



Intune Implementation Guide

Guide Description

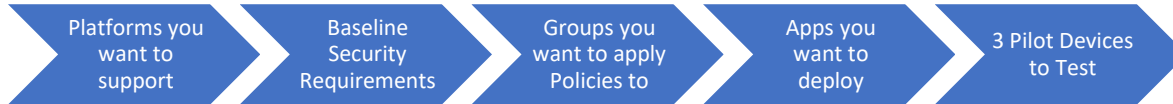
*The purpose of this guide is to lay out the steps for implementing Intune. This guide is assuming you have the **M365 Business** License. It can apply to EMS licenses but some features will not be covered such as Conditional Access and Windows Autopilot. After you complete this guide you will have:*

- *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



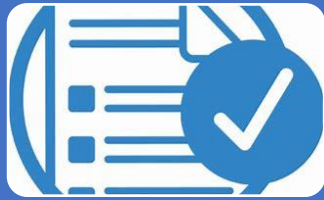
- a. Determine Platforms that you will support
 - i. IOS/Android
 - ii. MAC/Windows
- b. Have baseline security requirements compiled that you want to implement
 - i. Min/Max OS versions
 - ii. Password Requirements
 - iii. Encryption Enabled
- c. Determine if there will be separate groups for separate 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 appropriate Licensing
- Add Necessary Groups for Policy Assignment
- Configure Device Autoenrollment



Phase 2: Policy and Profile Creation

- Configure Device Policies
 - iOS
 - Android
 - Windows
- Create Device Profile



Phase 3: Add Apps

- Adding Applications
- Adding Microsoft Authenticator App



Phase 4: Configuring Enrollment

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



Phase 5: Enroll Devices

- Enroll Devices: Windows
- 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](#)
- [Configure Device Autoenrollment](#)

Phase 2: Policy and Profile Creation

- [Configure Device Policies](#)
 - [iOS](#)
 - [Android](#)
 - [Windows](#)
- [Create Device Profiles](#)

Phase 3: Add Apps

- [Adding Applications](#)
- [Adding Microsoft Authenticator App](#)

Phase 4: Configuring Enrollment

- [Setting Apple Enrollment](#)
- [Setting Android Enrollment](#)
- [Setting Terms and Conditions](#)
- [Adding Company Branding](#)

Phase 5: Enrolling Devices

- [Enroll Devices: Windows](#)
- [Enroll Devices: iOS and Android](#)

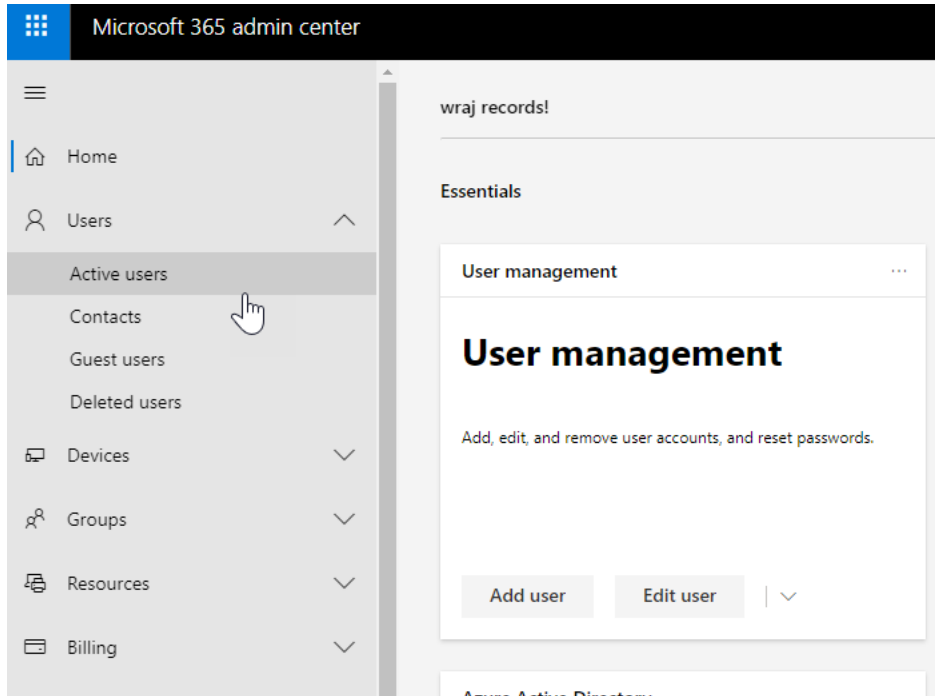
Phase 6: Testing and Broad Deployment

- Pilot Testing and Remediation

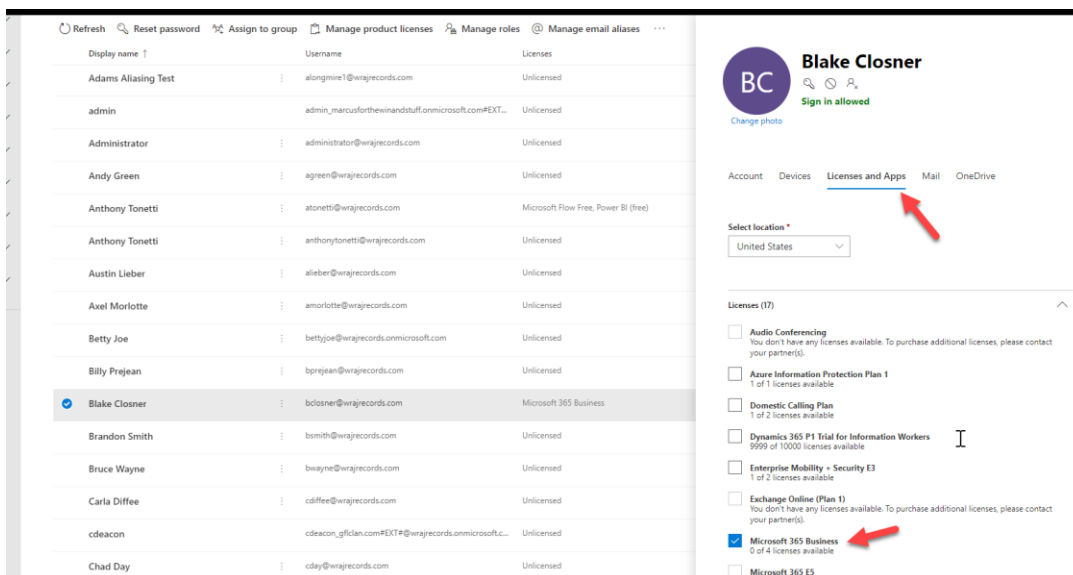
Licensing Users

1. Ensure All appropriate Users are Licensed

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



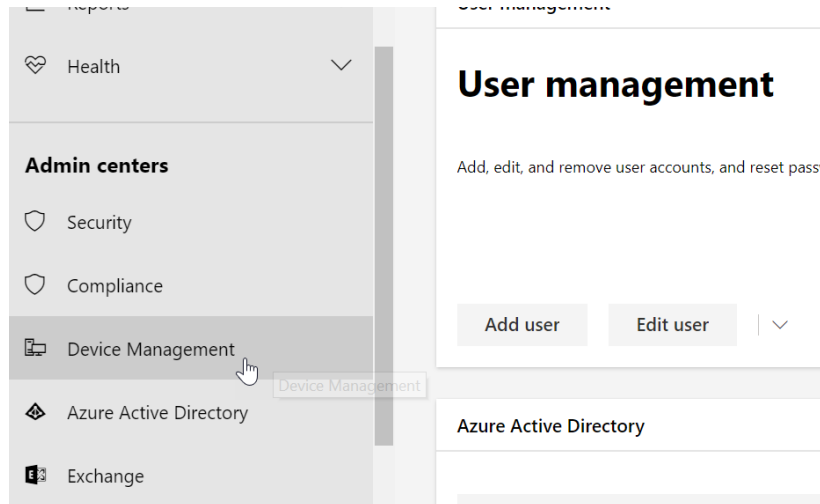
b. Select a User > Click **Licenses and Apps** > Ensure an M365 License is Assigned



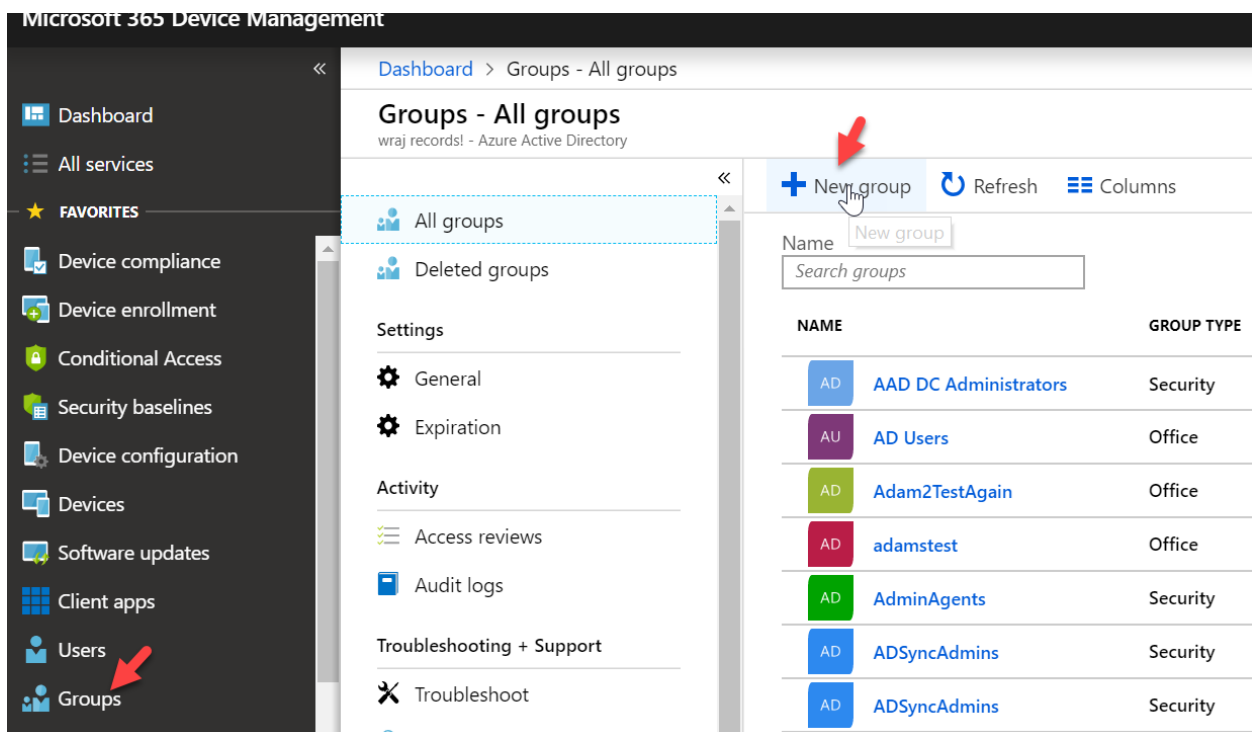
Create Groups

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

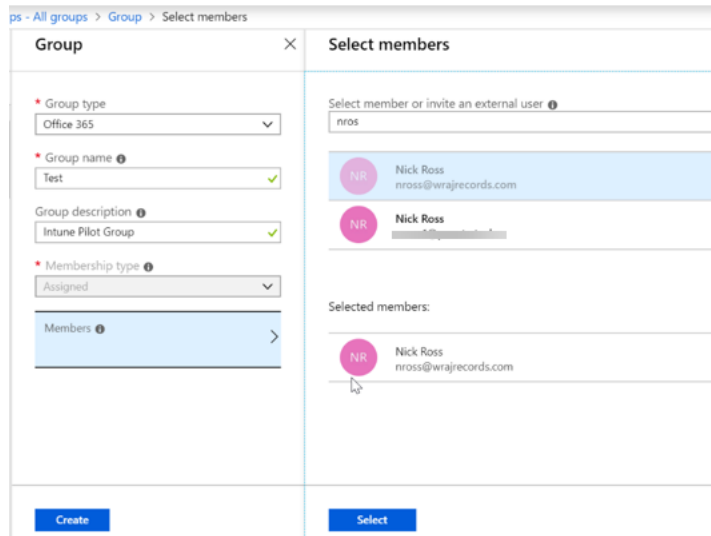
- a. Scroll Down in the 365 Admin Portal and Go to the **Device Management Portal**



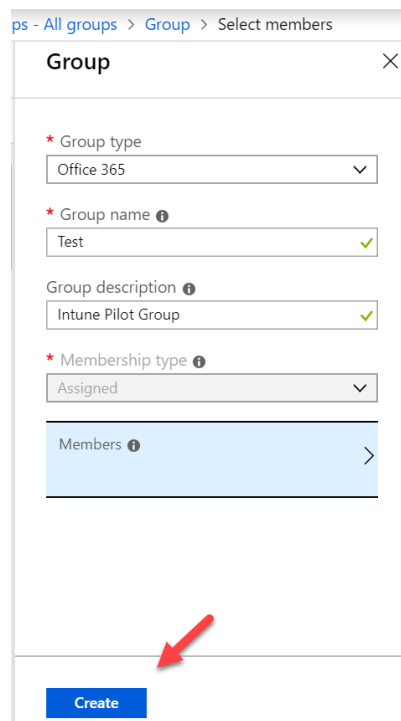
- b. Click on **Groups** and click **New Group**



- 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



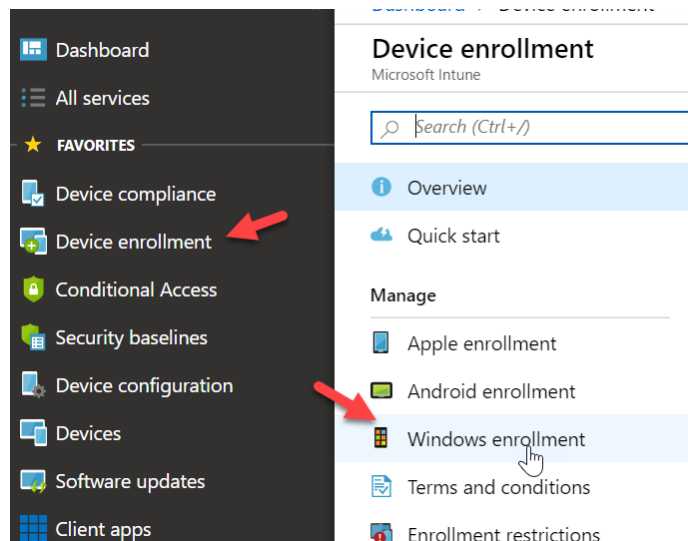
- d. Click **Create** when finished



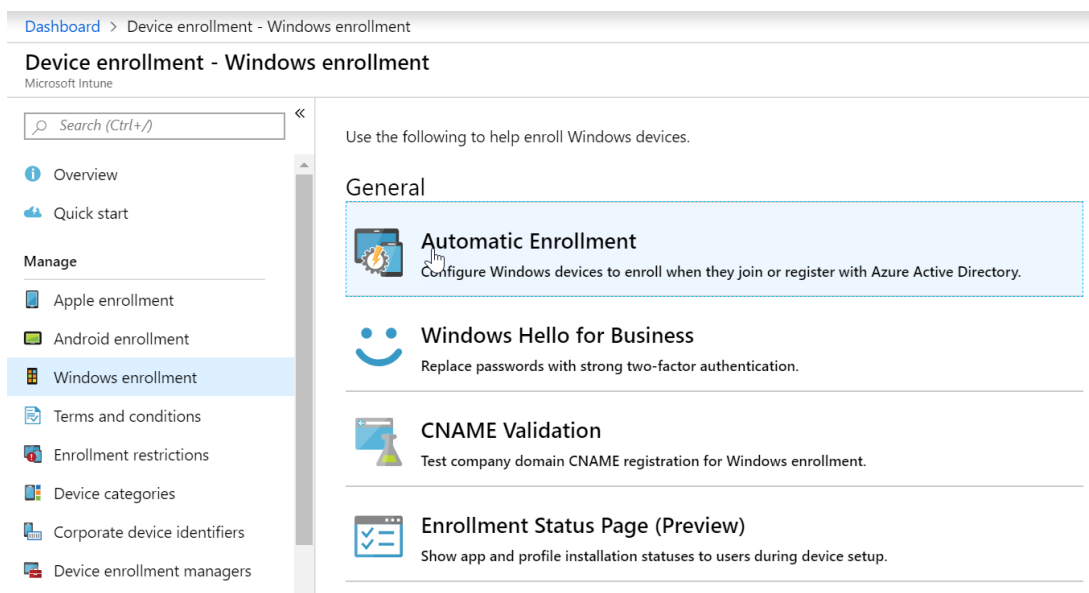
Device Autoenrollment

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

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 ⓘ

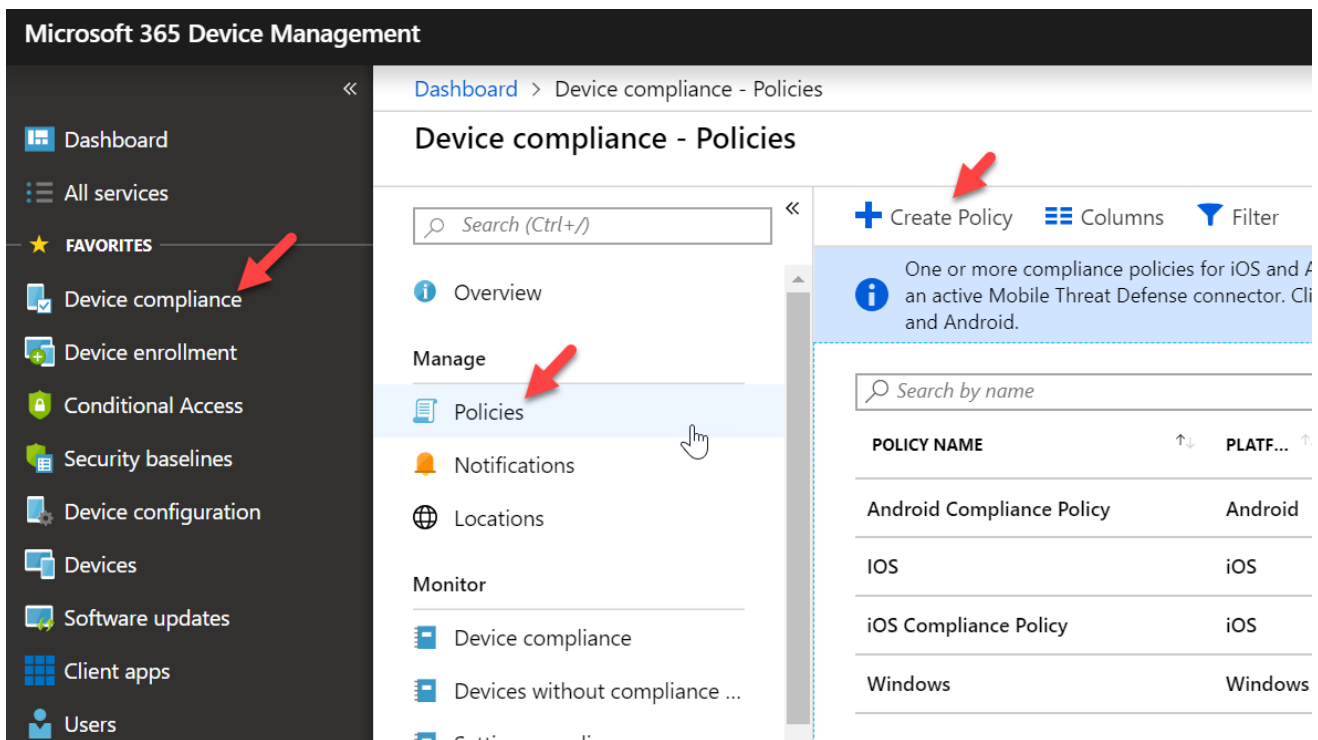
[Restore default MAM URLs](#)

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**



Microsoft 365 Device Management

Dashboard > Device compliance - Policies

Device compliance - Policies

Search (Ctrl+J)

[+ Create Policy](#)
[Columns](#)
[Filter](#)

One or more compliance policies for iOS and Android require an active Mobile Threat Defense connector. Click here for more information.

Search by name

POLICY NAME	PLATF...
Android Compliance Policy	Android
iOS	iOS
iOS Compliance Policy	iOS
Windows	Windows

- 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

Dashboard > Device compliance - Policies > Create Policy

Create Policy [X]

* Name
 ✓

Description
 ✓

* Platform
 ^

Select a platform

- Android
- Android enterprise
- iOS**
- macOS
- Windows Phone 8.1
- Windows 8.1 and later
- Windows 10 and later

Create

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

Dashboard > Device compliance - Policies > Create Policy > iOS compliance policy > Device Health

iOS compliance policy [X] | **Device Health** [X]

Select a category to configure settings.

- Email ⓘ 1 setting available >
- Device Health ⓘ 2 settings available >**
- Device Properties ⓘ 4 settings available >
- System Security ⓘ 10 settings available >

Jailbroken devices ⓘ **Block** Not configured

Require the device to be at or under the Device Threat Level ⓘ Not configured ▾

OK | OK

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

hboard > Device compliance - Policies > Create Policy > iOS compliance policy > Device Properties

iOS compliance policy
iOS

Select a category to configure settings.

- Email ⓘ
1 setting available >
- Device Health ⓘ
2 settings available >
- Device Properties ⓘ
4 settings available >
- System Security ⓘ
10 settings available >

OK

Device Properties
iOS

Operating System Version

Minimum OS version ⓘ

Maximum OS version ⓘ

Minimum OS build version ⓘ

Maximum OS build version ⓘ

OK

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

hboard > Device compliance - Policies > Create Policy > iOS compliance policy > System Security

iOS compliance policy
iOS

Select a category to configure settings.

- Email ⓘ
1 setting available >
- Device Health ⓘ
2 settings available >
- Device Properties ⓘ
4 settings available >
- System Security ⓘ
10 settings available >

OK

System Security
iOS

Require a password to unlock mobile devices. ⓘ Require Not configured

Simple passwords ⓘ Block Not configured

Minimum password length ⓘ ✓

Required password type ⓘ ▼

Number of non-alphanumeric characters in password ⓘ ▼

Maximum minutes after screen lock before password is required ⓘ ▼

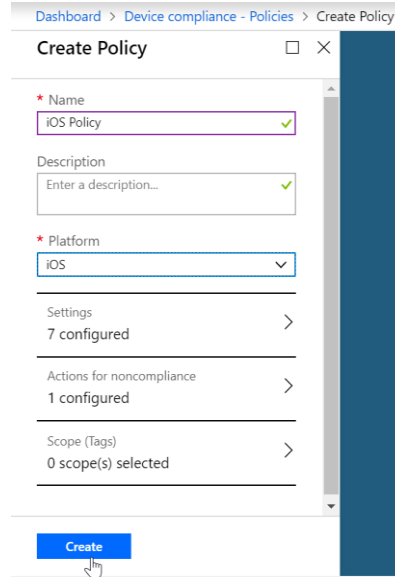
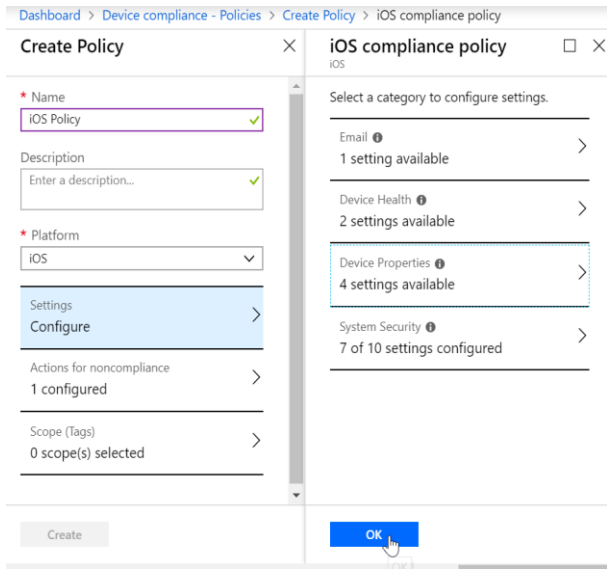
Maximum minutes of inactivity until screen locks ⓘ ▼

Password expiration (days) ⓘ ✓

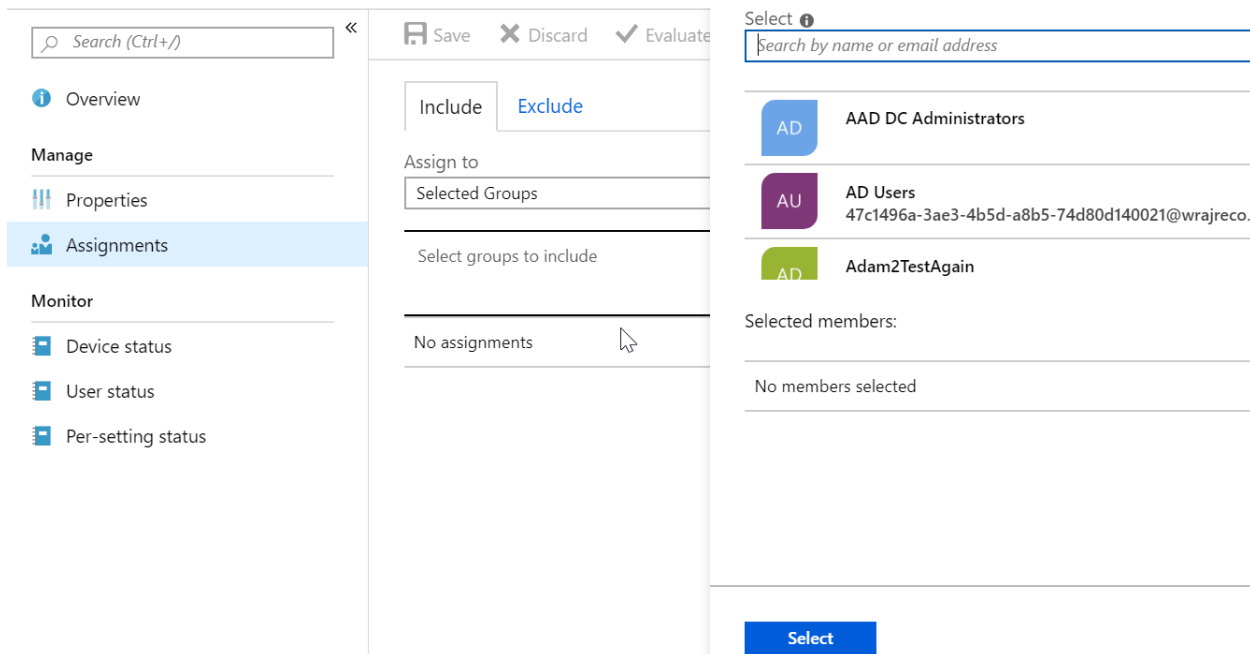
Number of previous passwords to prevent reuse ⓘ ✓

OK

f. Click ok and then Create



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



Android

- a. Click Create Policy

POLICY NAME	PLATF...	POLICY TYPE
Android Compliance Policy	Android	Android com
IOS	iOS	iOS compliar
iOS Compliance Policy	iOS	iOS compliar
Windows	Windows ...	Windows 10

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

Dashboard > Device compliance - Policies > Create Policy

Create Policy

* Name

Description

* Platform

- Select a platform
- Android
- Android enterprise
- iOS
- macOS
- Windows Phone 8.1
- Windows 8.1 and later
- Windows 10 and later

Scope (Tags)

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

Android compliance policy (Android) ×

Select a category to configure settings.

- Device Health ⓘ 6 settings available >
- Device Properties ⓘ 2 settings available >
- System Security ⓘ 10 settings available >

Device Health (Android) □ ×

- Rooted devices ⓘ **Block** Not configured
- Require the device to be at or under the Device Threat Level ⓘ Not configured ▾
- Google Play Protect
- Google Play Services is configured ⓘ **Require** Not configured
- Up-to-date security provider ⓘ **Require** Not configured
- Threat scan on apps ⓘ **Require** Not configured
- SafetyNet device attestation ⓘ Not configured ▾

OK OK

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 > Create Policy > Android compliance policy > Device Properties

Android compliance policy (Android) ×

Select a category to configure settings.

- Device Health ⓘ 3 of 6 settings configured >
- Device Properties ⓘ 2 settings available >
- System Security ⓘ 10 settings available >

Device Properties (Android) □ ×

- Operating System Version
- Minimum OS version ⓘ Not configured
- Maximum OS version ⓘ Not configured

OK OK

e. Under **System Security**, configure as follows:

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

Android compliance policy ✕

Android

Select a category to configure settings.

Device Health ⓘ
3 of 6 settings configured >

Device Properties ⓘ
2 settings available >

System Security ⓘ
10 settings available >

System Security □

Android

Require a password to unlock the device. If not configured, the use of passwords is optional, and left up to the user to configure.

[Learn more](#)

Require a password to unlock mobile devices. ⓘ Require Not configured

Required password type ⓘ Numeric complex ▾

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 ✓

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

Android compliance policy ✕

Android

Select a category to configure settings.

Device Health ⓘ
3 of 6 settings configured >

Device Properties ⓘ
2 settings available >

System Security ⓘ
10 settings available >

System Security □ ✕

Android

Encryption

Encryption of data storage on device. ⓘ Require Not configured

Device Security

Block apps from unknown sources ⓘ Block Not configured

Company Portal app runtime integrity ⓘ Require Not configured

Block USB debugging on device ⓘ Block Not configured

Minimum security patch level ⓘ Not configured

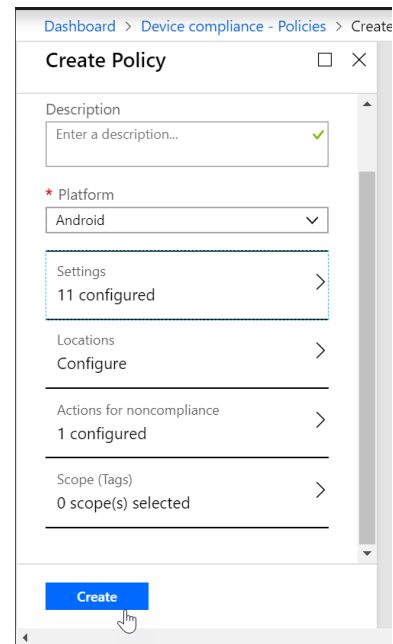
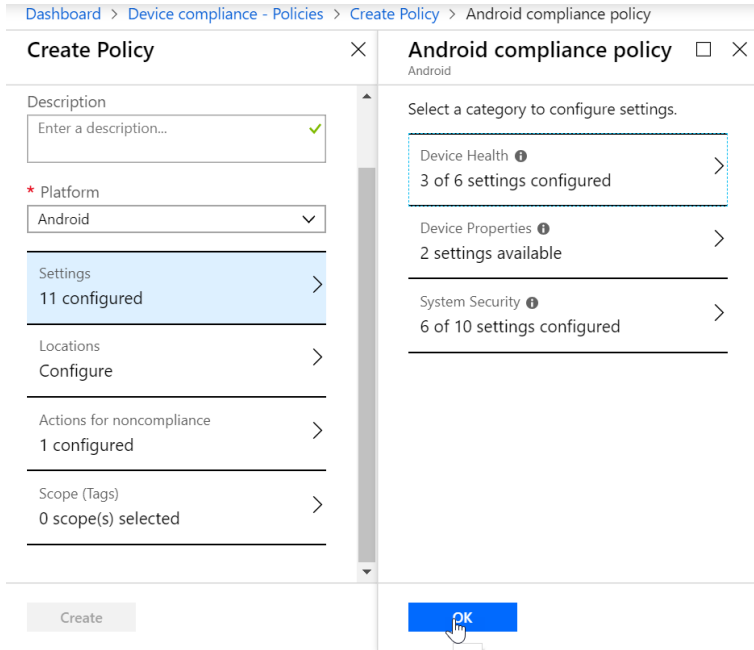
Restricted apps ⓘ Export

App name App Bundle ID Add

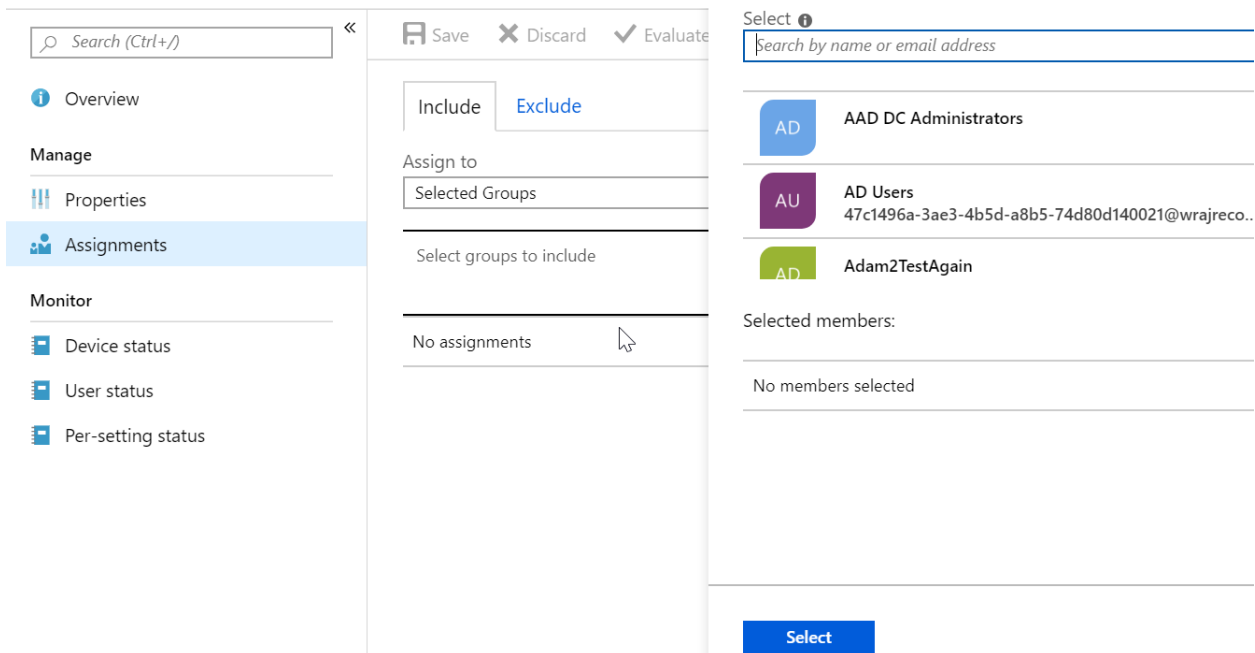
You have not restricted any apps.

OK OK

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



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



Windows

a. Click Create Policy

POLICY NAME	PLATF...	POLICY TYPE
Android Compliance Policy	Android	Android com
iOS	iOS	iOS compliar
iOS Compliance Policy	iOS	iOS compliar
Windows	Windows ...	Windows 10

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

Dashboard > Device compliance - Policies > Create Policy

Create Policy

* Name
 ✓

Description
 ✓

* Platform
 ^

- Select a platform
- Android
- Android enterprise
- iOS
- macOS
- Windows Phone 8.1
- Windows 8.1 and later
- Windows 10 and later

Create

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

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

Dashboard > Device compliance - Policies > Create Policy > Windows 10 compliance policy > System Security

Windows 10 compliance policy

Windows 10 and later

Select a category to configure settings.

- Device Health >
3 of 3 settings configured
- Device Properties >
5 settings available
- Configuration Manager Compliance >
1 setting available
- System Security >
16 settings available
- Windows Defender ATP >
1 setting available

OK

System Security

Windows 10 and later

Password

Require a password to unlock mobile devices. Require Not configured

Simple passwords Block Not configured

Password type Device default

Minimum password length 8

Maximum minutes of inactivity before password is required 15 Minutes

Password expiration (days) 90

Number of previous passwords to prevent reuse 3

Require password when device returns from idle state (Mobile and Holographic) Require Not configured

OK

Dashboard > Device compliance - Policies > Create Policy > Windows 10 compliance policy > System Security

Windows 10 compliance policy

Windows 10 and later

Select a category to configure settings.

- Device Health >
3 of 3 settings configured
- Device Properties >
5 settings available
- Configuration Manager Compliance >
1 setting available
- System Security >
16 settings available
- Windows Defender ATP >
1 setting available

OK

System Security

Windows 10 and later

Encryption of data storage on device. Require Not configured

Device Security

Firewall Require Not configured

Antivirus Require Not configured

Antispyware Require Not configured

Defender

Windows Defender Antimalware Require Not configured

Windows Defender Antimalware minimum version Not configured

Windows Defender Antimalware signature up-to-date Require Not configured

Real-time protection Require Not configured

OK

f. Click Ok and Create

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

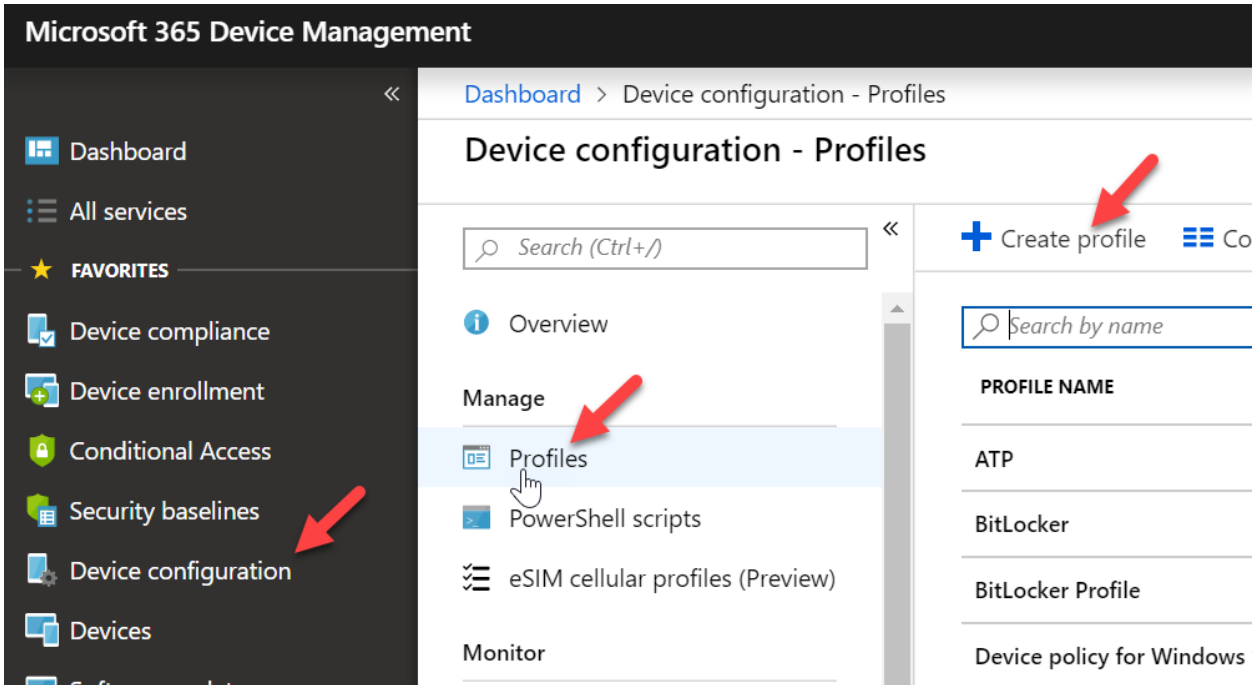
Create Device Profile

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

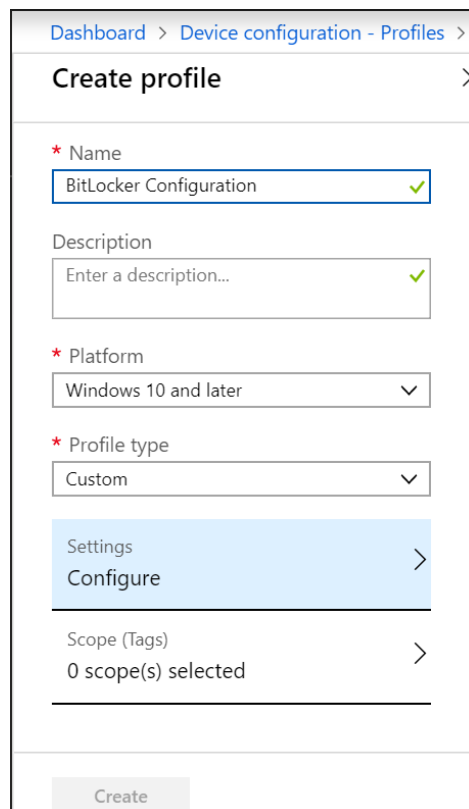
- You create a wifi profile that automatically configures the wifi on device that are enrolled with Intune
- Assume that you want to provision all iOS devices with the settings required to connect to a file share on the corporate network. You create a VPN profile that contains the settings to connect 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:
 - [Administrative templates](#)
 - [Custom](#)
 - [Delivery optimization](#)
 - [Device features](#)
 - [Device restrictions](#)
 - [Edition upgrade and mode switch](#)
 - [Education](#)
 - [Email](#)
 - [Endpoint protection](#)
 - [Identity protection](#)
 - [Kiosk](#)
 - [PKCS certificate](#)
 - [SCEP certificate](#)
 - [Trusted certificate](#)
 - [Update policies](#)
 - [VPN](#)
 - [Wi-Fi](#)
 - [Windows Defender ATP](#)
 - [Windows Information Protection](#)

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**



- b. Enter a **Name**, **Description** (if applicable), choose **Windows 10 or later** from the platform, and select **Custom** from Profile Type

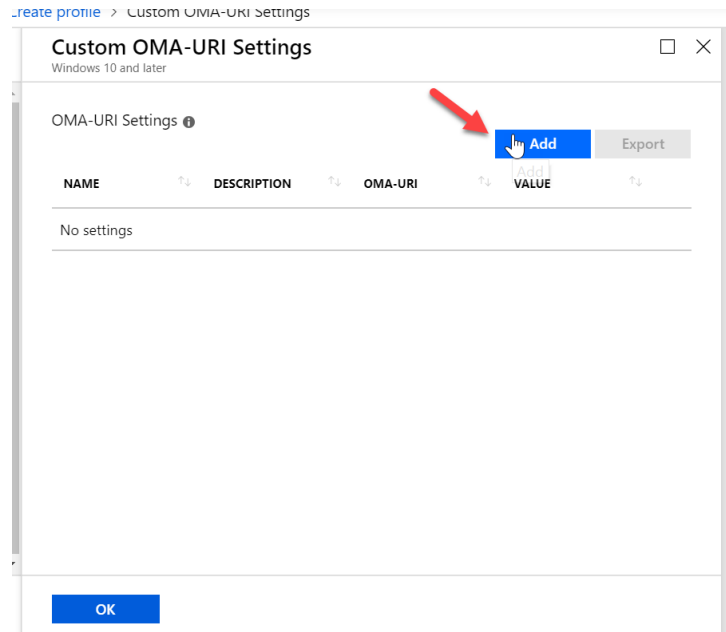


The screenshot shows the 'Create profile' form. The breadcrumb is 'Dashboard > Device configuration - Profiles >'. The form has the following fields:

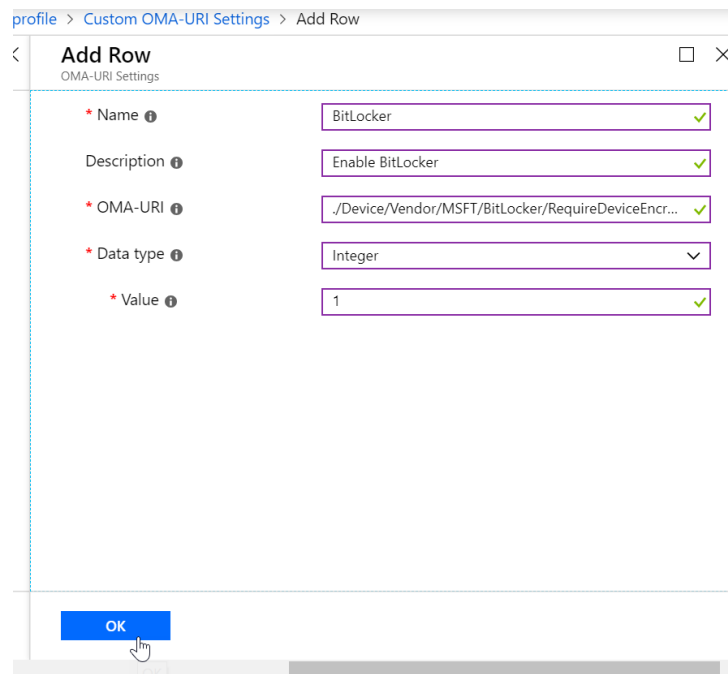
- Name:** BitLocker Configuration (with a green checkmark)
- Description:** Enter a description... (with a green checkmark)
- Platform:** Windows 10 and later (dropdown menu)
- Profile type:** Custom (dropdown menu)
- Settings:** Configure (button with a right arrow)
- Scope (Tags):** 0 scope(s) selected (button with a right arrow)

At the bottom of the form is a 'Create' button.

c. Click **Add**



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



e. Click Ok and Create

Dashboard > Device configuration - Profiles > Create profile > Custom OMA-URI Settings

Create profile × Custom OMA-URI Settings □ ×

Windows 10 and later

OMA-URI Settings ⓘ

NAME DESCRIPTION OMA-URI VALUE

BitLocker	Enable BitLocker	/Device/Vendor/M...	1	...
-----------	------------------	---------------------	---	-----

Buttons: Add, Export, OK

Dashboard > Device configuration - Profiles > C

Create profile □ ×

* Name: BitLocker Configuration ✓

Description: Enter a description... ✓

* Platform: Windows 10 and later

* Profile type: Custom

Settings: 1 configured

Scope (Tags): 0 scope(s) selected

Buttons: Create

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

Search (Ctrl+/)

Save Discard Evaluate

Include Exclude

Assign to: Selected Groups

Select groups to include

No assignments

Select ⓘ

Search by name or email address

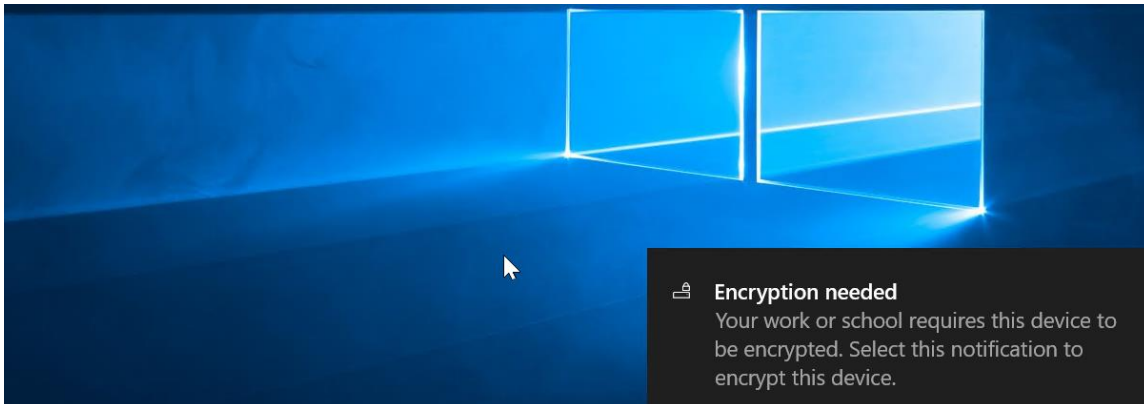
- AD AAD DC Administrators
- AU AD Users
47c1496a-3ae3-4b5d-a8b5-74d80d140021@wrajreco..
- AD Adam2TestAgain

Selected members:

No members selected

Select

- 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](#)

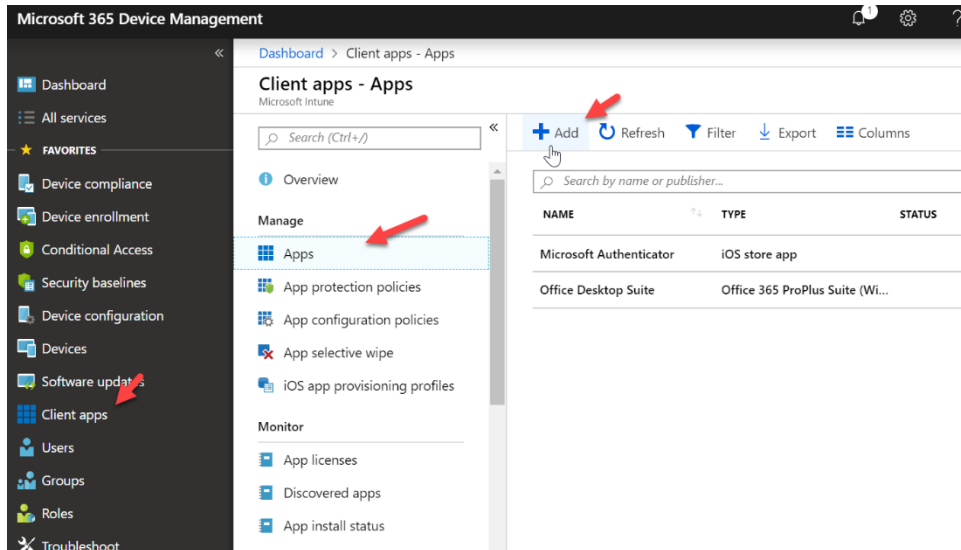
Yes

No

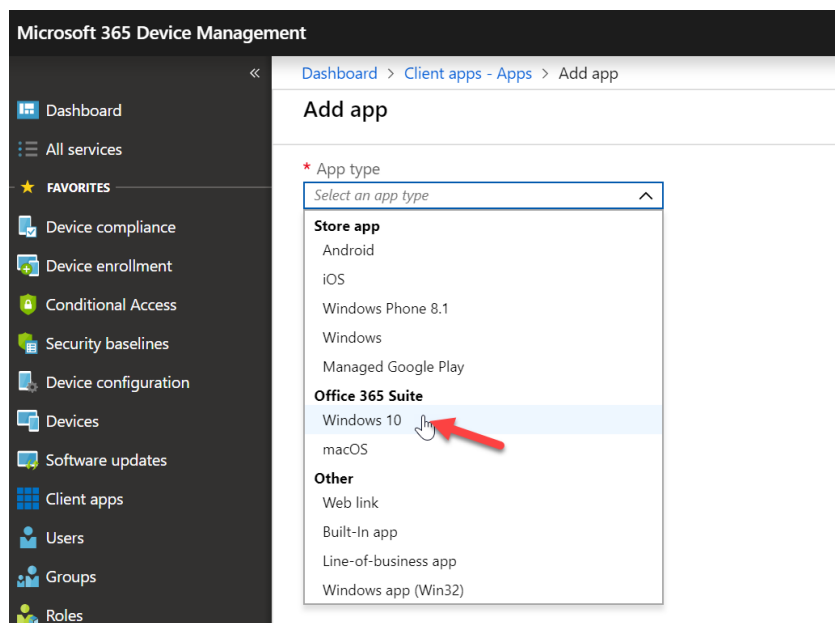
Add an Application

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:

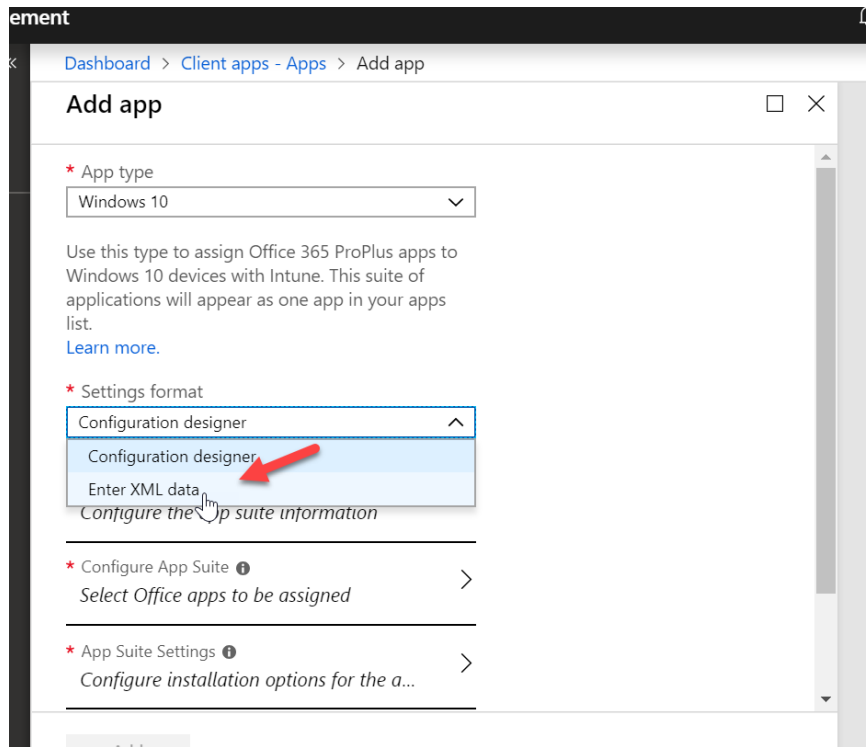
- a. In the Device Management Admin center go to **Client Apps>Apps>Add**



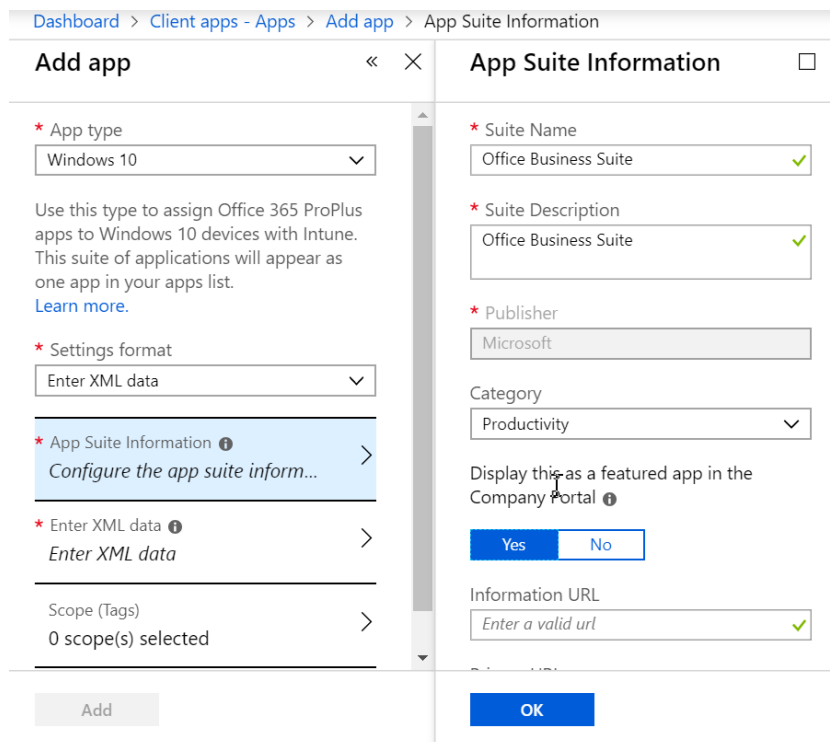
- b. Select Windows 10 under Office 365 Suite from the dropdown list:



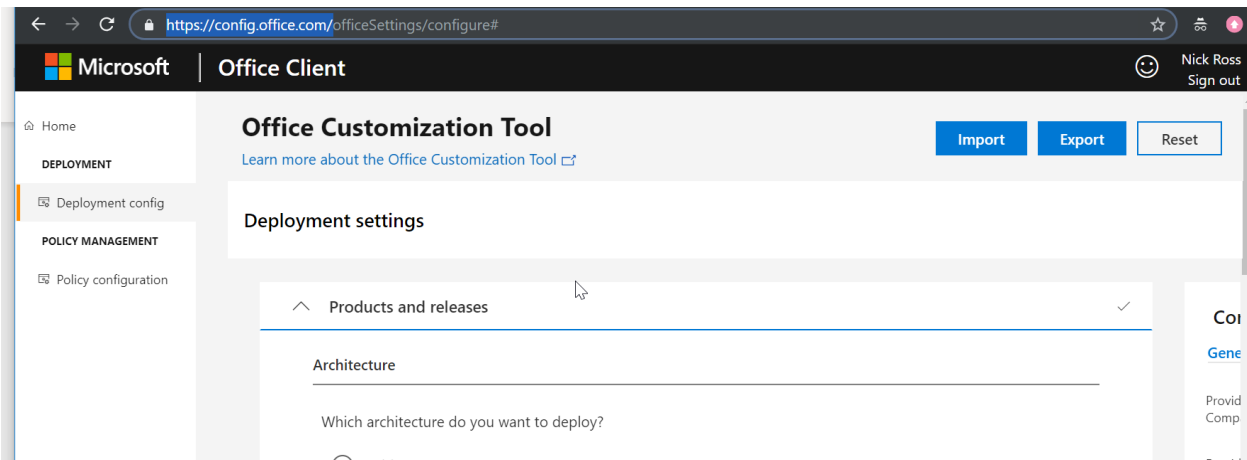
- c. Under **Settings Format** select **Enter XML data** *Note* We are making this selection because we have M365 Business Plan. If we have a plan that comes with Proplus (E3,E5, M365 E3, M365 E5) we would select Configuration Designer:



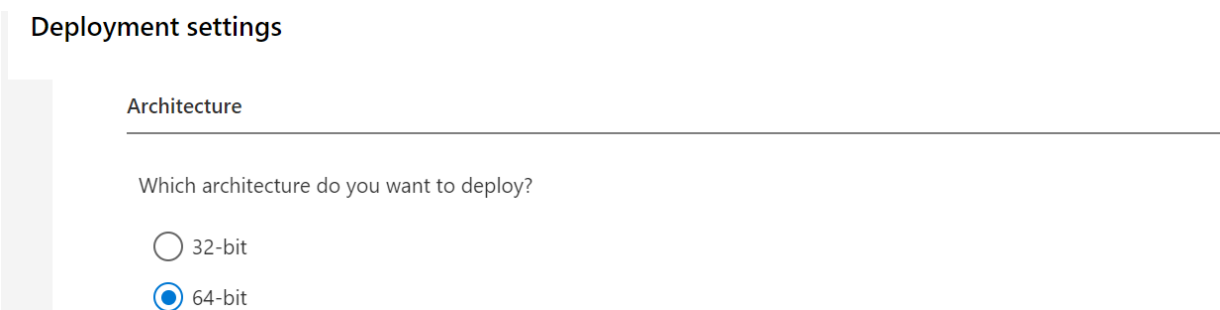
- d. Under **App Suite Information**, configure the following and click ok:



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



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



Office Customization Tool

[Learn more about the Office Customization Tool](#) Import Export

Deployment settings

Which products and apps do you want to deploy?

Office Suites

- Office 365 Business
- None
- Office 365 ProPlus
- Office 365 Business**
- Office Professional Plus 2019 - Volume License
- Office Standard 2019 - Volume License

Additional Products

- Select Additional product

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

Deployment settings

Turn apps on or off to include or exclude them from being deployed

Access <input checked="" type="checkbox"/> On	Excel <input checked="" type="checkbox"/> On
OneDrive (Groove) <input type="checkbox"/> Off	Skype for Business <input checked="" type="checkbox"/> On
OneDrive Desktop <input checked="" type="checkbox"/> On	OneNote 2016 <input type="checkbox"/> Off
Outlook <input checked="" type="checkbox"/> On	PowerPoint <input checked="" type="checkbox"/> On
Publisher <input checked="" type="checkbox"/> On	Teams <input checked="" type="checkbox"/> On
Word <input checked="" type="checkbox"/> On	

Update channel

Select the update channel, which controls the timing of feature updates [Learn more](#)

Monthly Channel

Update channel

Select the update channel, which controls the timing of feature updates [Learn more](#)

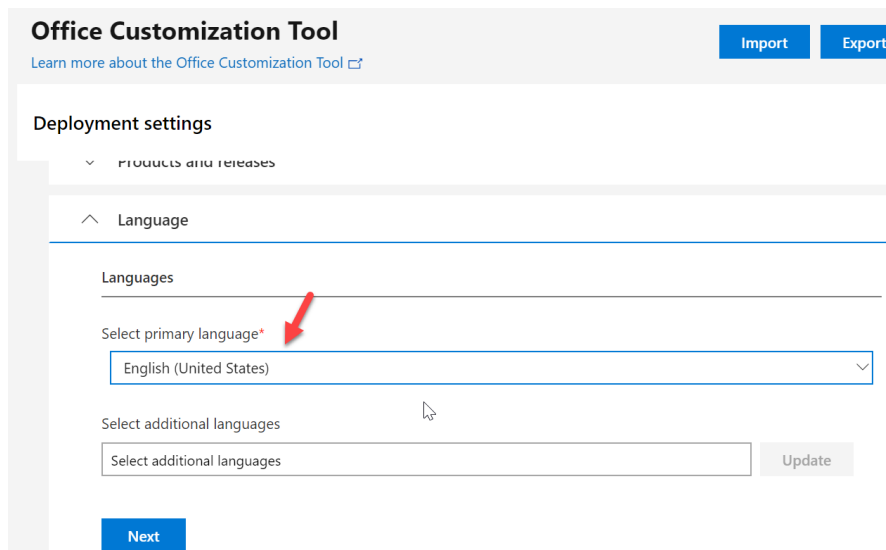
Monthly Channel

Which version do you want to deploy? [Learn more](#)

Latest

Next

- h. Under **Language** select **English** or your primary language



Office Customization Tool Import Export


[Learn more about the Office Customization Tool](#)

Deployment settings

Products and releases

Language

Languages

Select primary language* 

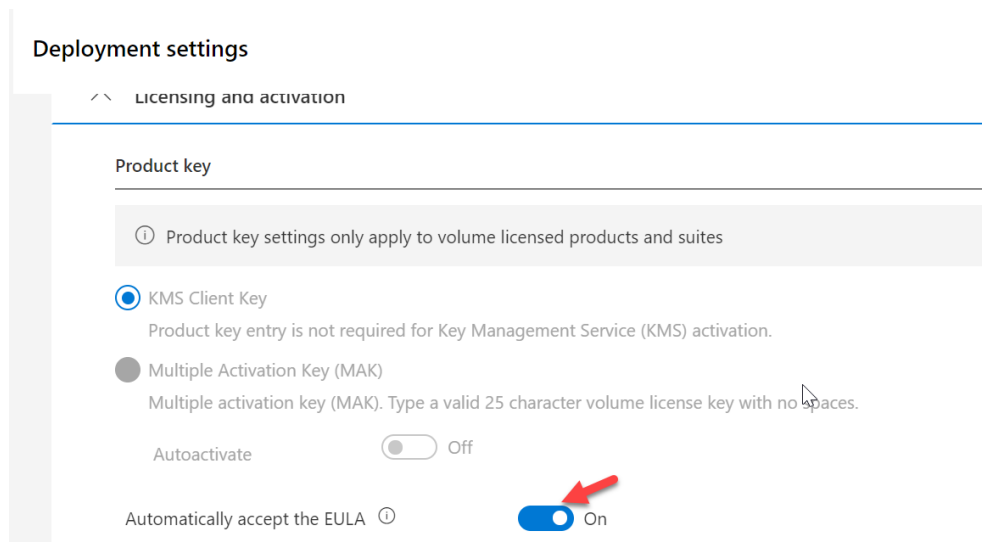
English (United States)

Select additional languages

Select additional languages Update

Next

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



Deployment settings

Licensing and activation


Product key

Product key settings only apply to volume licensed products and suites

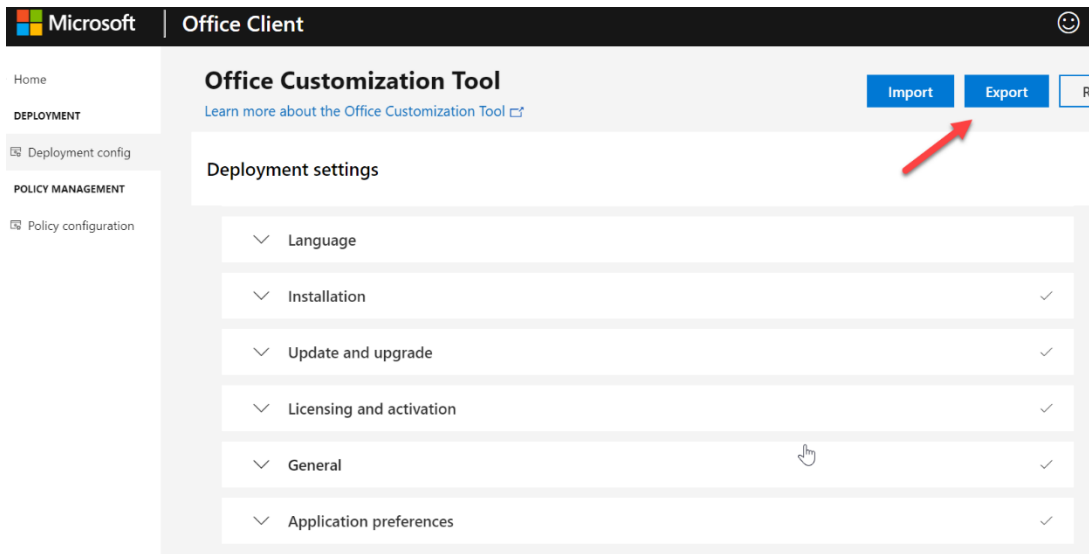
KMS Client Key
Product key entry is not required for Key Management Service (KMS) activation.

Multiple Activation Key (MAK)
Multiple activation key (MAK). Type a valid 25 character volume license key with no spaces.

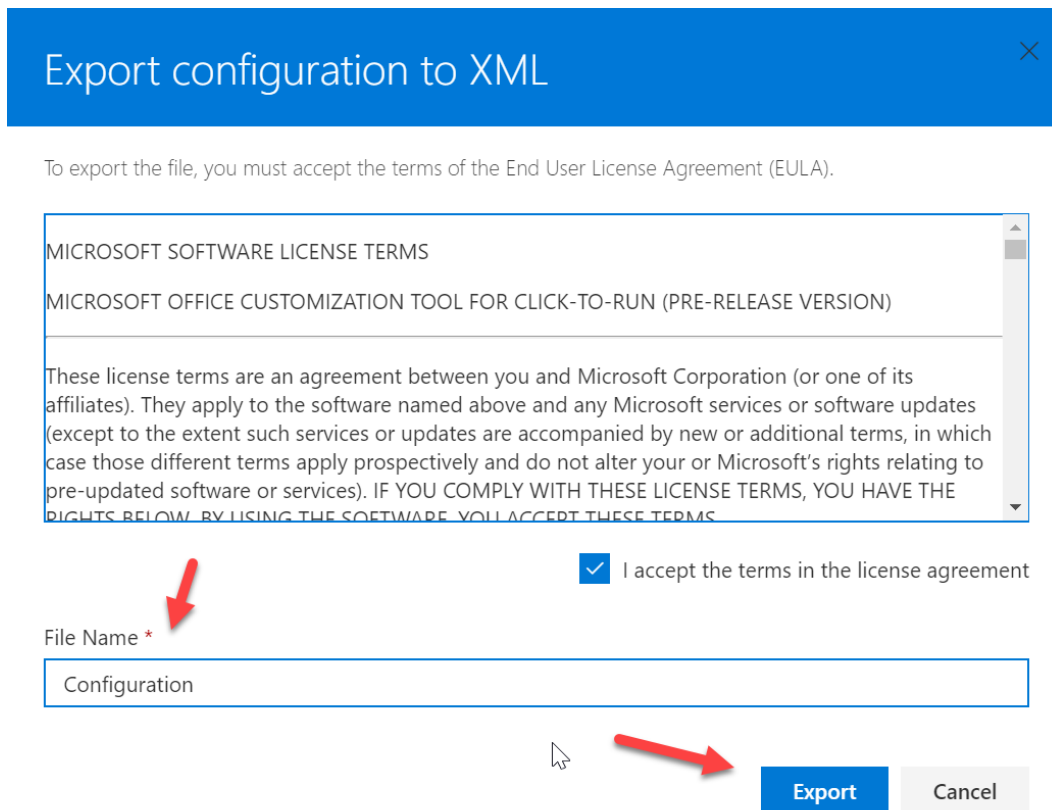
Autoactivate Off

Automatically accept the EULA On 

j. Leave all other settings defaulted and click **Export**



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



l. Open the XML file and copy the text:

How do you want to open this file?

Keep using this app

Office XML Handler

Other options

- Microsoft Edge New
- Microsoft Visual Studio 2017 New
- Notepad
- WordPad

Always use this app to open .xml files

OK

```

Configuration (3) - Notepad
File Edit Format View Help
<Configuration ID="48c3708d-dd05-4f72-a0a7-64fa31dfa55a" DeploymentConfigurationID="00000000-0000-0000-0000-000000000000">
  <Add OfficeClientEdition="64" Channel="Monthly" ForceUpgrade="TRUE">
    <Product ID="0365BusinessRetail">
      <Language ID="en-us" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="OneNote" />
    </Product>
  </Add>
  <Property Name="SharedComputerLicensing" Value="0" />
  <Property Name="PinIconsToTaskbar" Value="TRUE" />
  <Property Name="SCLCacheOverride" Value="0" />
  <Updates Enabled="TRUE" />
  <RemoveMSI />
  <Display Level="Full" AcceptEULA="TRUE" />
</Configuration>

```

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

Dashboard > Client apps - Apps > Add app > Configuration File

Add app

* App type
Windows 10

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
Enter XML data

* App Suite Information ⓘ
App suite information is confi... >

* Enter XML data ⓘ
Enter XML data >

Scope (Tags)
0 scope(s) selected >

Add

Configuration File

Use the Office Customization tool to create the configuration files that are used to deploy Off large organizations.
[Learn more.](#)

```

<?xml version="1.0"?>
- <Configuration DeploymentConfigurationID="00000000-0000-0000-000000000000"
ID="17a57fce-d355-4dba-ac9d-fd356f4c995f">
  <Add ForceUpgrade="TRUE" Channel="Monthly" OfficeClientEdition="64">

```

OK

n. Click **Add**

ent

Dashboard > Client apps - Apps > Add app

Add app

Windows 10

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
Enter XML data

* App Suite Information ⓘ
App suite information is configured

* Enter XML data ⓘ
XML Data Entered

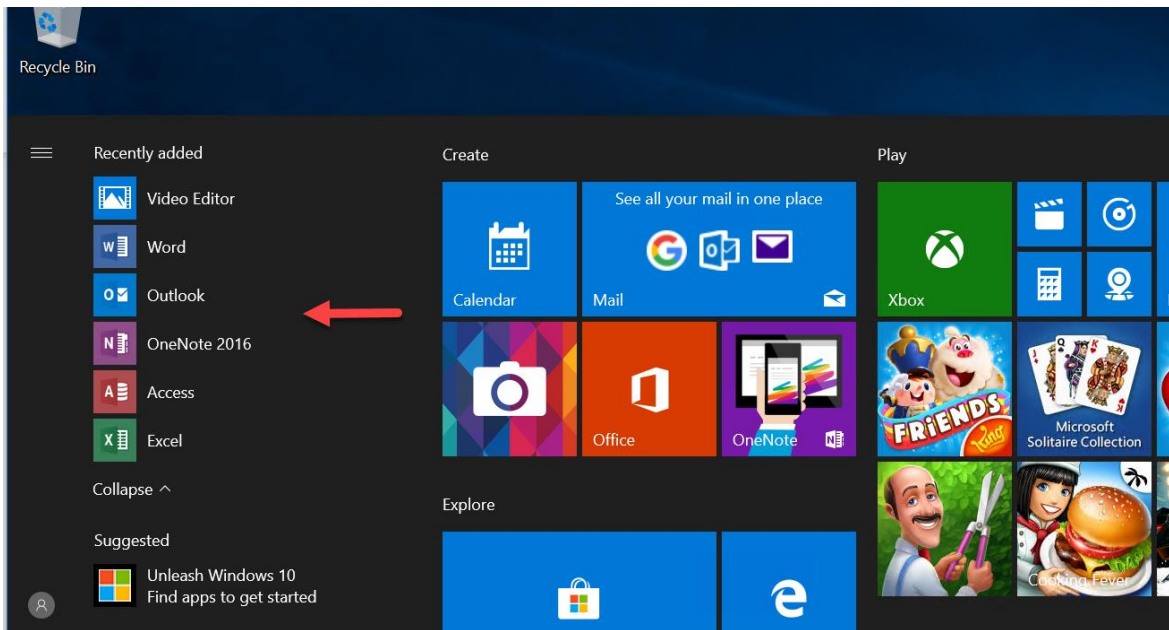
Scope (Tags)
0 scope(s) selected

Add

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

The screenshot shows the 'Office Desktop Suite - Assignments' interface on the left and the 'Add group' dialog on the right. In the 'Assignments' view, the 'Assignments' menu item is highlighted with a red arrow, and the 'Add group' button is also highlighted with a red arrow. The 'Add group' dialog shows an information message, a search bar, and a list of groups. The 'Assignment type' dropdown menu is open, with 'Required' selected and highlighted by a red arrow. The dialog also shows 'No groups selected' and 'Excluded Groups' sections.

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

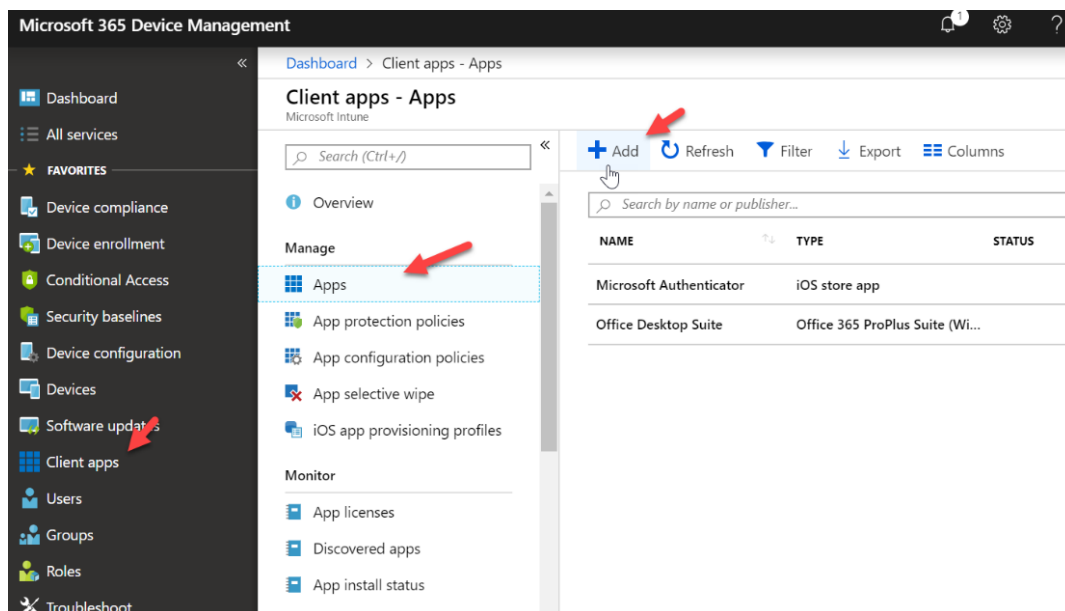


Adding the Microsoft Authenticator App

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:

Dashboard > Client apps - Apps > Add app > Search the App Store

Add app << X

* App type
iOS

* Search the App Store
Select app

* App information
Configure

Scope (Tags)
0 scope(s) selected

Search the App Store

Microsoft Authenticator United States (default)

Found 3 apps

	NAME	PUBLISHER
	Microsoft Authenticator	Microsoft Corporation
	SAASPASS Authenticator 2FA MFA	SAASPASS
	TOTP Authenticator - Fast 2FA	AppyFactor

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

Dashboard > Client apps - Apps > Add app > App information

Add app << X

* App type
iOS

* Search the App Store
Microsoft Authenticator

* App information
Configure

Scope (Tags)
0 scope(s) selected

App information □ X

* Appstore URL
https://itunes.apple.com/us/app/microsof...

* Minimum operating system
iOS 8.0

* Applicable device type
2 selected

Category
0 selected

Display this as a featured app in the Company Portal ⓘ

Yes No

Information URL
Enter a valid url ✓

Privacy URL
Enter a valid url ✓

OK

Add

d. Click Add

Dashboard > Client apps - Apps > Add app

Add app

* App type

* Search the App Store
 Microsoft Authenticator >

* App information
 Configure >

Scope (Tags)
 0 scope(s) selected >

Add

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

Dashboard > Client apps - Apps > Microsoft Authenticator - Assignments > Add group

Microsoft Authenticator - Assignments

Client Apps

Search (Ctrl+)

- Overview
- Manage
 - Properties
 - Assignments**
- Monitor
 - Device install status
 - User install status

Save Discard

Add group

GROUP	ASSIG...	MODE	VPN
No assignments, select 'Add group' to add a ...			

Assignment type

Select assignment type ^

- Available for enrolled devices
- Available with or without enrollment
- Required**
- Uninstall

No groups selected >

Excluded Groups >

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Select groups where you want to assign this app.

Android

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

The screenshot shows the Microsoft 365 Device Management Admin Center interface. The left-hand navigation pane is open, showing various service categories. The 'Client apps' category is expanded, and the 'Apps' sub-item is selected and highlighted with a red arrow. In the main content area, the 'Client apps - Apps' page is displayed. At the top right of this page, there is a toolbar with several icons: a plus sign for 'Add', a circular arrow for 'Refresh', a funnel for 'Filter', a download arrow for 'Export', and a list icon for 'Columns'. The 'Add' button is highlighted with a red arrow. Below the toolbar is a search bar labeled 'Search by name or publisher...'. Underneath the search bar is a table with columns for 'NAME', 'TYPE', and 'STATUS'. The table contains two entries: 'Microsoft Authenticator' (iOS store app) and 'Office Desktop Suite' (Office 365 ProPlus Suite (Wi...)).

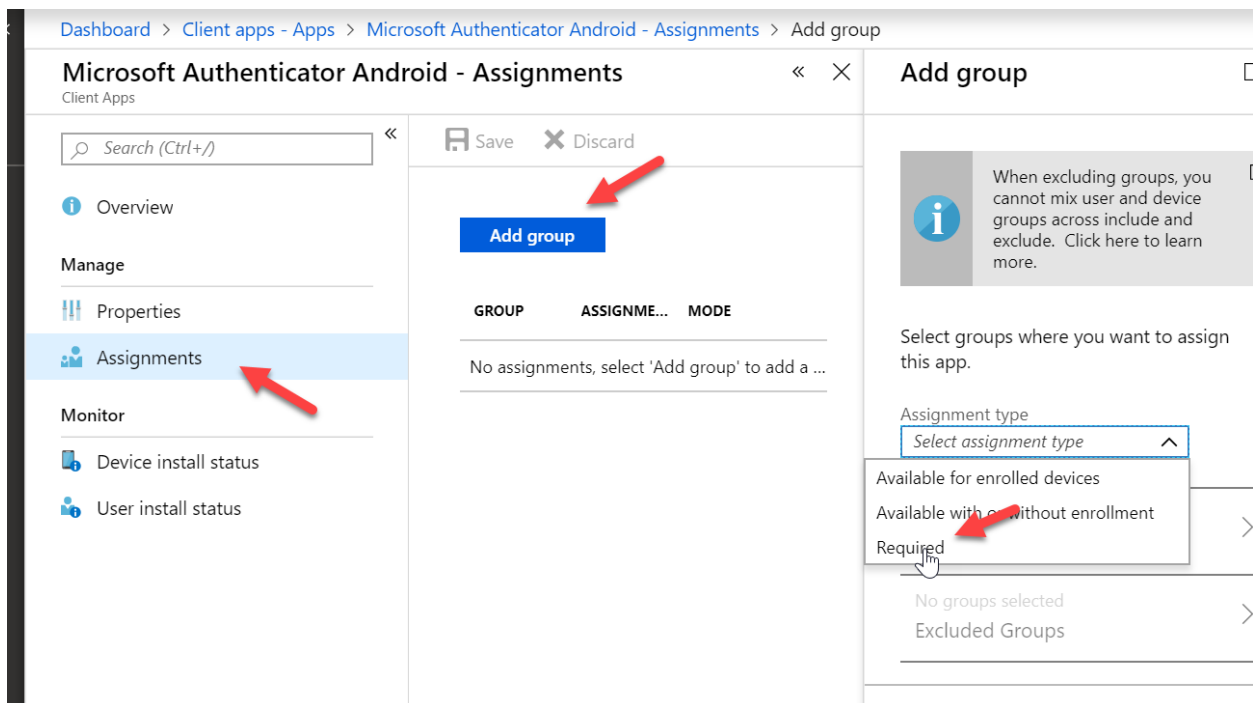
- b. For App Type, select **Android** and fill out the fields as follows, including the following for AppStore URL:

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

The screenshot shows the 'Add app' dialog box in the Microsoft 365 Device Management Admin Center. The dialog is split into two panes. The left pane is titled 'Add app' and contains three main sections: 'App type' (set to 'Android'), 'App information' (with a 'Configure' link), and 'Scope (Tags)' (0 scope(s) selected). The right pane is titled 'App information' and contains several fields: 'Name' (Microsoft Authenticator Android), 'Description' (Microsoft Authenticator Android), 'Publisher' (Microsoft), 'Appstore URL' (s?id=com.azure.authenticator&hl=en_US), and 'Minimum operating system' (Android 4.0 (Ice Cream Sandwich)). There is also a 'Category' field (0 selected) and a checkbox for 'Display this as a featured app in the Company Portal'. At the bottom of the dialog, there are 'Add' and 'OK' buttons.

c. Click **Add**

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



Dashboard > Client apps - Apps > Microsoft Authenticator Android - Assignments > Add group

Microsoft Authenticator Android - Assignments

Client Apps

Search (Ctrl+/)

Save Discard

Add group

GROUP	ASSIGNME...	MODE
No assignments, select 'Add group' to add a ...		

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Select groups where you want to assign this app.

Assignment type
Select assignment type

Available for enrolled devices

Available with or without enrollment

Required

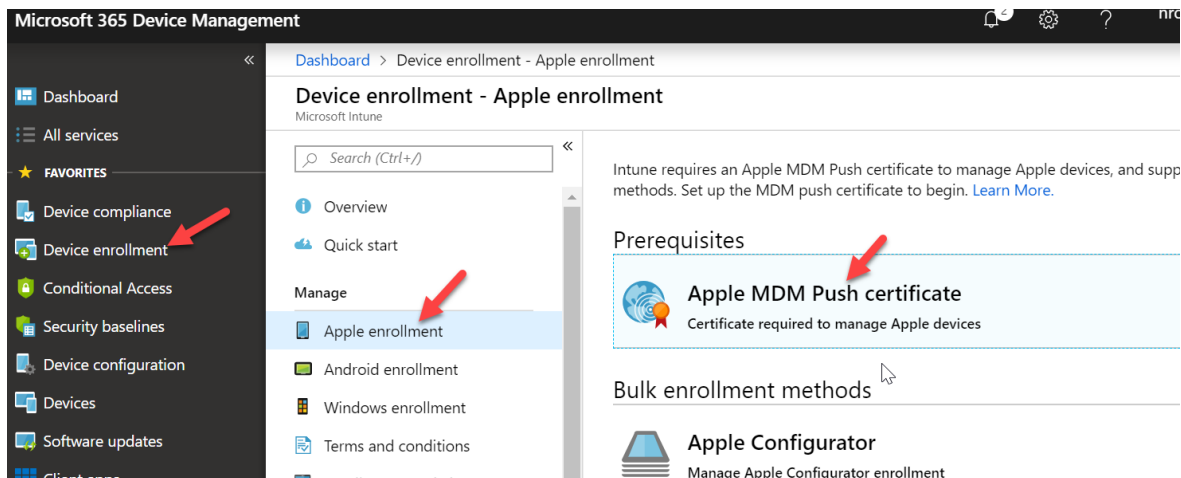
No groups selected

Excluded Groups

Set up Apple MDM Push Certificate

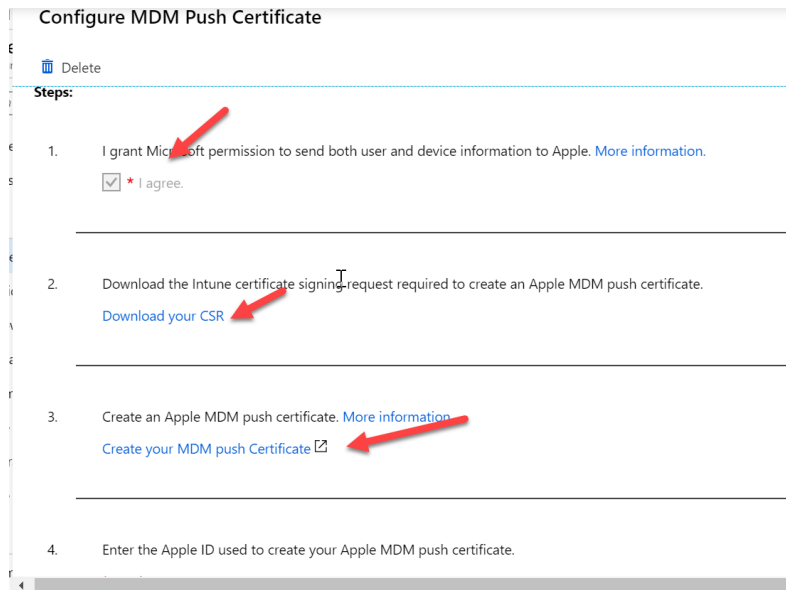
The Apple MDM Push Certificate allows us to start enrolling iOS devices. You can think of this cert as a shell account in which you can put all over your customers under. The certificate is associated with the Apple ID used to create it. As a best practice, use a company Apple ID for management tasks 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**

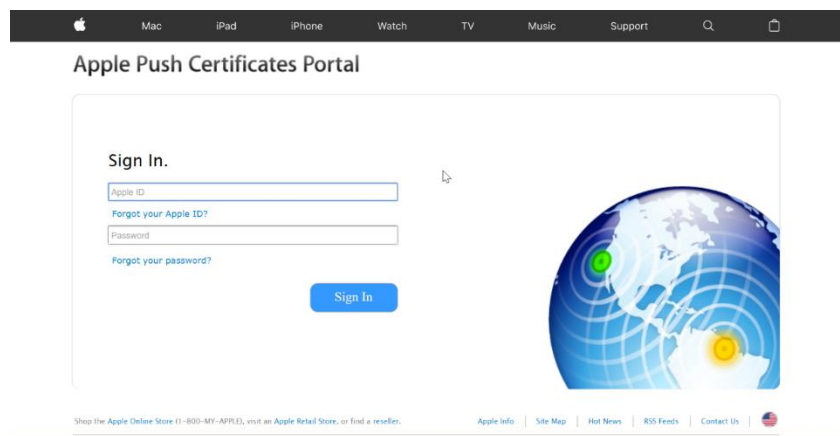


- b. Agree to the terms and conditions, Download your CSR (save to another location or keep in downloads. The file is used to request a trust relationship certificate from the Apple Push Certificates Portal.), and click **Create your MDM Push Certificate** to open the Apple center

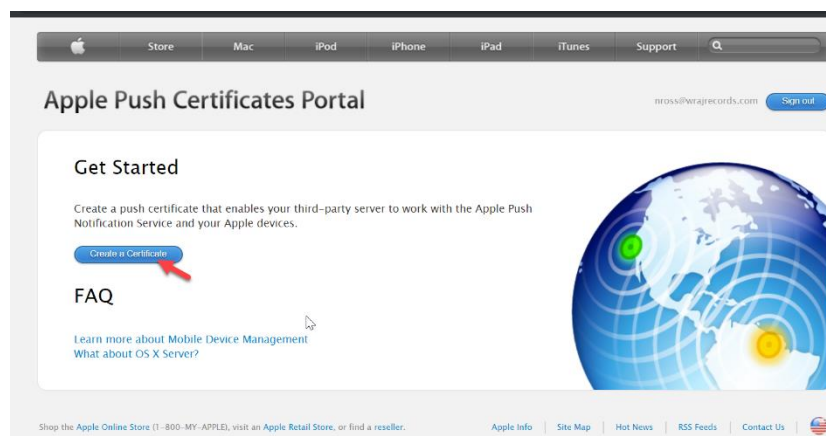
File Name	Date Modified	File Type	Size
HIPAABusinessAssociateAgr(WW)(ENG)(Februar...	9/30/2018 1:54 PM	Microsoft Word Doc...	51 KB
IMG_1436	10/28/2018 8:18 PM	JPG File	53 KB
IntuneCSR.csr	11/2/2018 12:43 PM	CSR File	10 KB
invoice-48363	10/24/2018 4:32 PM	PDF File	59 KB
invoice-51422	10/4/2018 1:19 PM	PDF File	42 KB
invoice-51913	10/4/2018 1:18 PM	PDF File	62 KB
invoice-55188	10/22/2018 12:23 PM	PDF File	64 KB



- 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)



- d. After you sign in click Create Certificate



- a. Upload your CSR file and then Download the MDM Push 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

IntuneCSR.csr




Apple Push Certificates Portal

nross@wrajrecords.com

Confirmation ✔

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


Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Nov 2, 2019




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

Home > Microsoft Intune > Device enrollment - Apple enrollment > Configure MDM Push Certificate


Configure MDM Push Certificate

 Delete

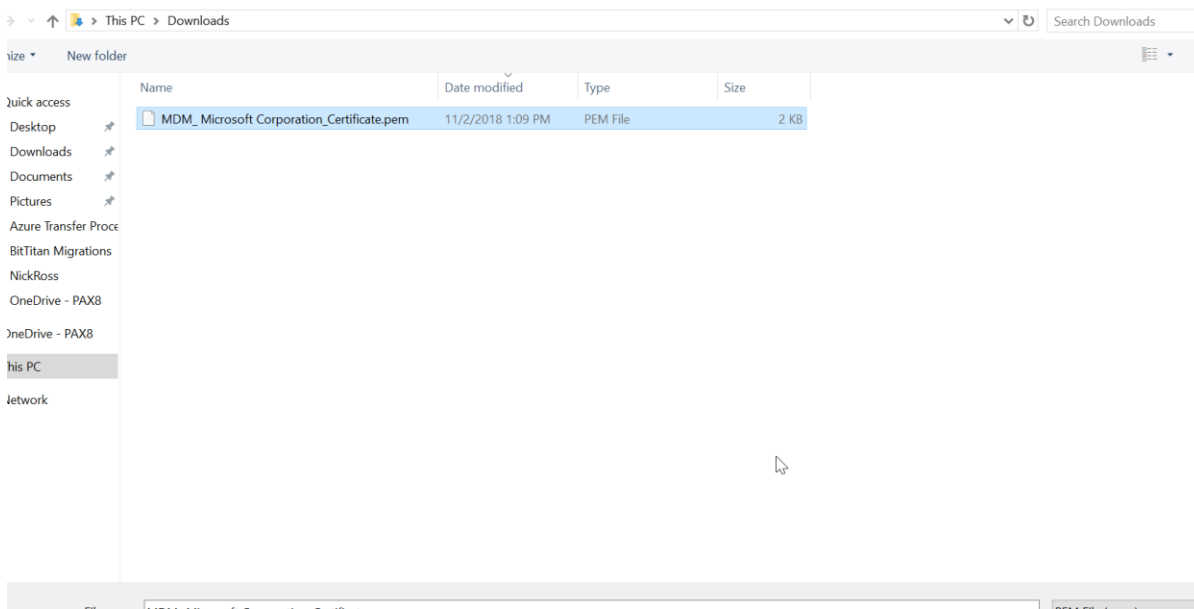
4. Enter the Apple ID used to create your Apple MDM push certificate.

* Apple ID
 

5. Browse to your Apple MDM push certificate to upload


* Apple MDM push certificate
 


Upload



f. You will see the status as active

Configure MDM Push Certificate

 Delete

Status:  Active

Last Updated: 12/3/2018

Apple ID: nross@wrajrecords.com

Days Until Expiration: 217

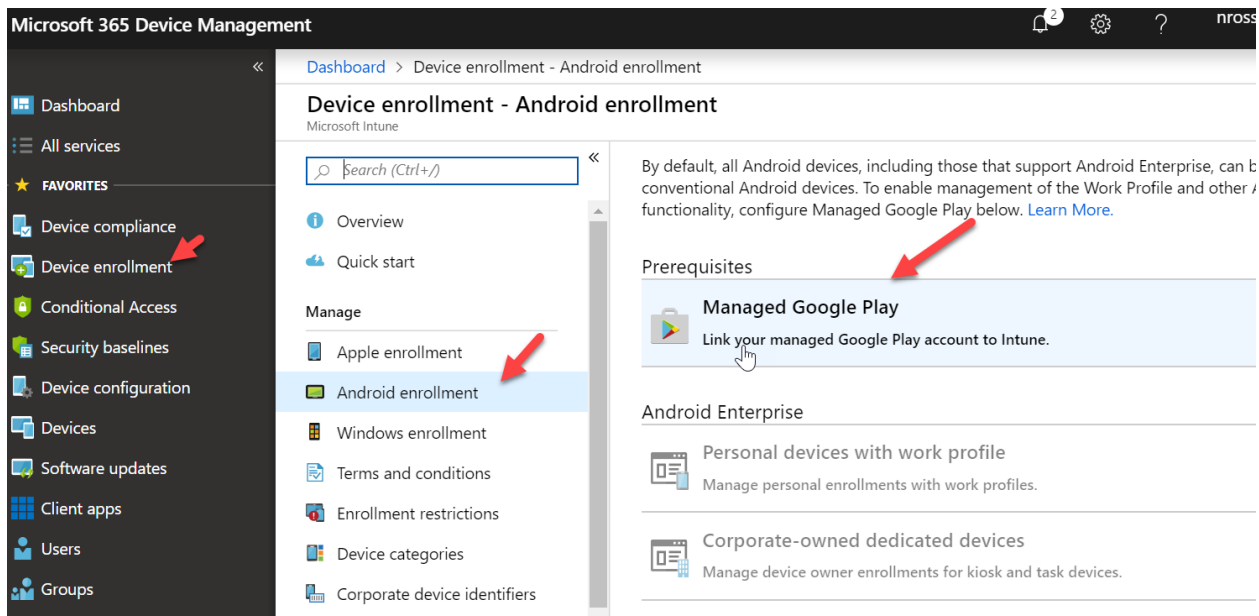
Expiration: 11/2/2019

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**





The screenshot shows the Microsoft 365 Device Management Admin Portal. The left-hand navigation pane has 'Device enrollment' highlighted with a red arrow. The main content area shows 'Device enrollment - Android enrollment' with a search bar and a list of options. 'Android enrollment' is selected in the 'Manage' section, also highlighted with a red arrow. Under 'Prerequisites', the 'Managed Google Play' section is highlighted with a red arrow, containing the instruction 'Link your managed Google Play account to Intune.' Below this, the 'Android Enterprise' section is visible, with sub-sections for 'Personal devices with work profile' and 'Corporate-owned dedicated devices'.


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

Managed Google Play

Android enrollment

 Disconnect

<p>Status:  Not Setup</p> <p>Organization: Not Available</p>	<p>Google Account: Not Available</p> <p>Registration Date: Not Available</p>
---	--



You must connect Intune to your company's managed Google Play account to manage Android enterprise enrollment. [Learn More.](#)




1. I grant Microsoft permission to send both user and device information to Google. [Learn More.](#)

I agree.

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

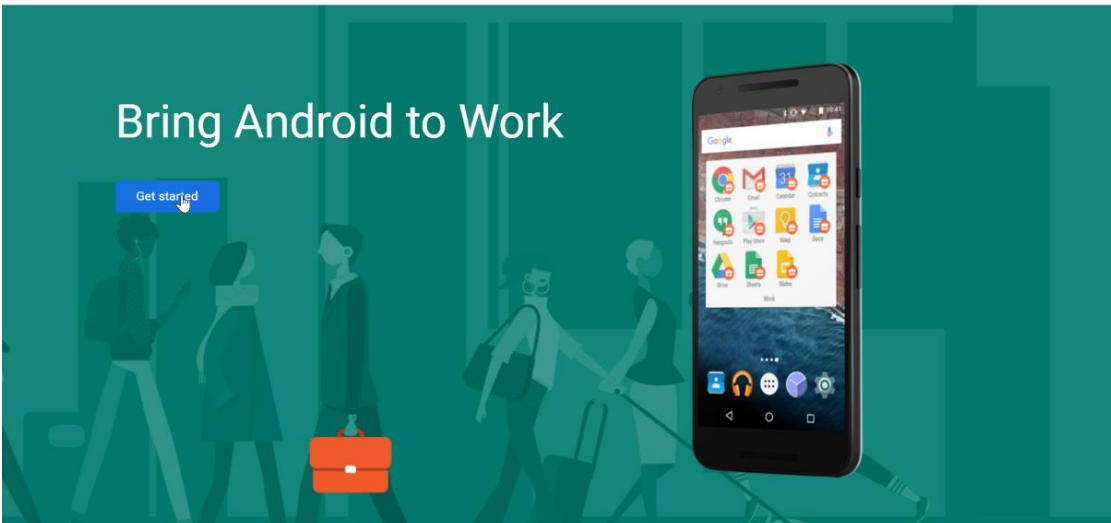
[Launch Google to connect now.](#)

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

Bring Android to Work

[Get started](#)



- d. Enter your Business Name and click Next

Business name

We need some details about your business

Business name

Enterprise mobility management (EMM) provider

Microsoft Intune

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

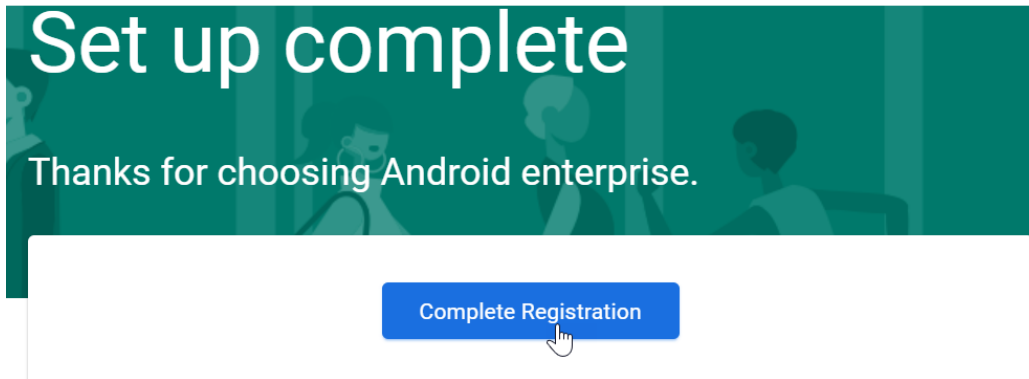
- e. If you are in the EU, you can enter the contact of an EU representative. If not, simply agree to the terms and click confirm:

EU Representative

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.


Managed Google Play

Android enrollment

 Disconnect

Status:  Setup ←

Organization: TMinus365

 Managed Google Play successfully conf
Managed Google Play successfully configur

Google Account: thetradingnest@gmail.com

Registration Date: 3/30/2019, 2:24:37 PM

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

1. I grant Microsoft permission to send both user and device information to Google. [Learn More](#).

I agree.

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

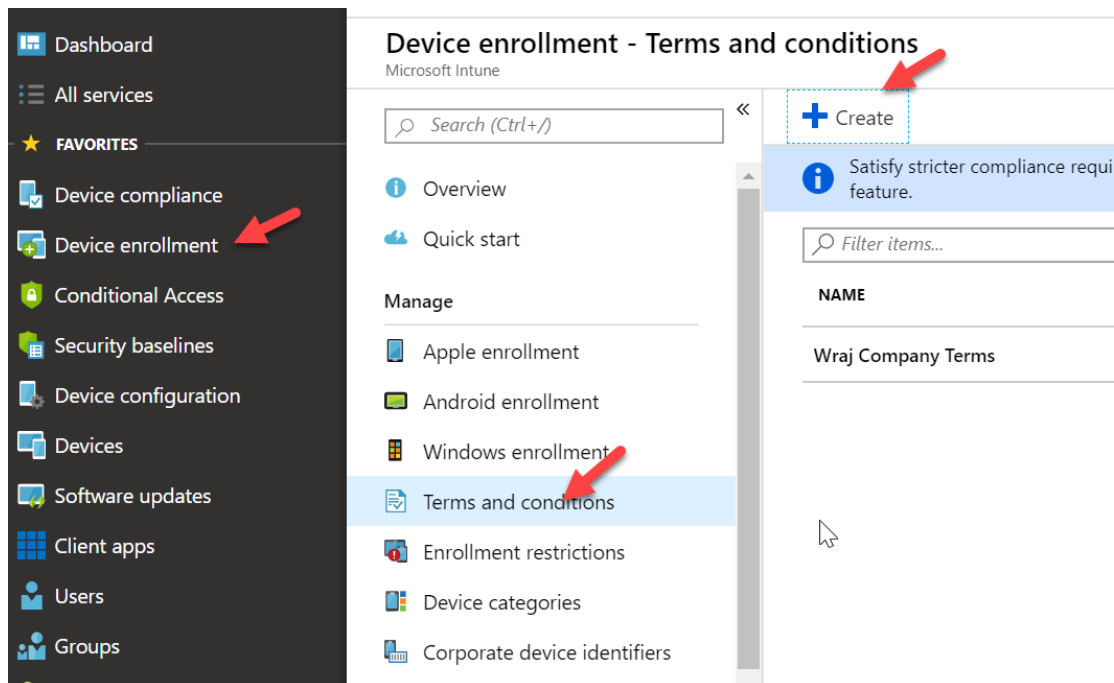
Launch Google to connect now.

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.

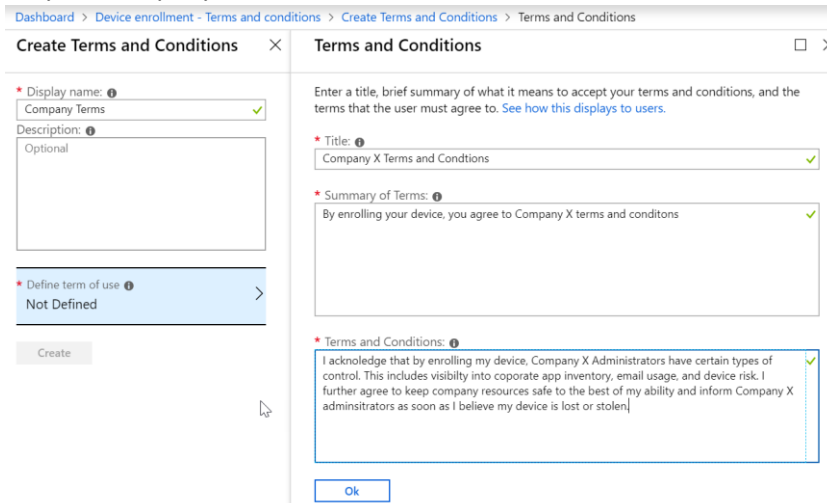
- In the Device Management Admin Portal, go to **Device Enrollment>Terms and Conditions>Create**



The screenshot displays the Microsoft Intune admin portal interface for 'Device enrollment - Terms and conditions'. The left-hand navigation pane is visible, with 'Device enrollment' highlighted. The main content area includes a search bar, a 'Create' button, and a list of terms and conditions. A table with the following content is shown:

NAME
Wraj Company Terms

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



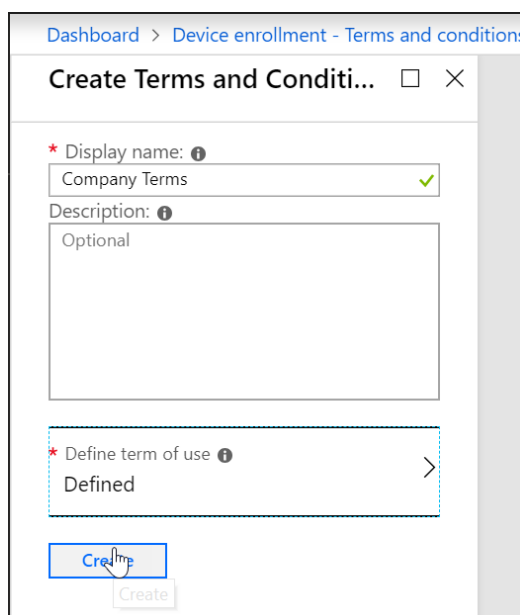
Ex. Summary of Terms

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

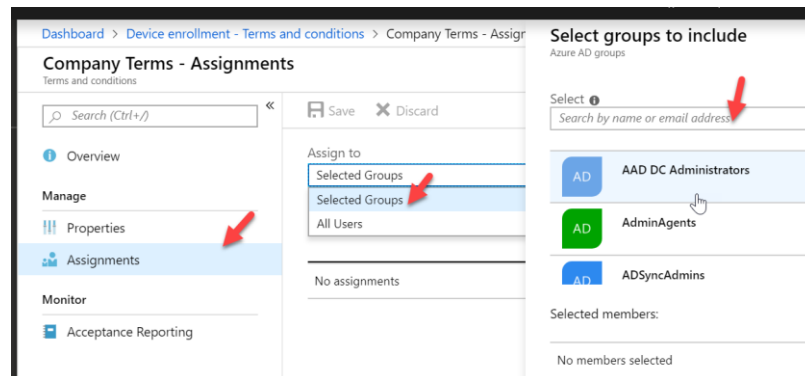
Ex. Terms and Conditions

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**



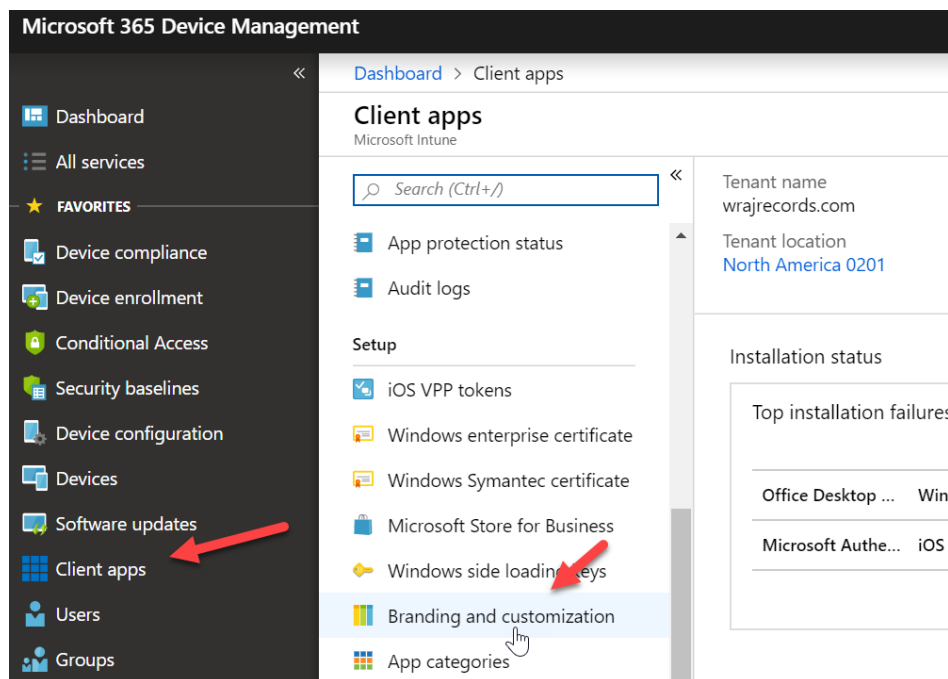
- d. Click on the Policy after creation and click **Assignments** to assign the Terms to All Users or a select group:



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 OOB 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
Refresh

Enter your company's support information to provide your employee with a contact for Intune-related information, along with the custom settings you configure, will be visible throughout the Intune user experience. [Learn more.](#)

Company information

* Company name:

Privacy statement URL:

Support information

Contact name:

Phone number:

Email address:

Website name:

Website URL:

Additional information:

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

Company identity branding

^ 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

Display

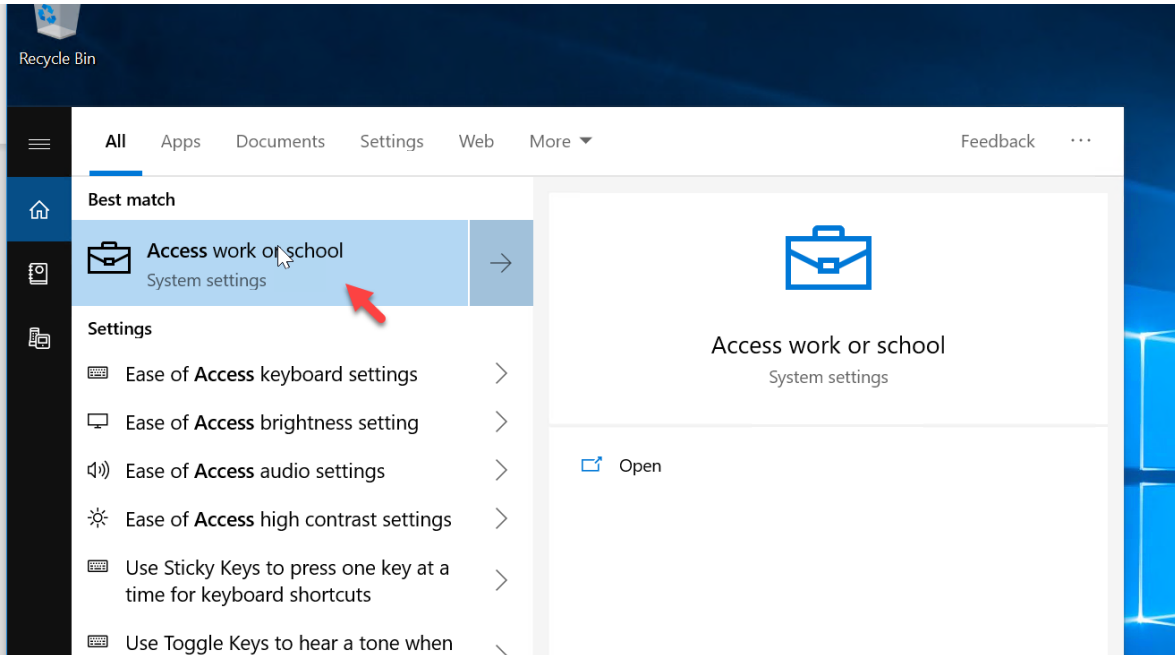
Text color: White ⓘ

^ Logo to use on white or light background

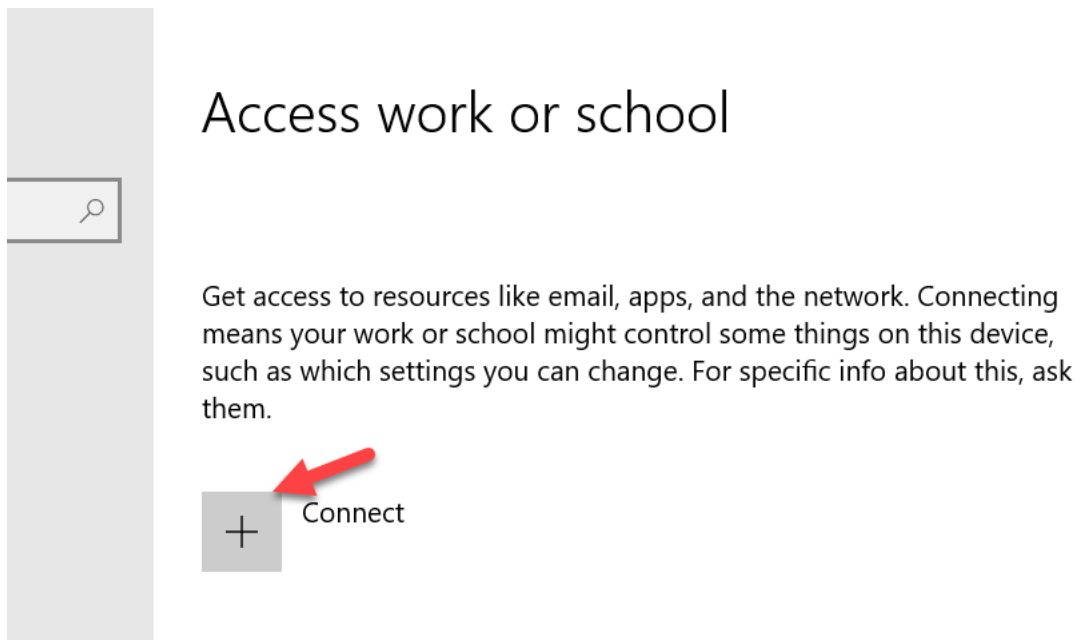
Upload your logo

Enroll Devices: Windows

- 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**

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

d. Sign-In with the Users Azure AD credentials

Let's get you signed in

Work or school account

someone@example.com

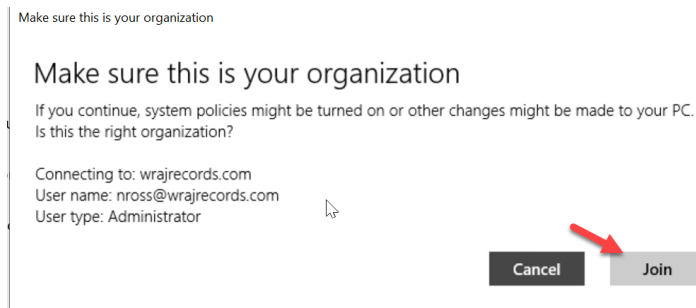
Which account should I use?

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**



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 recordsl.

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.

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)

Microsoft 365 Device Management

Dashboard > Device compliance - Policies

Device compliance - Policies

Windows - Device status

Device compliance policy

Search (Ctrl+/)

Columns Export

Data in this view is live.

Filter items...

DEVICE	USER PRINCIPAL NAME	COMPLIANCE STATUS
DESKTOP-MEO0NQ6	None	Not evaluated
DESKTOP-TRBCT6F	jsonnier@wrajrecords.com	Not Compliant
WindowsAuto	None	Not evaluated

Overview

Manage

- Properties
- Assignments

Monitor

- Device status
- User status
- 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

Data in this view is live.

Filter items...

DEVICE	USER PRINCIPAL NAME	DEPLOYMENT STATUS	LAST STATUS UPDATE
DESKTOP-MEO0NQ6	None	Pending	
DESKTOP-TRBCT6F	jsonnier@wrajrecords.com	Failed	1/10/19, 10:57 AM
WindowsAuto	nross@wrajrecords.com	Error	3/30/19, 5:20 PM

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

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

WindowsAuto

Search (Ctrl+/)

Retire Wipe Delete Remote lock Sync Reset passcode Restart

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Managed Apps

Device name: WindowsAuto

Enrolled by User: Nick Ross

Management name: nross_Windows_3/30/2019_9:01 PM

Compliance: Not Compliant

Ownership: Corporate

Operating system: Windows

Serial number: 0000-0013-4890-0606-7785-1571-70

Device model: Virtual Machine

Phone number: ---

Last check-in time: 3/30/2019, 5:20:18 PM

See more

Device actions status

ACTION	STATUS	DATE/TIME
No results		

b. Click on **Windows** as it is our policy

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

WindowsAuto - Device compliance

Search (Ctrl+/)

Export

Filter by name

POLICY	USER PRINCIPAL NAME	STATE
Built-in Device Compliance Policy	nross@wrajrecords.com	Compliant
Windows	nross@wrajrecords.com	Error

Overview

Manage

Properties

Monitor

Hardware

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:

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

Windows

Policy settings

Export

SETTING	STATE	STATE DETAILS
Antispyware	Compliant	
Number of non-alphanumeric characters in passw...	Compliant	
Antivirus	Compliant	
Password expiration (days)	Compliant	
Encryption of data storage on device.	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:

App Store Preview

This app is only available on the App Store for iOS devices.



Intune Company Portal 4+

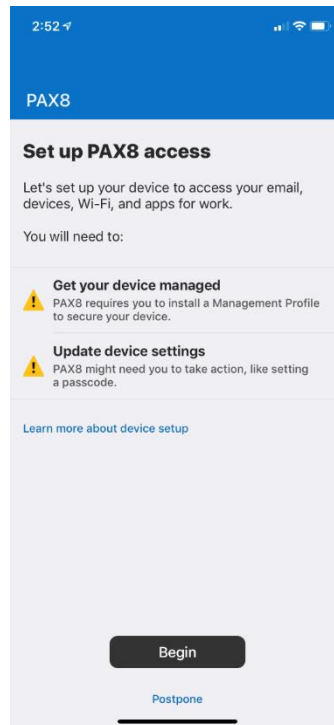
Company resources on the go
Microsoft Corporation

#61 in Business
★★★★★ 4.5, 118.7K Ratings

Free



- 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:

[iOS](#)

[Android](#)

Pilot Testing and Remediation

During our Pilot we want to discover:

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

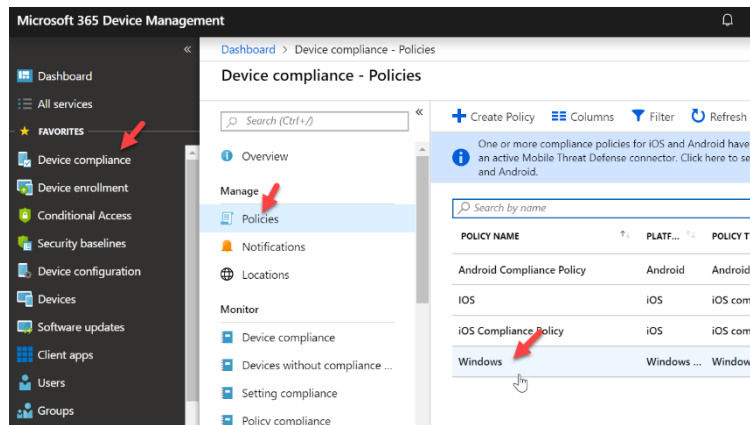
- End User Experience for Communications to Broad audience
- Common Troubleshooting Techniques for each platform

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

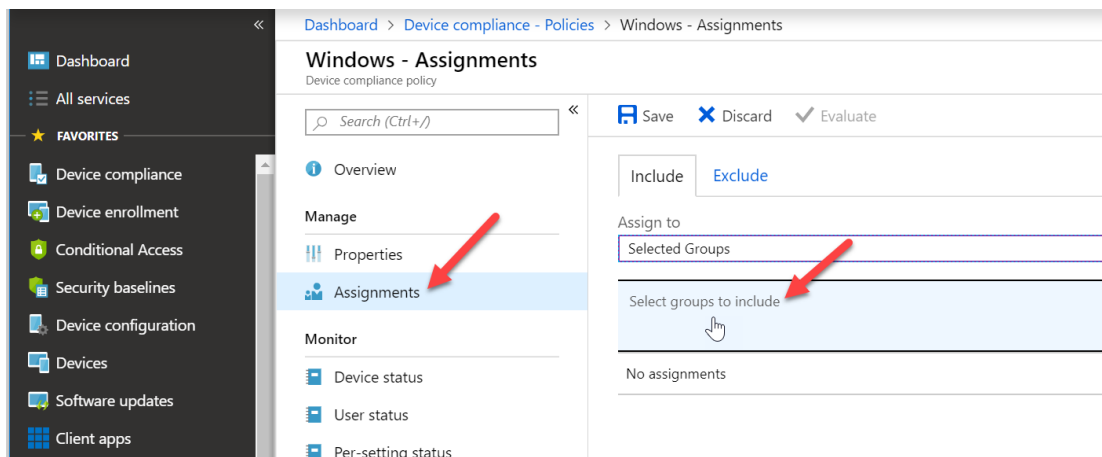
- Why is this service important?
- What pain points will it help them solve?
- What can end users expect?
- What are the steps to get my device enrolled

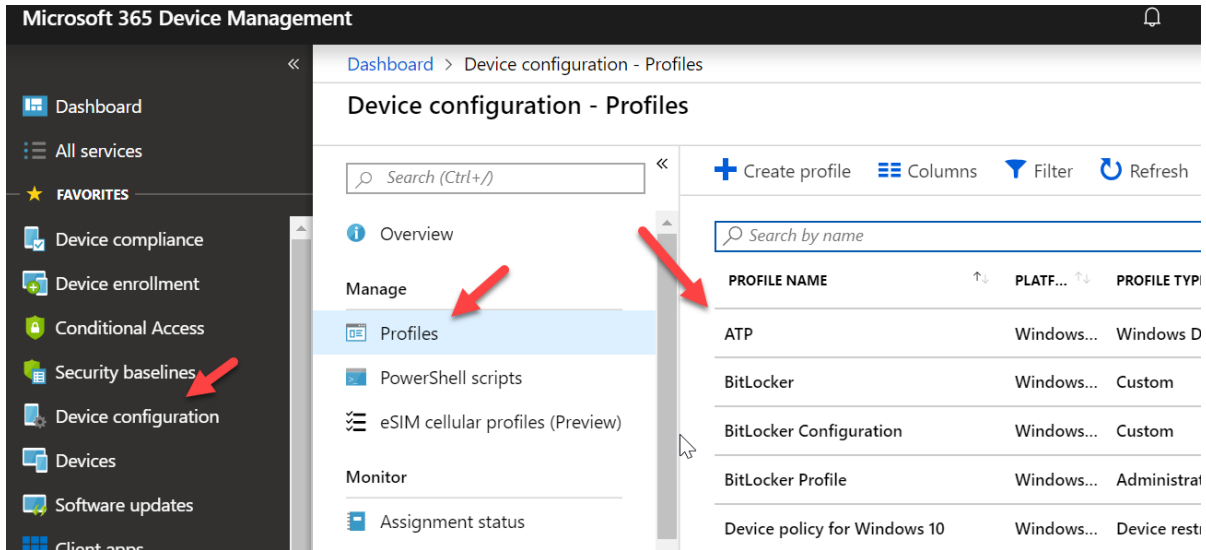
Lastly, after we have this pushed out and a target date for deployment, we can go back into the Device Management Admin Center and begin to add our groups to our policies and profiles:

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



- 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





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