device status			WindowsAuto		None		Not e	valuated
		User status			2					
		Per-setting status								

h. You can click on **Device status** to see compliance status. Note, it can take some time before the evaluation will complete. In this case, I see the device I just joined as "Not Evaluated". We just must wait for that to complete.

Monitoring

I can come back in later to see that it is in error:

== Columns 👱 Export			
1 Data in this view is live.			
,⊖ Filter items			
DEVICE	↑↓ USER PRINCIPAL NAME	E THE DEPLOYMENT STATUS	↑↓ LAST STATUS UPDATE
DESKTOP-MEO0NQ6	None	Pending	
DESKTOP-TRBCT6F	jsonnier@wrajrecord	ds.com 😢 Failed	1/10/19, 10:57 AM
WindowsAuto	nross@wrajrecords.	com 🚽 🕕 Error	3/30/19, 5:20 PM
	Ν		



WindowsAuto					
, Search (Ctrl+/)	*	🗙 Retire 🍤 Wipe 🗴 Delete 🔒 R	Remote lock 🔇 Sync	🔎 Reset passcode	U Restart
Overview	-	Device name WindowsAuto		Enrolled by User Nick Ross	
Manage		Management name nross_Windows_3/30/2019_9:01 PM		Compliance Not Compliant	
Properties		Ownership Corporate		Operating system Windows	
Monitor		Serial number		Device model	
🖡 Hardware		0000-0013-4890-0606-7785-1571-70		Virtual Machine	
Discovered apps	1	Phone number		Last check-in time 3/30/2019, 5:20:18	PM
🚦 Device compliance 🦰		See more			
Device configuration			\$	8	
App configuration		Device actions status			
💼 Security baselines		ACTION	STATUS		DATE/TIME
🚴 Managed Apps		No results			

a. Click on this line item and the go to **Device Compliance** on the next page:

b. Click on Windows as it is our policy

Dashboard > Device compliance - Policies > Windows > Device status > WindowsAuto - Device compliance

WindowsAuto - Devic	ce complia	nce				
	*	↓ Export				
Overview						
Manage		POLICY	τţ	USER PRINCIPAL NAME	\uparrow_{\downarrow}	STATE
Properties	- 1	Built-in Device Com	pliance Policy	nross@wrajrecords.com		📀 Compliant
Monitor		Windows	-{lmj	nross@wrajrecords.com		 Error
Hardware			0			
Discovered apps						
Device compliance						



c. Here you can see why the device is out of compliance and take action steps to remediate. In this case it looks like we just need to finish setting up BitLocker to encrypt the drive:

Vindows olicy settings			
Export			
SETTING îų	STATE	\uparrow_{\downarrow}	STATE DETAILS
Antispyware	🛇 Compliant		
Number of non-alphanumeric characters in passw	📀 Compliant		
Antivirus	📀 Compliant		
Password expiration (days)	📀 Compliant		
Encryption of data storage on device.	1 Error		-2016281112 (Remediation failed)
Minimum password length	🛇 Compliant		
Maximum minutes of inactivity before password is	Not applicable		
Password type	🛇 Compliant		
Firewall	🛇 Compliant		
Require BitLocker	Not applicable		

Enroll Devices: iOS and Android

iOS and Android device enrollment can be completed by downloading the Intune Company Portal app from the app store or google play store:





a. Users will be walked through a wizard after they enter their Azure AD credentials which begins with the following:



b. For a detailed list of the entire user experience, you can follow this support guide from Microsoft:

<u>iOS</u>

<u>Android</u>

Pilot Testing and Remediation

During our Pilot we want to discover:

- Common FAQs
- Whether we need to tighten or loosen our policies



- End User Experience for Communications to Broad audience
- Common Troubleshooting Techniques for each platform

After this is complete, we want to create communications to our audience for enrollment:

- Why is this service important?
- What pain points will it help them solve?
- What can end users expect?
- What are the steps to get my device enrolled

Lastly, after we have this pushed out and a target date for deployment, we can go back into the Device Management Admin Center and begin to add our groups to our policies and profiles:

a. Go to Device Compliance and click on policy you want to add a group to:



b. Go to **Assignments** and select your groups that you want to apply the policy to. You can do the same with **Device Profiles** by going to the **Device Configuration** section

×	Dashboard > Device compliance - Policies	s > Windows - Assignments
🗔 Dashboard	Windows - Assignments	
Ξ All services	«	Save X Discard V Evaluate
— ★ FAVORITES —————	Search (Ctrl+/)	
Device compliance	() Overview	Include Exclude
듉 Device enrollment	Manage	Assign to
Conditional Access	III Properties	Selected Groups
🔓 Security baselines	Assignments	Select groups to include
Levice configuration	Monitor	- Chm
Devices	Device status	No assignments
Software updates	User status	
Client apps	Per-setting status	



Microsoft 365 Device Manag	Microsoft 365 Device Management									
	«	Dashboard > Device configuration	- Profile	s						
🖪 Dashboard		Device configuration - Pro	ofiles							
🗄 All services — 🗙 FAVORITES ————————————————————————————————————			~	•	Create profile	Columns	T Filter	U Refresh		
🛃 Device compliance	•	(i) Overview	Â	[𝒫 Search by name					
듉 Device enrollment		Manage			PROFILE NAME	\uparrow_{\downarrow}	PLATF $\uparrow \downarrow$	PROFILE TYP		
Conditional Access		🖭 Profiles			АТР		Windows	Windows D		
🔓 Security baselines	E	PowerShell scripts		-	BitLocker		Windows	Custom		
Device configuration		🚝 eSIM cellular profiles (Preview)		-	BitLocker Configuration		Windows	Custom		
The Devices		Monitor	43	· _	BitLocker Profile		Windows	Administra		
Client apps		Assignment status		-	Device policy for Windo	ows 10	Windows	Device rest		

Conclusion

I hope this article provided you some targeted guidance on implementing Intune. Any feedback to improve your experience would be greatly appreciated. I would also like to hear if there is more content that you would like to see in this guide. Any feedback can be sent to my email below:

Msp4msps@tminus365.com

