



# 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



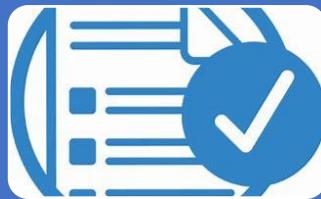
- a. Determine Platforms that you will support
  - i. IOS/Android
  - ii. MAC/Windows
- b. Have baseline security requirements complied that you want to implement
  - i. Min/Max OS versions
  - ii. Password Requirements
  - iii. Encryption Enabled
- c. Determine if there will be separate groups for separate 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 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](#)

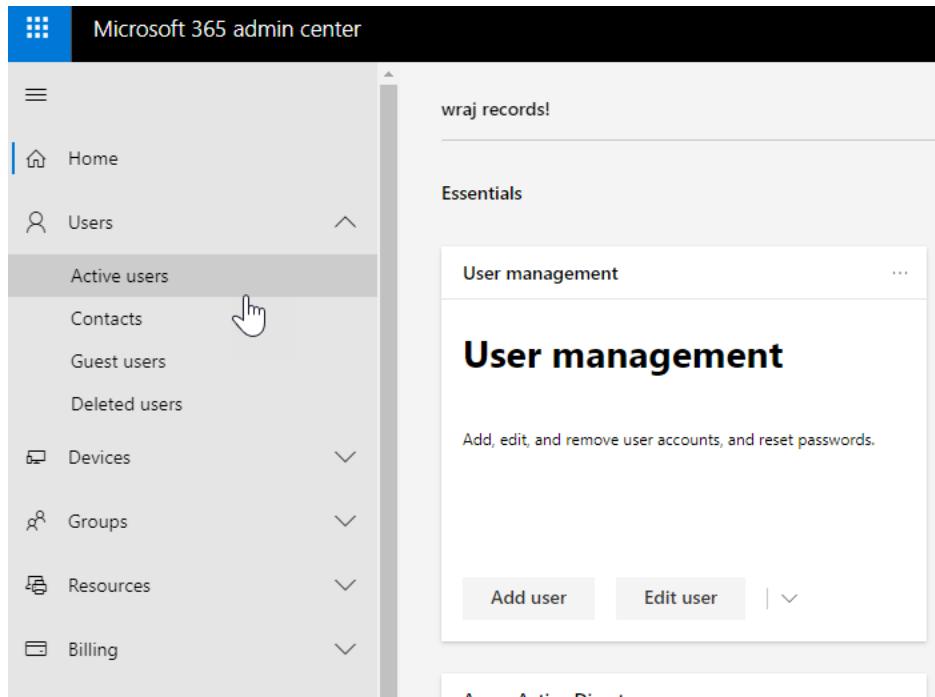
Phase 6: Testing and Broad Deployment

- Pilot Testing and Remediation

## Licensing Users

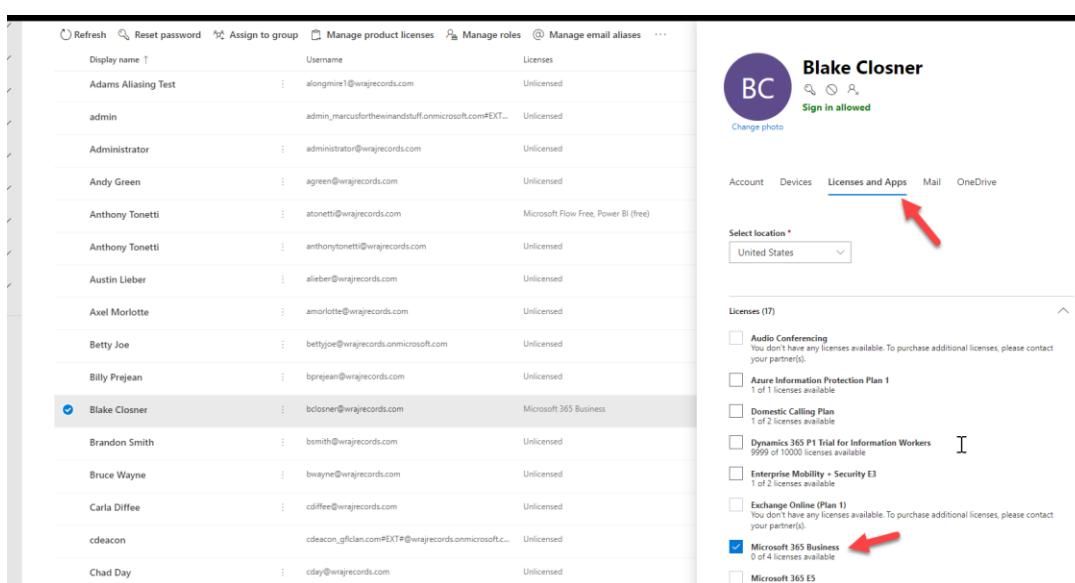
### 1. Ensure All appropriate Users are Licensed

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



The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is titled "Microsoft 365 admin center" and includes sections for Home, Users (with "Active users" selected), Devices, Groups, Resources, and Billing. The main content area is titled "User management" and contains the heading "User management". Below it is a sub-instruction: "Add, edit, and remove user accounts, and reset passwords." At the bottom of this section are "Add user" and "Edit user" buttons. A red arrow points to the "Edit user" button.

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



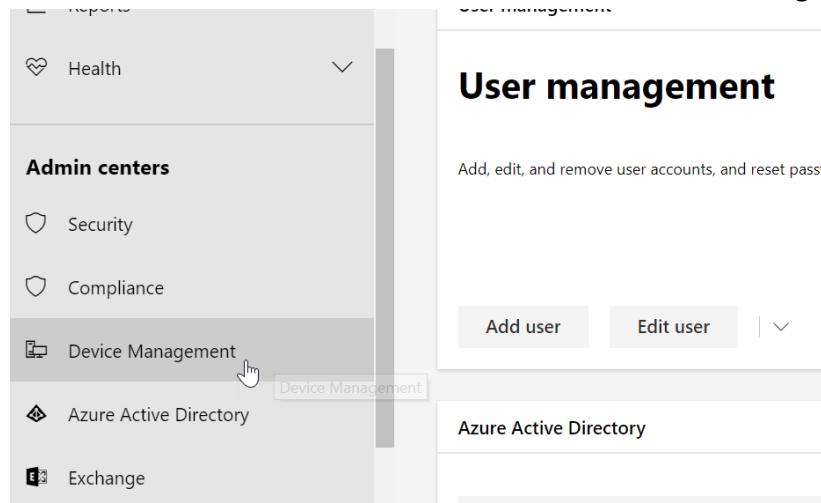
The screenshot shows the "User management" page for a specific user named "Blake Closner". The user's profile picture is shown, along with their name and a "Sign in allowed" status. Below the profile are tabs for Account, Devices, Licenses and Apps (which is currently selected and highlighted with a red arrow), Mail, and OneDrive. The "Licenses and Apps" section displays a list of available licenses:

- Audio Conferencing
- Azure Information Protection Plan 1
- Domestic Calling Plan
- Dynamics 365 P1 Trial for Information Workers
- Enterprise Mobility + Security E3
- Exchange Online (Plan 1)
- Microsoft 365 Business (selected, highlighted with a red arrow)
- Microsoft 365 E5

## Create Groups

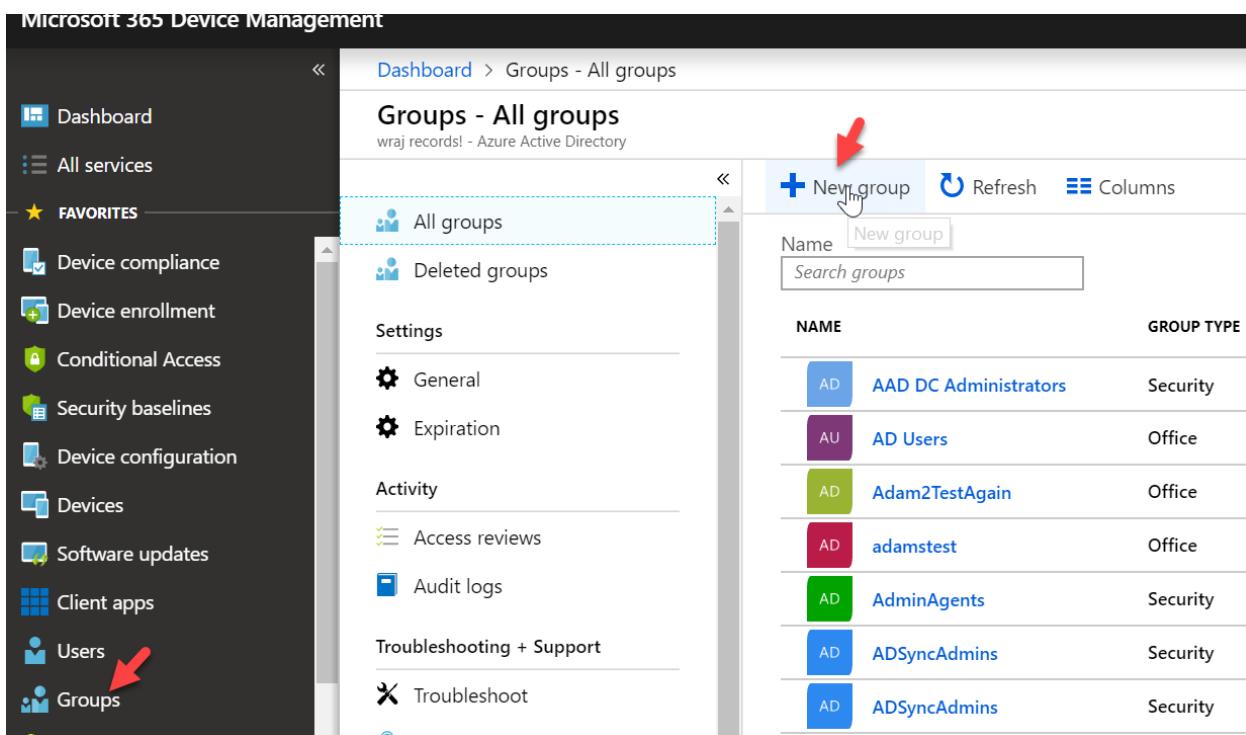
Create different groups if you want to separate out different people into different Intune Policies.

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



The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a sidebar with various admin centers: Health, Admin centers (Security, Compliance, Device Management, Azure Active Directory, Exchange), and Reports. The 'Device Management' option is highlighted with a mouse cursor. The main content area is titled 'User management' with the sub-instruction 'Add, edit, and remove user accounts, and reset password'. Below this are buttons for 'Add user' and 'Edit user'. A section for 'Azure Active Directory' is visible at the bottom.

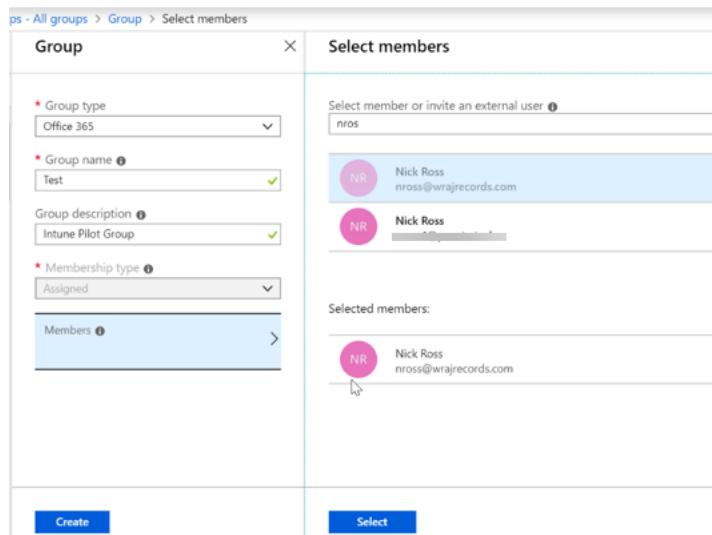
- Click on **Groups** and click **New Group**



The screenshot shows the Microsoft 365 Device Management portal. The left sidebar includes options like Dashboard, All services, Favorites (Device compliance, Device enrollment, Conditional Access, Security baselines, Device configuration, Devices, Software updates, Client apps, Users, Groups). The 'Groups' option is highlighted with a red arrow. The main content area is titled 'Groups - All groups' and shows a list of existing groups: AAD DC Administrators, AD Users, Adam2TestAgain, adamstest, AdminAgents, ADSyncAdmins, and ADSyncAdmins. At the top right, there's a 'New group' button with a red arrow pointing to it, and other buttons for Refresh and Columns. A search bar is also present.

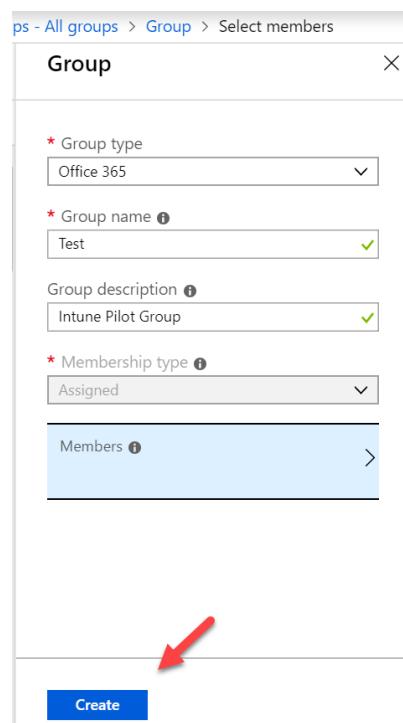
Name	Group Type
AAD DC Administrators	Security
AD Users	Office
Adam2TestAgain	Office
adamstest	Office
AdminAgents	Security
ADSsyncAdmins	Security
ADSsyncAdmins	Security

- 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



The screenshot shows the 'Select members' dialog for a new group named 'Test'. The 'Members' section lists 'nros' as a search term, with two results: 'Nick Ross' (nross@wrajrecords.com) and another user. The 'Selected members' section contains one item: 'Nick Ross' (nross@wrajrecords.com). At the bottom are 'Create' and 'Select' buttons.

- d. Click **Create** when finished

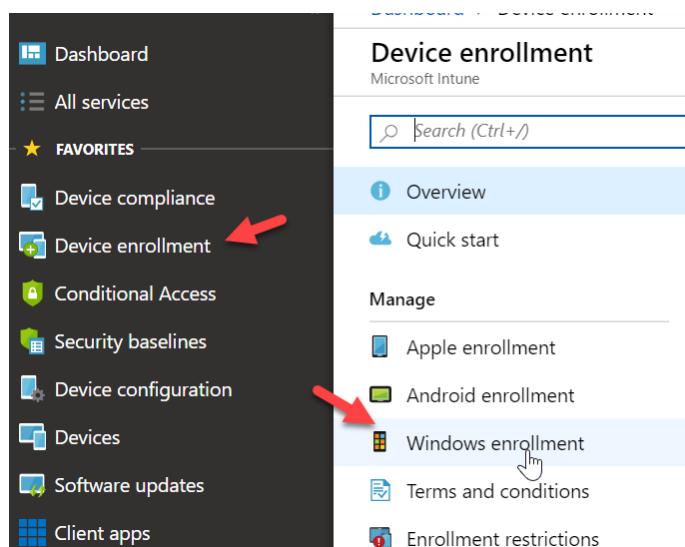


The screenshot shows the 'Group' creation dialog with the same fields as before: Group type (Office 365), Group name (Test), Group description (Intune Pilot Group), and Membership type (Assigned). The 'Members' section is empty. A red arrow points to the 'Create' button at the bottom left of the dialog.

## Device Autoenrollment

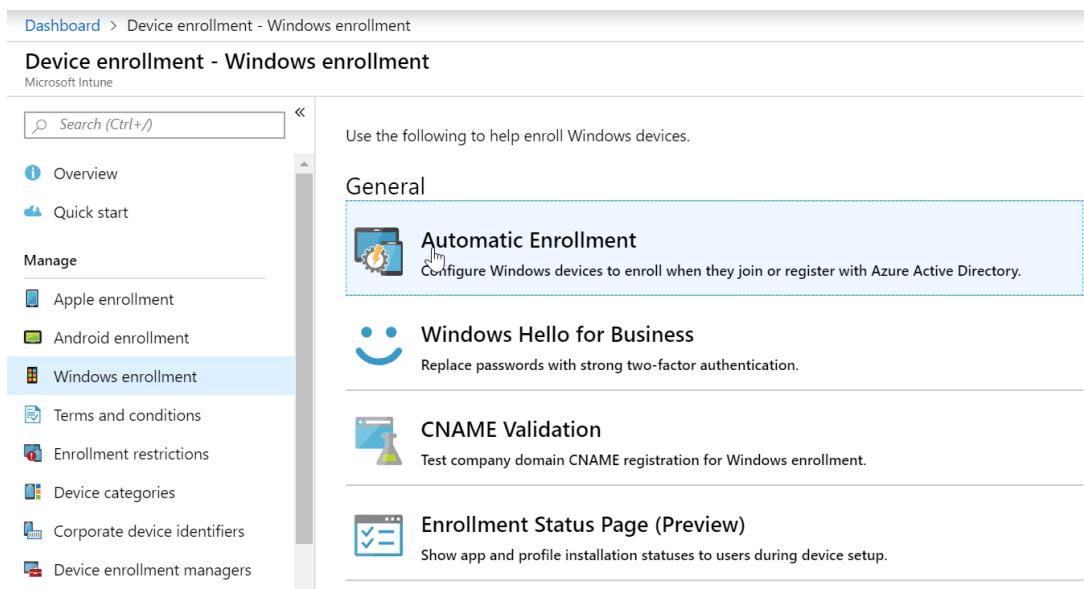
Ensure Device Autoenrollment is Turned On. Autoenrollment allows devices that join to Azure AD to automatically be enrolled in Intune and have policies push down to them:

### a. Go to Device Enrollment and click Windows Enrollment



The screenshot shows the Microsoft Intune Device Enrollment interface. On the left, there's a sidebar with various service icons. Under the 'FAVORITES' section, 'Device enrollment' is highlighted with a red arrow pointing to it. On the right, the main content area is titled 'Device enrollment' and 'Microsoft Intune'. It features a search bar and navigation links like 'Overview' (which is highlighted with a blue background), 'Quick start', 'Manage', 'Apple enrollment', 'Android enrollment', 'Windows enrollment' (which has a hand cursor icon over it, indicating it's being clicked), 'Terms and conditions', and 'Enrollment restrictions'.

### b. Select Automatic Enrollment



The screenshot shows the 'Device enrollment - Windows enrollment' page. The left sidebar has 'Windows enrollment' selected. The main content area starts with a general note: 'Use the following to help enroll Windows devices.' Below this, under the 'General' heading, there's a section titled 'Automatic Enrollment' with a sub-note: 'Configure Windows devices to enroll when they join or register with Azure Active Directory.' Further down, there are sections for 'Windows Hello for Business' (with a note about replacing passwords with strong two-factor authentication), 'CNAME Validation' (with a note about testing company domain CNAME registration for Windows enrollment), and 'Enrollment Status Page (Preview)' (with a note about showing app and profile installation statuses to users during device setup).

- 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

MDM user scope    

MDM terms of use URL

MDM discovery URL

MDM compliance URL

[Restore default MDM URLs](#)

MAM User scope

MAM Terms of use URL

MAM Discovery URL

MAM Compliance URL

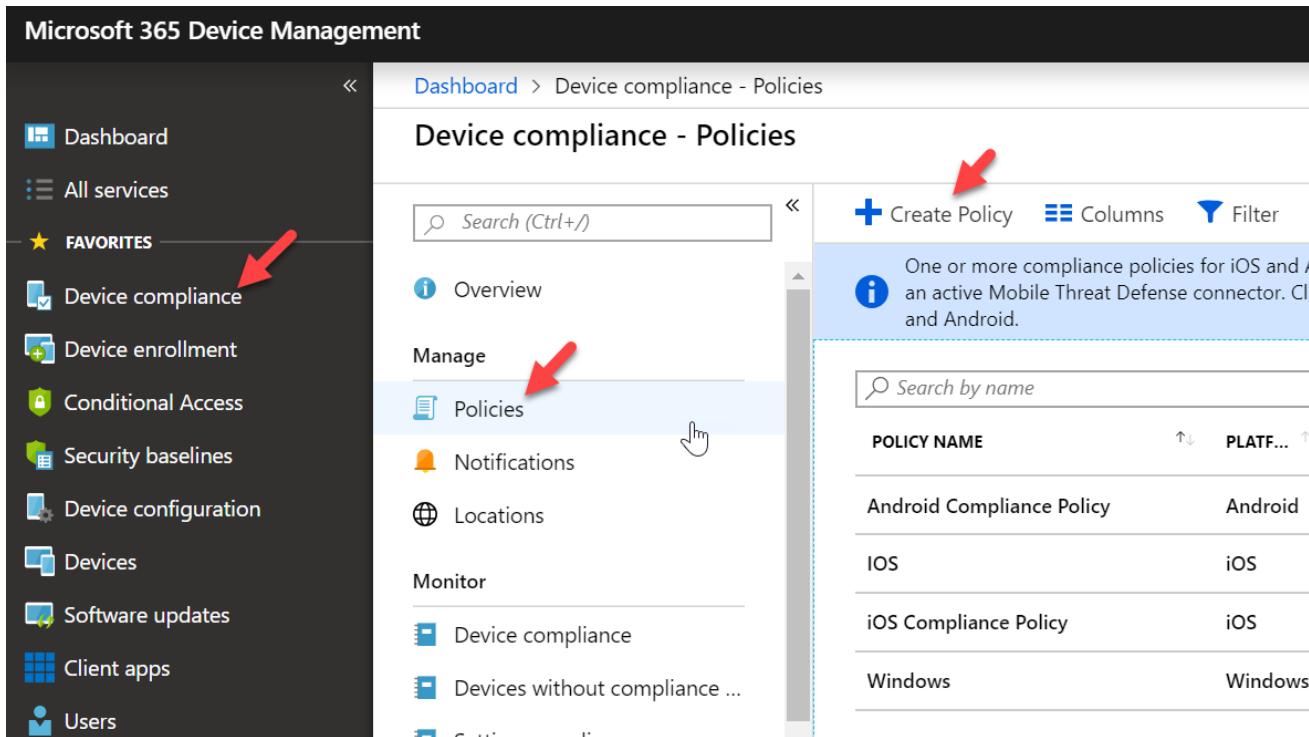
[Restore default MAM URLs](#)

## 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

- 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+ /)

**Create Policy** Columns Filter

One or more compliance policies for iOS and A  
an active Mobile Threat Defense connector. Cli  
and Android.

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

**FAVORITES**

- Device compliance (highlighted with red arrow)
- Device enrollment
- Conditional Access
- Security baselines
- Device configuration
- Devices
- Software updates
- Client apps
- Users

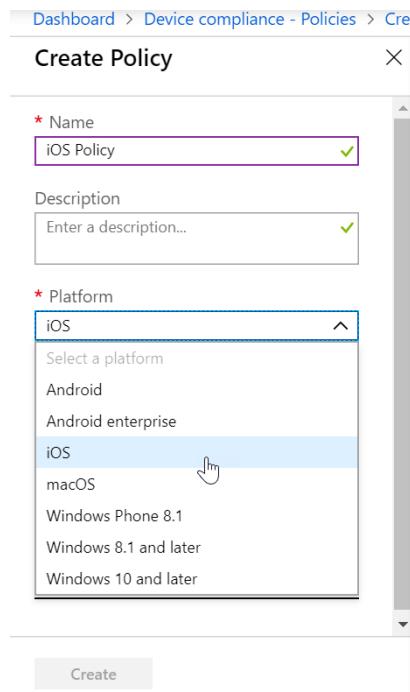
**Manage**

- Overview
- Policies (highlighted with red arrow)
- Notifications
- Locations

**Monitor**

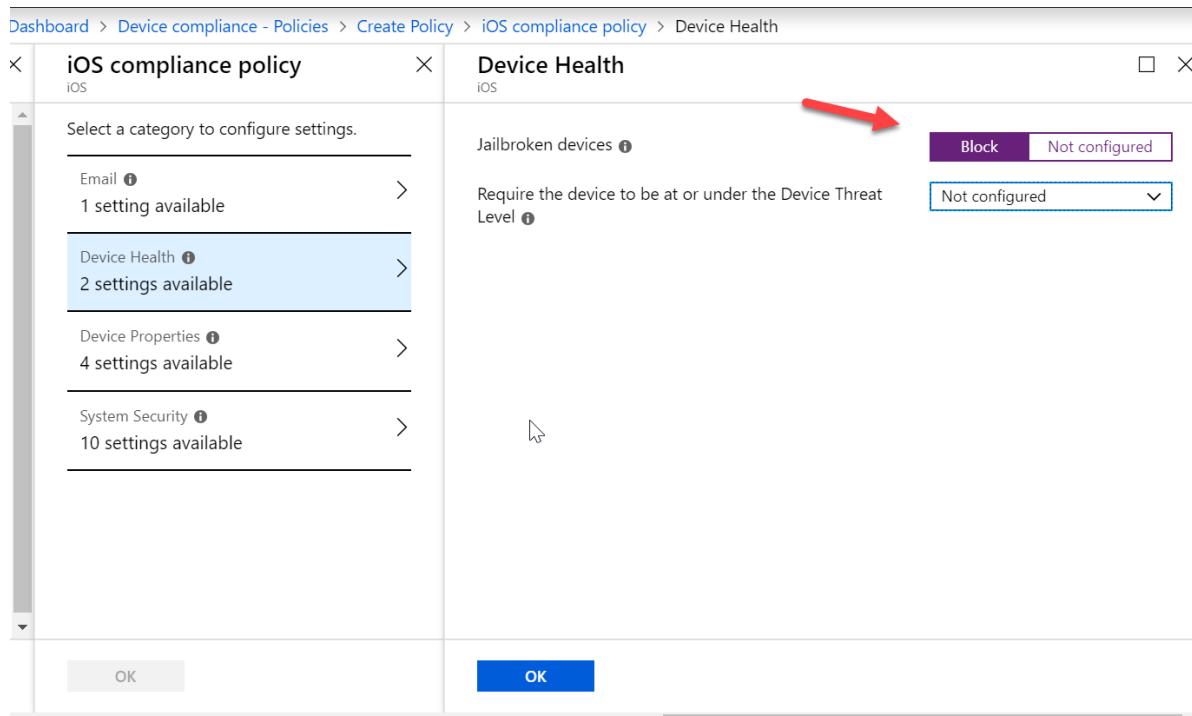
- Device compliance
- Devices without compliance ...
- Setting compliance

- 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



The screenshot shows the 'Create Policy' dialog. The 'Name' field contains 'iOS Policy'. The 'Description' field is empty. The 'Platform' dropdown is set to 'iOS', which is highlighted in blue. Other options in the dropdown include 'Select a platform', 'Android', 'Android enterprise', 'macOS', 'Windows Phone 8.1', 'Windows 8.1 and later', and 'Windows 10 and later'. A 'Create' button is at the bottom.

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



The screenshot shows the 'Device Health' configuration screen for the 'iOS compliance policy'. On the left, there are four categories: 'Email' (1 setting available), 'Device Health' (2 settings available, highlighted in blue), 'Device Properties' (4 settings available), and 'System Security' (10 settings available). On the right, under 'Device Health', there is a section for 'Jailbroken devices'. It shows a status of 'Not configured' with a dropdown menu. A red arrow points to the 'Block' button in the dropdown menu. At the bottom, there are 'OK' buttons for both the left and right sections.

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

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

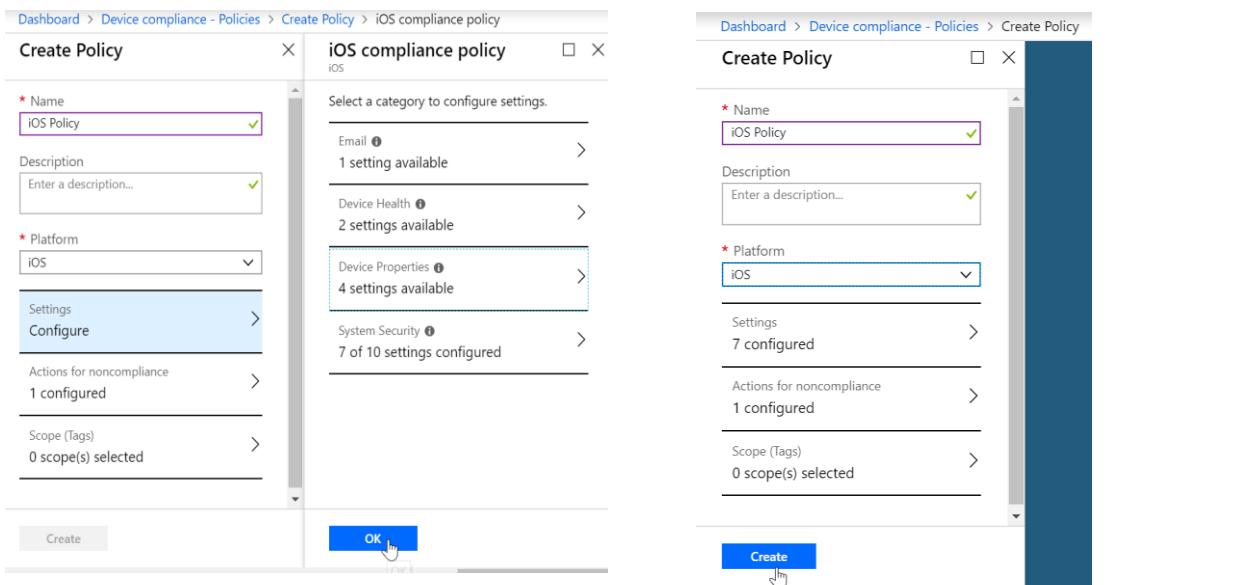
<b>iOS compliance policy</b> iOS  Select a category to configure settings. <hr/> Email ⓘ 1 setting available > <hr/> Device Health ⓘ 2 settings available > <hr/> Device Properties ⓘ 4 settings available > <hr/> System Security ⓘ 10 settings available > <hr/>	<b>Device Properties</b> iOS  Operating System Version Minimum OS version ⓘ Not configured Maximum OS version ⓘ Not configured Minimum OS build version ⓘ Not configured Maximum OS build version ⓘ Not configured  OK <b>OK</b>
--	---

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

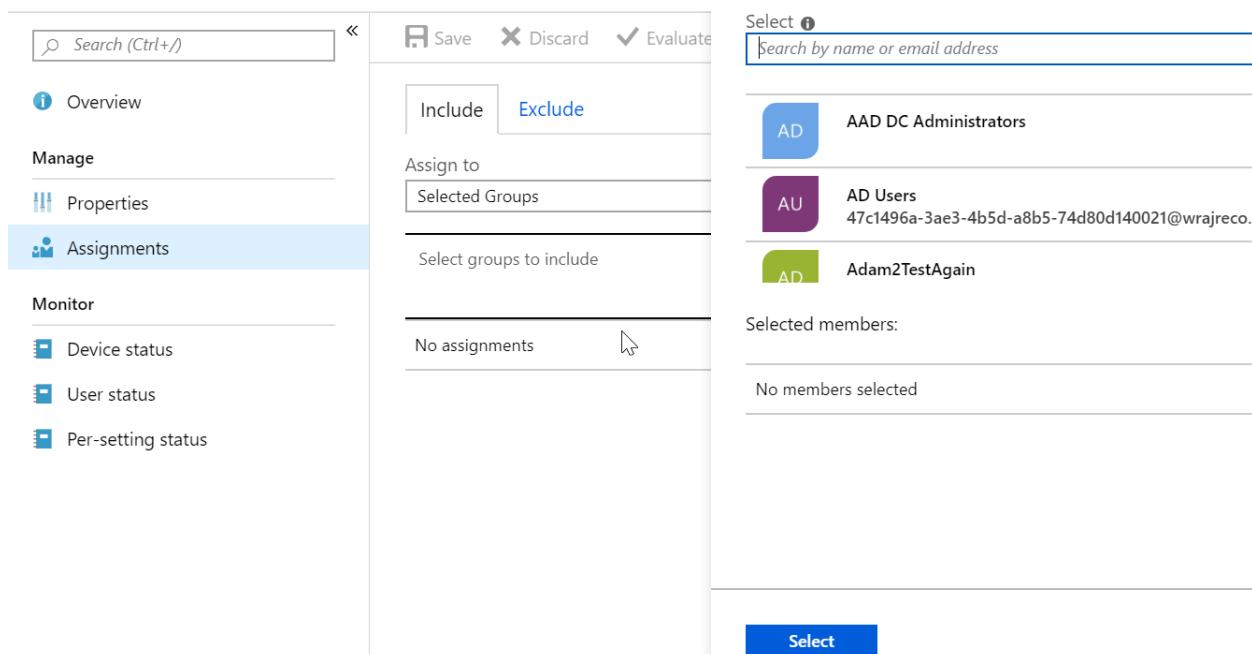
iBoard > Device compliance - Policies > Create Policy > iOS compliance policy > System Security

<b>iOS compliance policy</b> iOS  Select a category to configure settings. <hr/> Email ⓘ 1 setting available > <hr/> Device Health ⓘ 2 settings available > <hr/> Device Properties ⓘ 4 settings available > <hr/> System Security ⓘ 10 settings available > <hr/>	<b>System Security</b> iOS  Require a password to unlock mobile devices. ⓘ Simple passwords ⓘ Block Not configured Minimum password length ⓘ 4 ✓ Required password type ⓘ Numeric Number of non-alphanumeric characters in password ⓘ Not configured Maximum minutes after screen lock before password is required ⓘ 15 Minutes ✓ Maximum minutes of inactivity until screen locks ⓘ 15 Minutes ✓ Password expiration (days) ⓘ 90 ✓ Number of previous passwords to prevent reuse ⓘ 3 ✓  OK <b>OK</b>
--	--

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

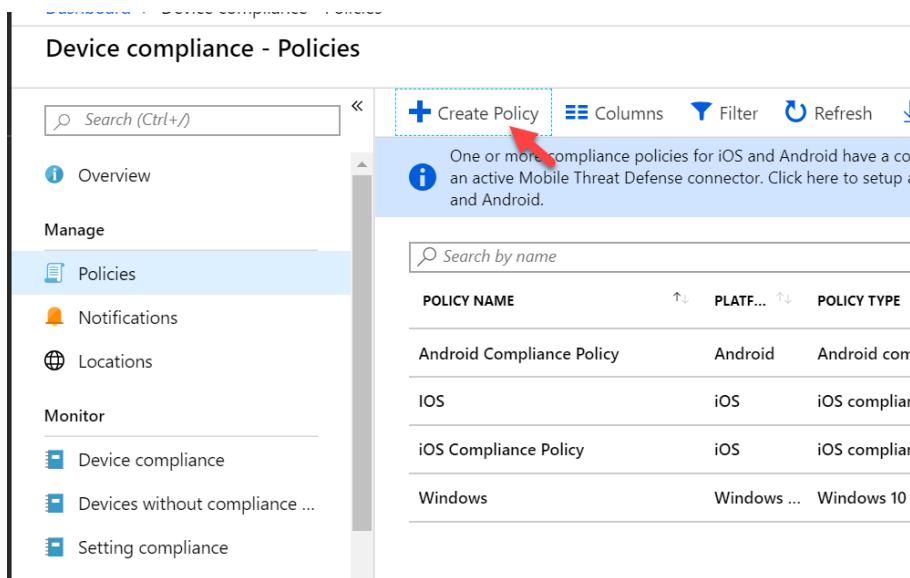


g. Select Assignments and select the group of users you want this policy applied to:



## Android

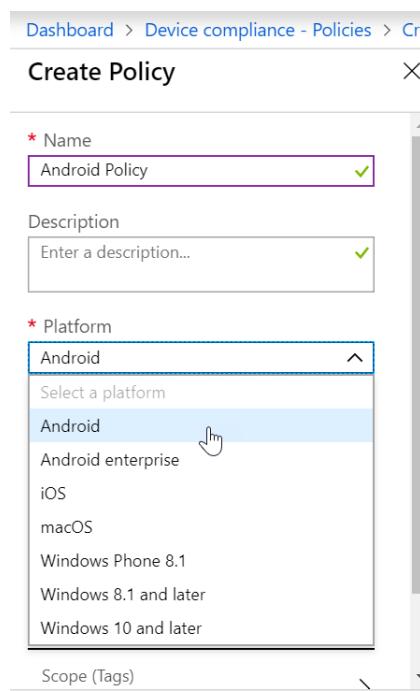
- Click Create Policy



The screenshot shows the 'Device compliance - Policies' page. On the left, there's a sidebar with 'Overview', 'Manage' (selected), 'Notifications', 'Locations', 'Monitor' (with 'Device compliance' selected), 'Devices without compliance ...', and 'Setting compliance'. The main area has a search bar and a 'Create Policy' button (highlighted with a red arrow). A tooltip says: 'One or more compliance policies for iOS and Android have a connection to an active Mobile Threat Defense connector. Click here to setup a policy for iOS and Android.' Below is a table with columns: POLICY NAME, PLATF..., and POLICY TYPE. It lists four policies: 'Android Compliance Policy' (Android, Android compliance), 'iOS' (iOS, iOS compliance), 'iOS Compliance Policy' (iOS, iOS compliance), and 'Windows' (Windows, Windows 10 compliance).

POLICY NAME	PLATF...	POLICY TYPE
Android Compliance Policy	Android	Android compliance
iOS	iOS	iOS compliance
iOS Compliance Policy	iOS	iOS compliance
Windows	Windows ...	Windows 10 compliance

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



The screenshot shows the 'Create Policy' dialog. It has fields for 'Name' (set to 'Android Policy'), 'Description' (empty), and 'Platform' (set to 'Android'). The 'Platform' dropdown menu is open, showing options like 'Select a platform', 'Android', 'Android enterprise', 'iOS', 'macOS', 'Windows Phone 8.1', 'Windows 8.1 and later', and 'Windows 10 and later'. There's also a 'Scope (Tags)' section at the bottom.

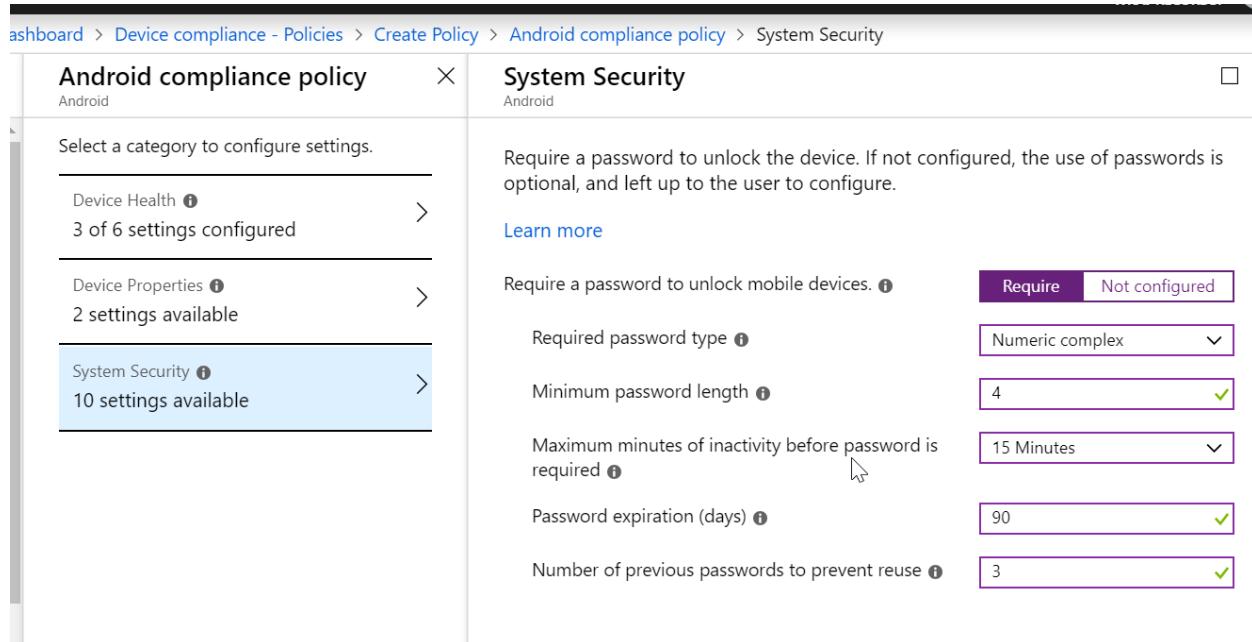
c. Under Settings>Device Health, configure the following:

Android compliance policy	Device Health
Android	Android
Select a category to configure settings.	
Device Health ⓘ 6 settings available	Rooted devices ⓘ
Device Properties ⓘ 2 settings available	Require the device to be at or under the Device Threat Level ⓘ
System Security ⓘ 10 settings available	Google Play Protect
	Google Play Services is configured ⓘ
	Up-to-date security provider ⓘ
	Threat scan on apps ⓘ
	SafetyNet device attestation ⓘ
OK	OK

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

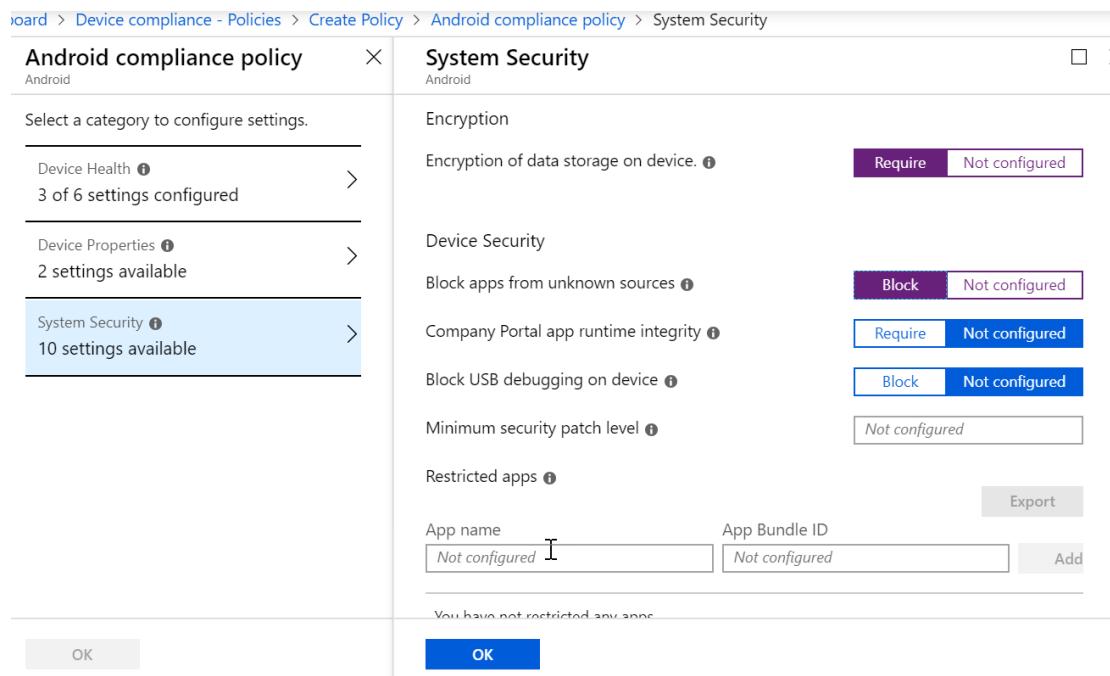
board > Device compliance - Policies > Create Policy > Android compliance policy > Device Properties	
Android compliance policy	Device Properties
Android	Android
Select a category to configure settings.	Operating System Version
Device Health ⓘ 3 of 6 settings configured	Minimum OS version ⓘ
Device Properties ⓘ 2 settings available	Not configured
System Security ⓘ 10 settings available	Maximum OS version ⓘ
OK	OK

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



The screenshot shows the 'System Security' configuration page for an 'Android compliance policy'. On the left, there's a sidebar with categories: 'Device Health' (3 of 6 settings configured), 'Device Properties' (2 settings available), and 'System Security' (10 settings available). The 'System Security' section is currently selected. On the right, the configuration details are listed:

- Require a password to unlock mobile devices.**: Configuration status is 'Not configured'.
- Required password type**: Set to 'Numeric complex'.
- Minimum password length**: Set to '4'.
- Maximum minutes of inactivity before password is required**: Set to '15 Minutes'.
- Password expiration (days)**: Set to '90'.
- Number of previous passwords to prevent reuse**: Set to '3'.



This screenshot shows the same 'System Security' configuration page, but with more expanded options. The 'Encryption' section is now visible, containing the following settings:

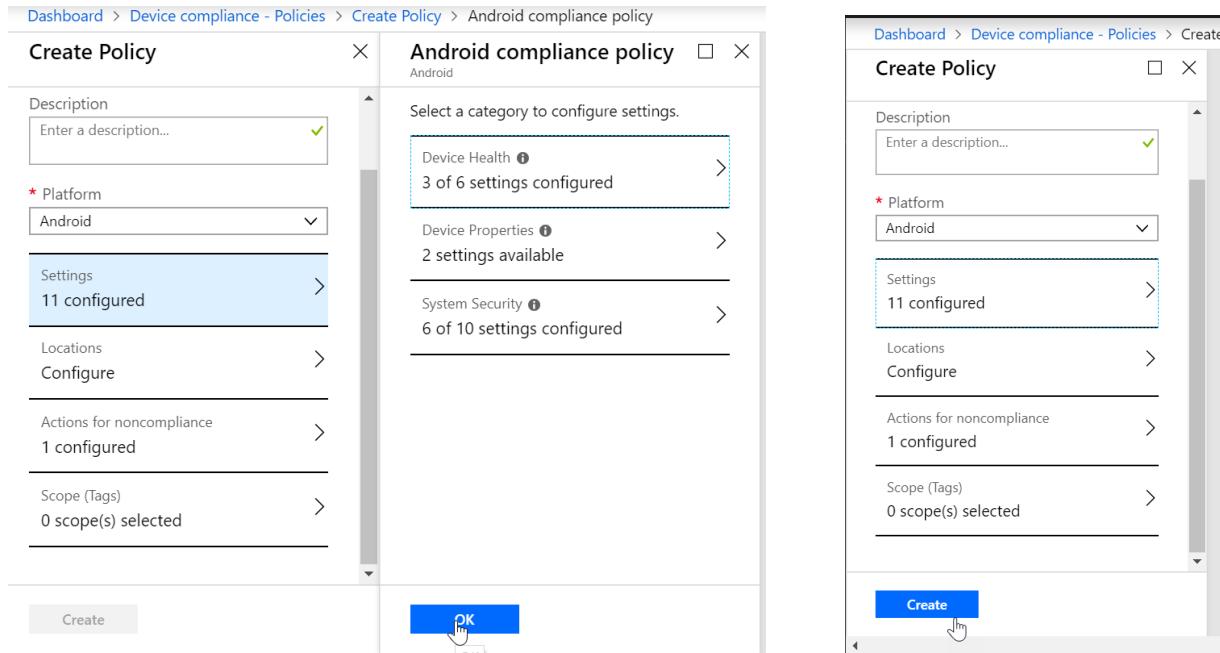
- Encryption of data storage on device.**: Configuration status is 'Not configured'.

The 'Device Security' section is also expanded, showing:

- Block apps from unknown sources**: Configuration status is 'Not configured'.
- Company Portal app runtime integrity**: Configuration status is 'Not configured'.
- Block USB debugging on device**: Configuration status is 'Not configured'.
- Minimum security patch level**: Configuration status is 'Not configured'.

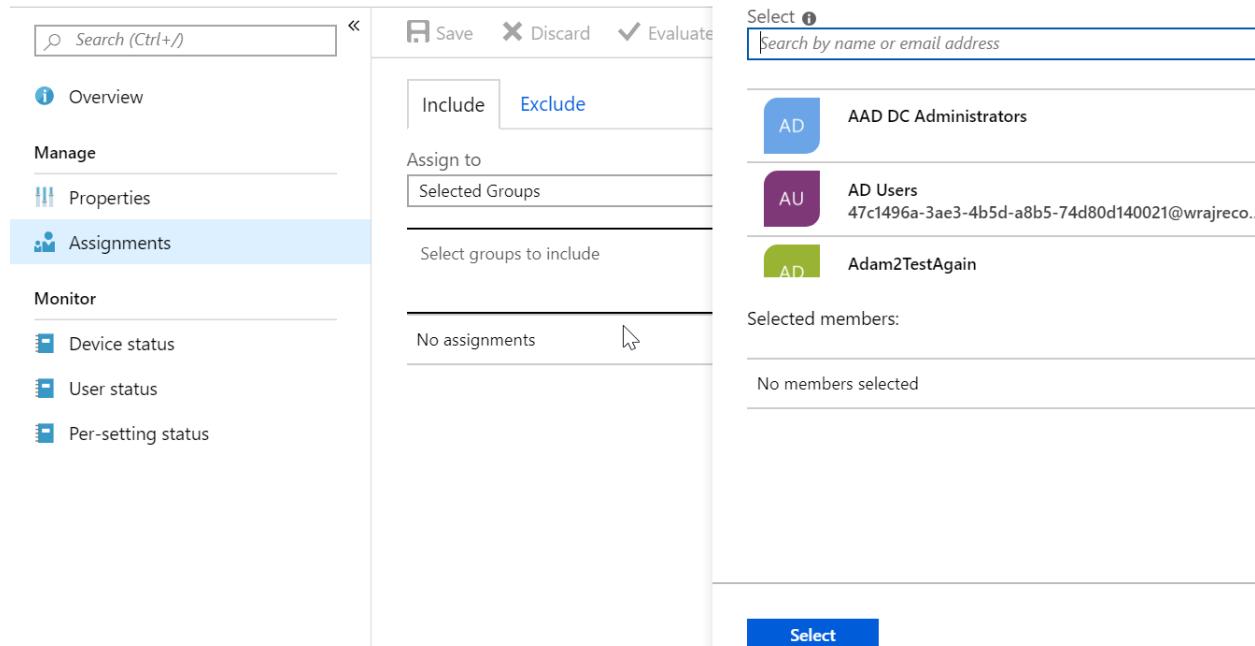
The 'Restricted apps' section is shown with fields for 'App name' and 'App Bundle ID', both set to 'Not configured'. There are 'Export' and 'Add' buttons next to these fields. A note at the bottom states: 'You have not restricted any apps.'

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



The screenshot shows the 'Create Policy' interface for an 'Android compliance policy'. On the left, there's a sidebar with options like 'Description', 'Platform' (set to 'Android'), 'Settings' (11 configured), 'Locations', 'Configure', 'Actions for noncompliance', and 'Scope (Tags)'. The main area shows 'Select a category to configure settings' with three sections: 'Device Health' (3 of 6 settings configured), 'Device Properties' (2 settings available), and 'System Security' (6 of 10 settings configured). At the bottom right is a blue 'OK' button with a cursor pointing at it.

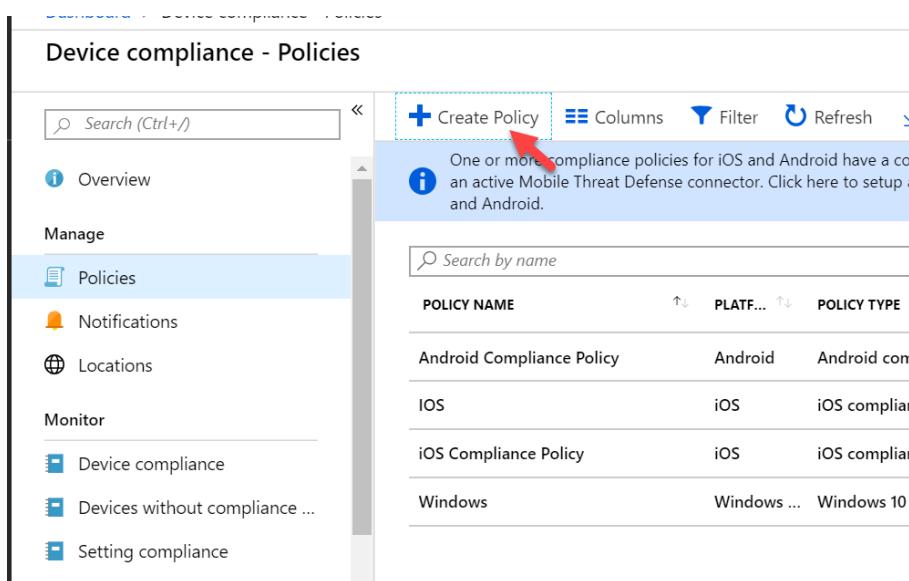
g. Select Assignments and select the group of users you want this to apply to:



The screenshot shows the 'Assignments' section of the Microsoft Intune interface. The 'Assignments' tab is selected in the sidebar. In the center, there's a 'Save', 'Discard', and 'Evaluate' button bar. Below it, there are tabs for 'Include' and 'Exclude', with 'Include' selected. The 'Assign to' section shows 'Selected Groups' and a link to 'Select groups to include'. At the bottom, it says 'No assignments'. To the right, a 'Select' dialog box is open, titled 'Select'. It has a search bar 'Search by name or email address'. Below it is a list of groups: 'AAD DC Administrators' (AD icon), 'AD Users' (AU icon with a long email address), and 'Adam2TestAgain' (AD icon). Underneath the list, it says 'Selected members:' and 'No members selected'. At the bottom of the dialog is a blue 'Select' button with a cursor pointing at it.

## Windows

- Click Create Policy



**Device compliance - Policies**

Search (Ctrl+)

Create Policy Columns Filter Refresh

One or more compliance policies for iOS and Android have a co... an active Mobile Threat Defense connector. Click here to setup a...

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

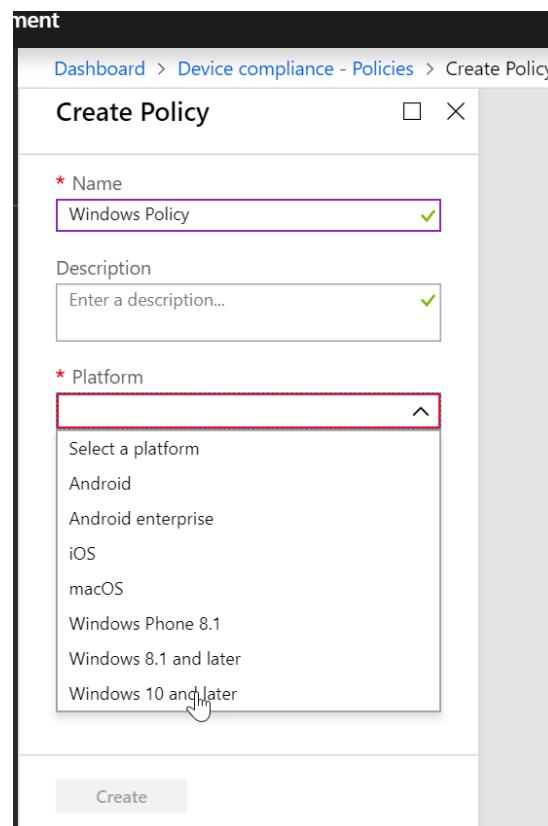
Manage

- Overview
- Policies (selected)
- Notifications
- Locations

Monitor

- Device compliance
- Devices without compliance ...
- Setting compliance

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



Dashboard > Device compliance - Policies > Create Policy

Create Policy

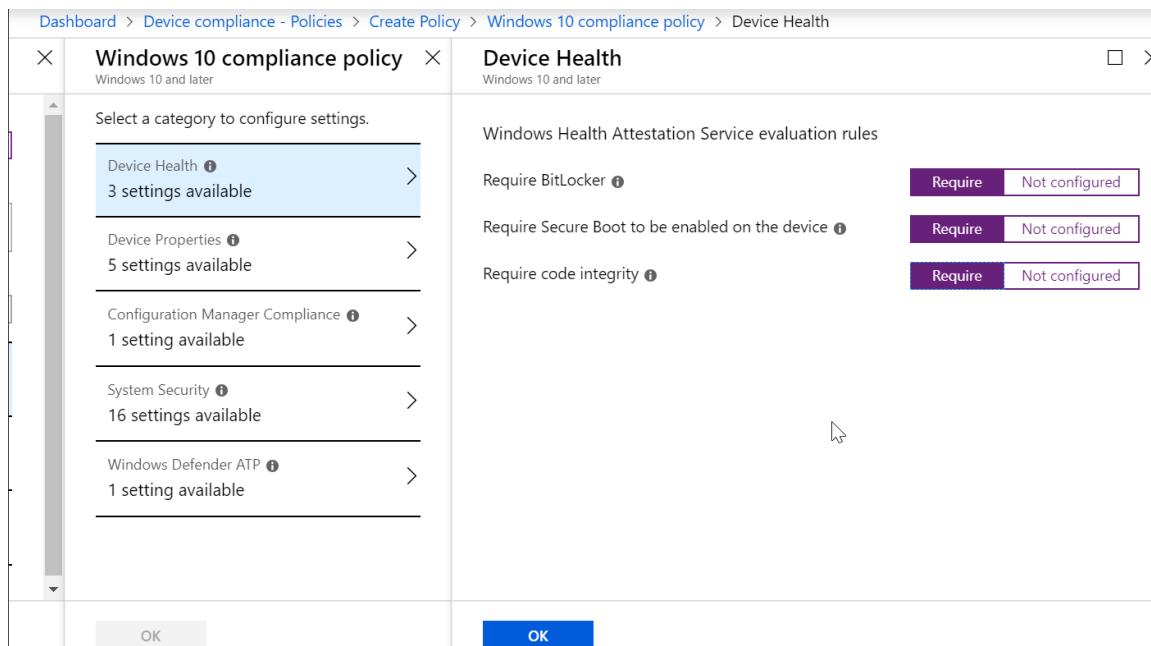
\* Name  
Windows Policy

Description  
Enter a description...

\* Platform  
Select a platform  
Android  
Android enterprise  
iOS  
macOS  
Windows Phone 8.1  
Windows 8.1 and later  
Windows 10 and later

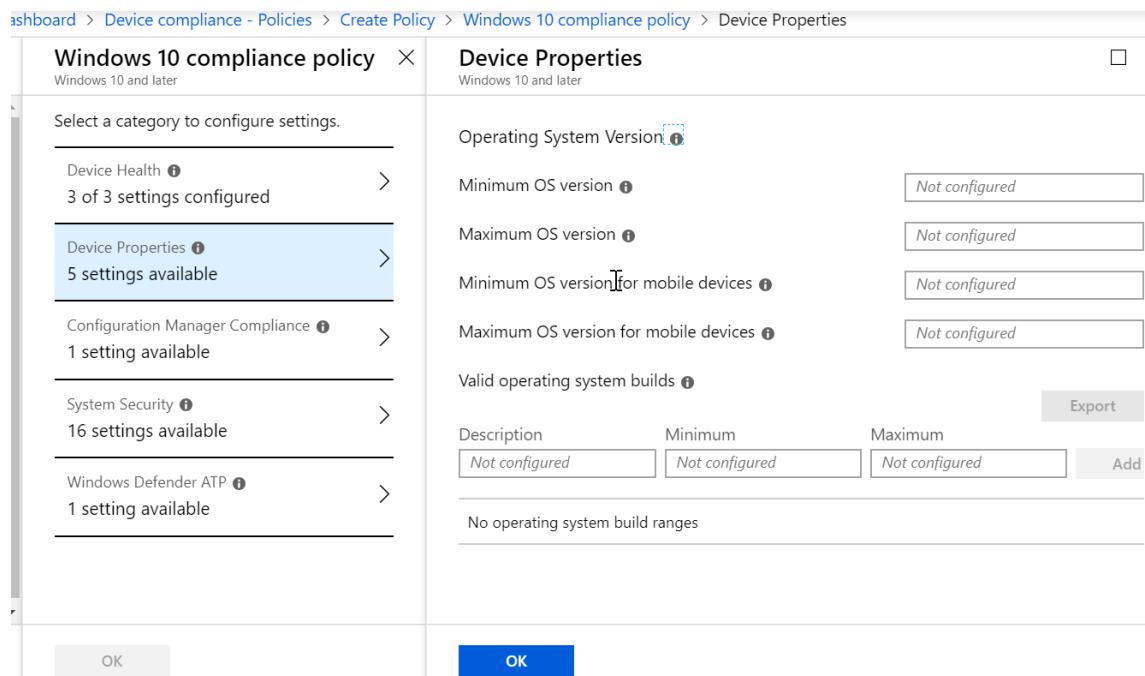
Create

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



The screenshot shows the 'Device Health' configuration page for a 'Windows 10 compliance policy'. The left pane lists categories: 'Device Health' (3 settings available), 'Device Properties' (5 settings available), 'Configuration Manager Compliance' (1 setting available), 'System Security' (16 settings available), and 'Windows Defender ATP' (1 setting available). The right pane shows 'Windows Health Attestation Service evaluation rules' with three items: 'Require BitLocker' (Require, Not configured), 'Require Secure Boot to be enabled on the device' (Require, Not configured), and 'Require code integrity' (Require, Not configured). Buttons at the bottom are 'OK' (grey) and 'OK' (blue).

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



The screenshot shows the 'Device Properties' configuration page for a 'Windows 10 compliance policy'. The left pane lists categories: 'Device Health' (3 of 3 settings configured), 'Device Properties' (5 settings available), 'Configuration Manager Compliance' (1 setting available), 'System Security' (16 settings available), and 'Windows Defender ATP' (1 setting available). The right pane shows 'Operating System Version' settings: 'Minimum OS version' and 'Maximum OS version' both set to 'Not configured'. It also shows 'Minimum OS version for mobile devices' and 'Maximum OS version for mobile devices' both set to 'Not configured'. A 'Valid operating system builds' section is present with a table for adding ranges. Buttons at the bottom are 'OK' (grey) and 'OK' (blue).

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

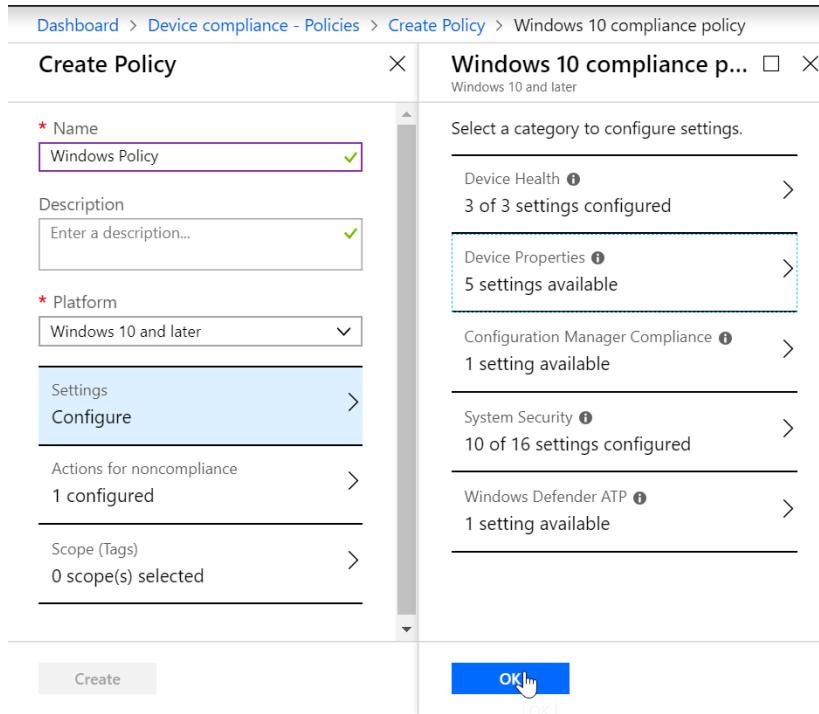
Dashboard > Device compliance - Policies > Create Policy > Windows 10 compliance policy > System Security

Windows 10 compliance policy		System Security	
Select a category to configure settings.		Windows 10 and later	
<a href="#">Device Health</a> 3 of 3 settings configured <a href="#">Device Properties</a> 5 settings available <a href="#">Configuration Manager Compliance</a> 1 setting available <b><a href="#">System Security</a></b> 16 settings available <a href="#">Windows Defender ATP</a> 1 setting available		<b>Password</b> Require a password to unlock mobile devices. <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Simple passwords</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Block</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Password type</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Device default</span> <b>Minimum password length</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">8</span> ✓ <b>Maximum minutes of inactivity before password is required</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">15 Minutes</span> <b>Password expiration (days)</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">90</span> ✓ <b>Number of previous passwords to prevent reuse</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">3</span> ✓ <b>Require password when device returns from idle state (Mobile and Holographic)</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span>	
<a href="#">OK</a>		<a href="#">OK</a>	

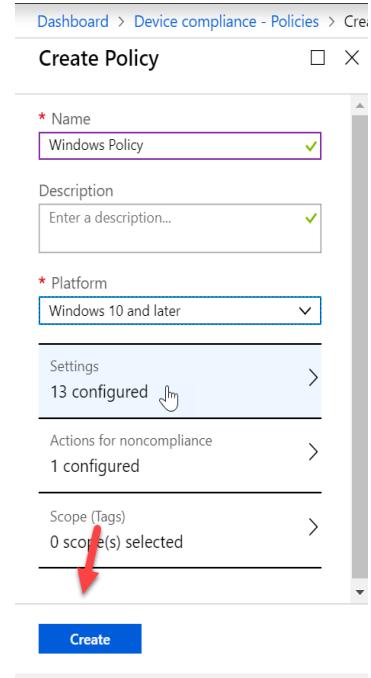
Dashboard > Device compliance - Policies > Create Policy > Windows 10 compliance policy > System Security

Windows 10 compliance policy		System Security	
Select a category to configure settings.		Windows 10 and later	
<a href="#">Device Health</a> 3 of 3 settings configured <a href="#">Device Properties</a> 5 settings available <a href="#">Configuration Manager Compliance</a> 1 setting available <b><a href="#">System Security</a></b> 16 settings available <a href="#">Windows Defender ATP</a> 1 setting available		<b>Encryption of data storage on device.</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Device Security</b> <b>Firewall</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Antivirus</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Antispyware</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Defender</b> <b>Windows Defender Antimalware</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Windows Defender Antimalware minimum version</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Windows Defender Antimalware signature up-to-date</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span> <b>Real-time protection</b> <a href="#">ⓘ</a> <span style="border: 1px solid #ccc; padding: 2px;">Require</span> <span style="border: 1px solid #ccc; padding: 2px;">Not configured</span>	
<a href="#">OK</a>		<a href="#">OK</a>	

f. Click Ok and Create

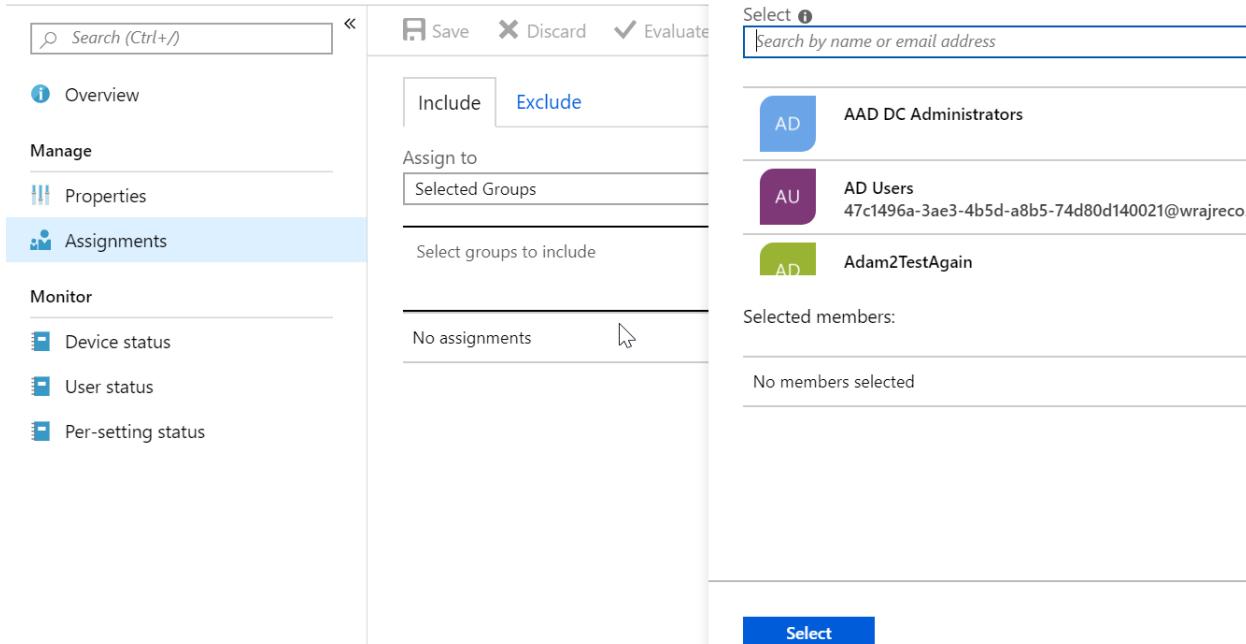


The screenshot shows the 'Create Policy' dialog for a 'Windows 10 compliance policy'. The 'Name' field is set to 'Windows Policy'. The 'Platform' dropdown is set to 'Windows 10 and later'. The 'Settings' section shows 'Configure' selected. Under 'Actions for noncompliance', '1 configured' is listed. Under 'Scope (Tags)', '0 scope(s) selected' is shown. On the right, the 'Windows 10 compliance p...' configuration page is displayed, showing various settings categories like Device Health, Device Properties, Configuration Manager Compliance, System Security, and Windows Defender ATP, each with their respective settings status. At the bottom is an 'OK' button.



This screenshot shows the same 'Create Policy' dialog after configuration. The 'Name' field is still 'Windows Policy'. The 'Platform' dropdown is now set to 'Windows 10 and later'. The 'Settings' section shows '13 configured'. Under 'Actions for noncompliance', '1 configured' is listed. Under 'Scope (Tags)', '0 scope(s) selected' is shown. A red arrow points to the 'Create' button at the bottom. The configuration page on the right is identical to the previous screenshot.

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



The screenshot shows the 'Assignments' blade in the Microsoft Intune portal. The left sidebar includes 'Overview', 'Properties', and 'Assignments' (which is selected). The main area shows a 'Save' button, a 'Discard' button, and an 'Evaluate' button. Below these are tabs for 'Include' and 'Exclude'. The 'Assign to' section shows 'Selected Groups' and a 'Select groups to include' button. The 'No assignments' button is visible. To the right, a 'Select' blade is open, titled 'Select'. It contains a search bar 'Search by name or email address' and a list of users and groups: 'AAD DC Administrators', 'AD Users' (with a long GUID), and 'Adam2TestAgain'. Below this is a 'Selected members:' section which currently says 'No members selected'. At the bottom is a 'Select' button.

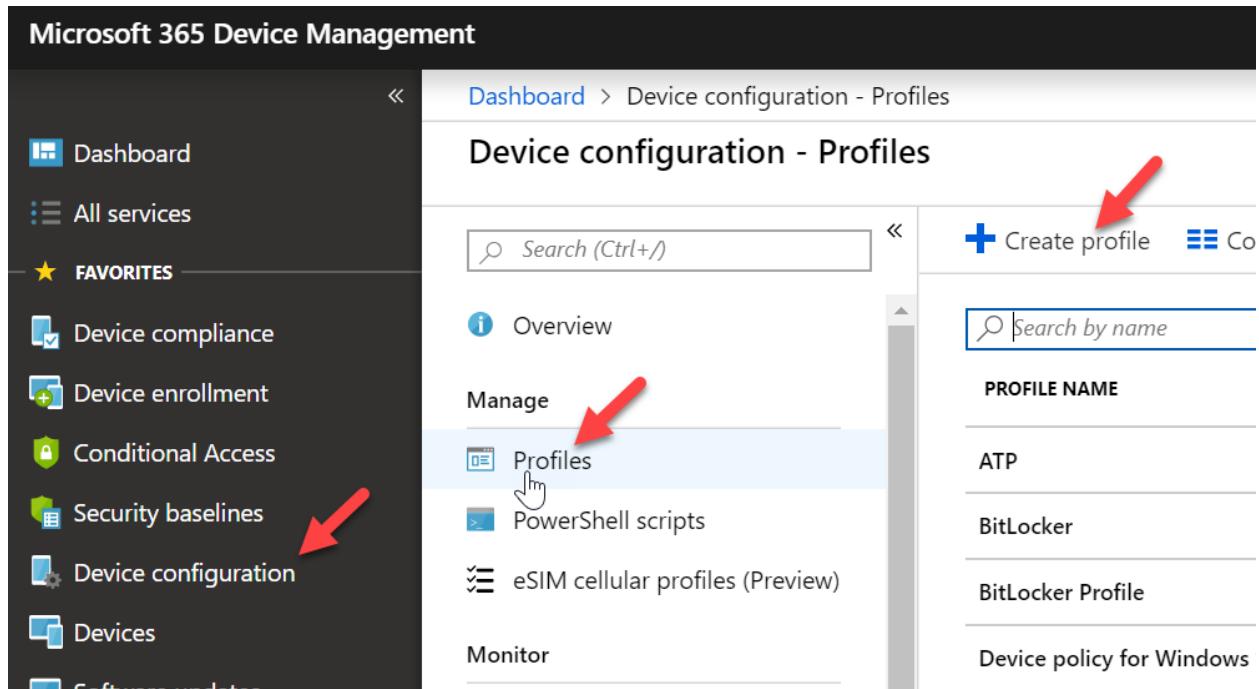
## Create Device Profile

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](#)

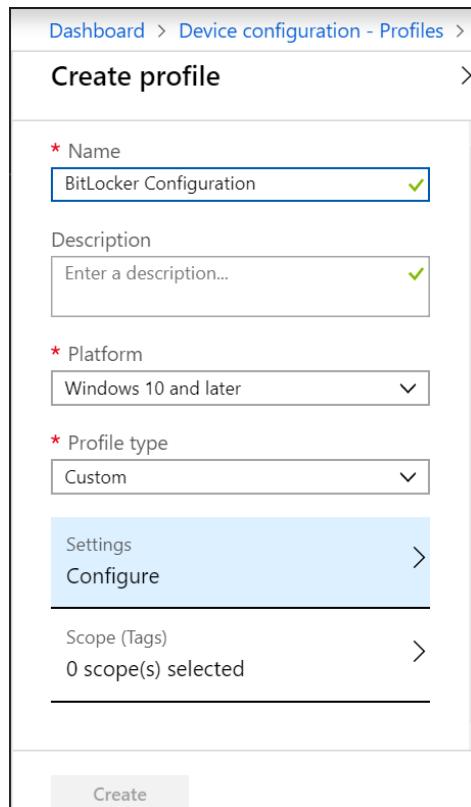
Since we configured a policy in the previous section to Require Bitlocker, we are going to set up a profile for Bitlocker so that users are immediately prompted to configure if they do not have it already.

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



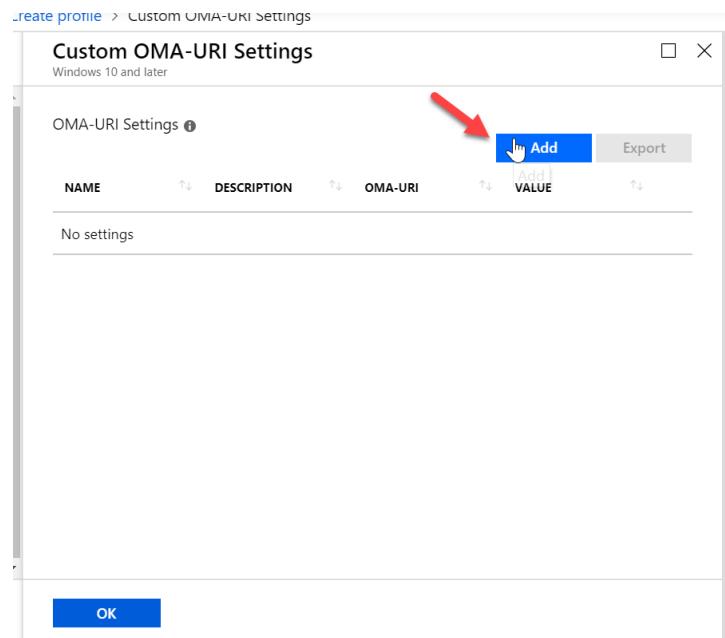
The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a navigation sidebar with various options like Dashboard, All services, Favorites (Device compliance, Device enrollment, Conditional Access, Security baselines, Device configuration, Devices, Software distribution), and more. A red arrow points to the 'Device configuration' option. The main area is titled 'Device configuration - Profiles' and shows a list of sections: Overview, Manage (Profiles, PowerShell scripts, eSIM cellular profiles (Preview)), and Monitor. On the right, there's a search bar and a 'Create profile' button with a plus sign, also highlighted by a red arrow. Below it, there's a 'PROFILE NAME' input field containing 'ATP'.

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

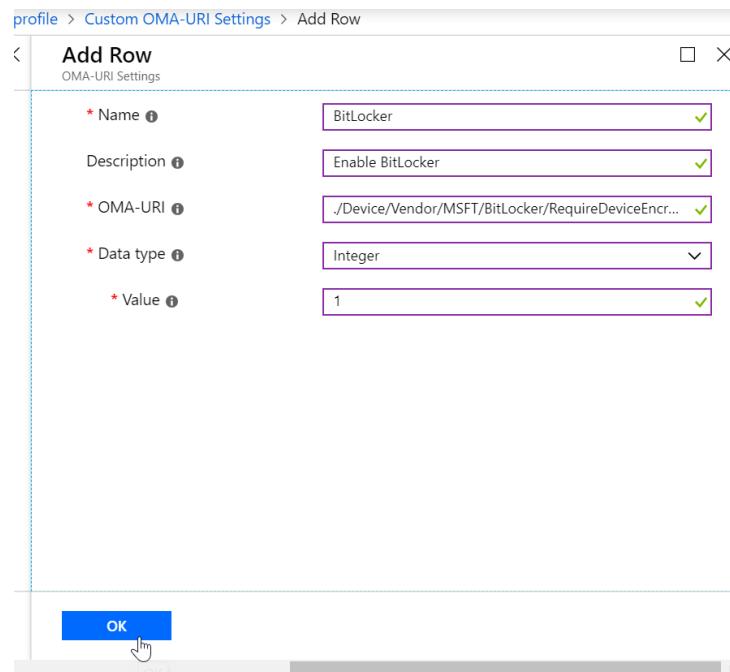


The screenshot shows the 'Create profile' dialog box. It has fields for Name (BitLocker Configuration), Description (Enter a description...), Platform (Windows 10 and later), and Profile type (Custom). Below these are two expandable sections: 'Settings' (Configure) and 'Scope (Tags)' (0 scope(s) selected). At the bottom is a 'Create' button.

c. Click Add



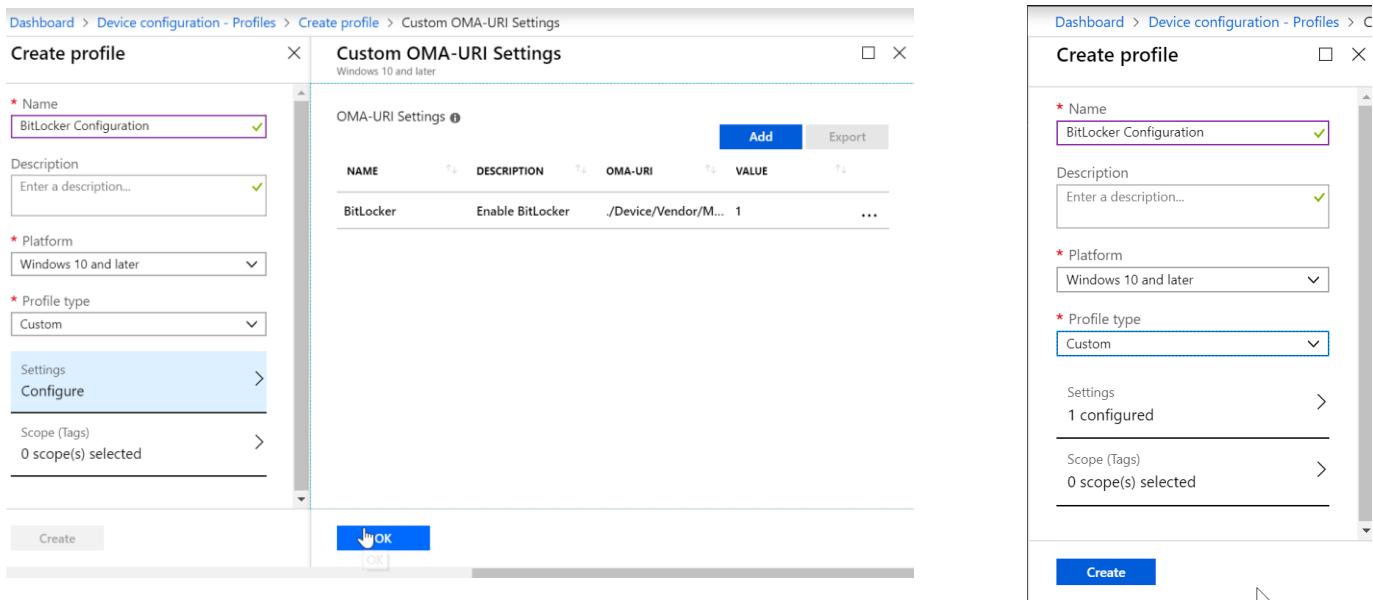
d. Enter the following, including: ./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption



The screenshot shows an 'Add Row' dialog box for 'Custom OMA-URI Settings'. It contains five fields: Name (BitLocker), Description (Enable BitLocker), OMA-URI (./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption), Data type (Integer), and Value (1). The 'Value' field is highlighted with a red box. At the bottom left is a blue 'OK' button.

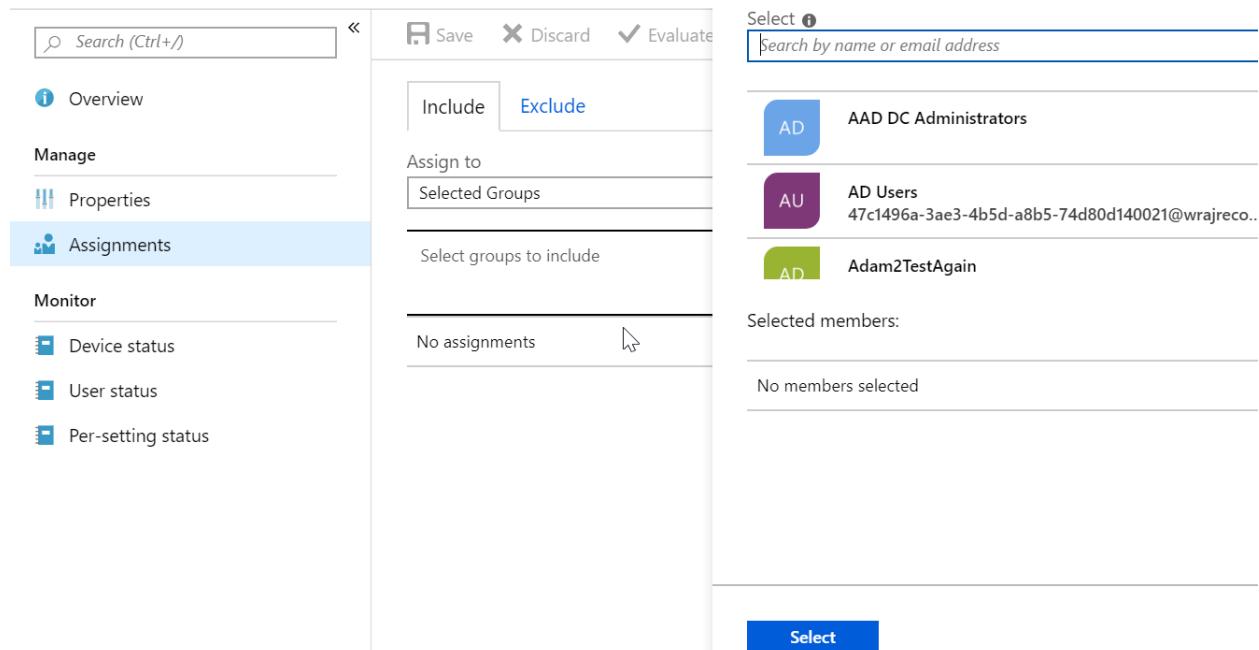
Name	Description	OMA-URI	Data type	Value
BitLocker	Enable BitLocker	./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption	Integer	1

e. Click Ok and Create



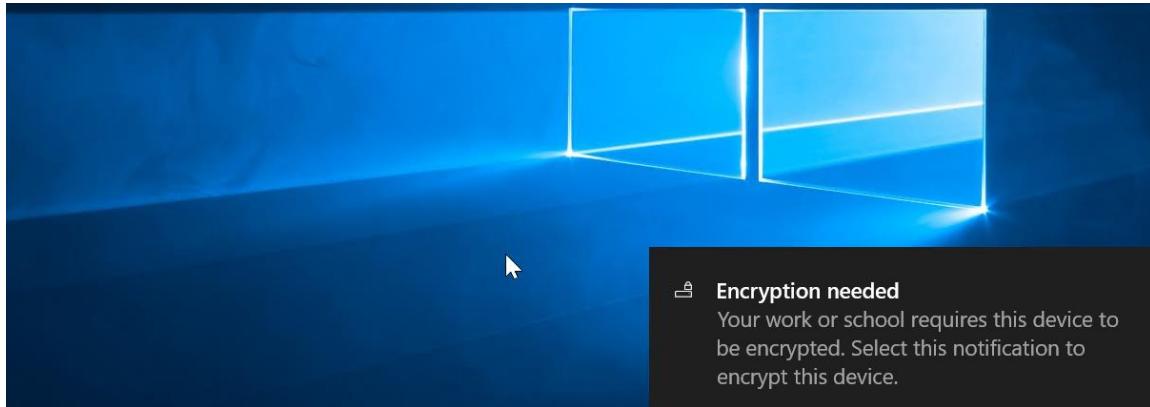
The screenshot shows two overlapping windows. The top window is titled 'Create profile' and has a sub-section titled 'Custom OMA-URI Settings'. It contains fields for Name (BitLocker Configuration), Description (Enter a description...), Platform (Windows 10 and later), Profile type (Custom), and Settings (Configure). The bottom window is also titled 'Create profile' and shows the same configuration details, with the 'OK' button highlighted.

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



The screenshot shows the 'Assignments' section of the profile creation interface. It includes a search bar, Save, Discard, and Evaluate buttons. The 'Include' tab is selected under 'Assign to Selected Groups'. A 'Select' dialog box is open on the right, showing a search bar and a list of groups: 'AAD DC Administrators' (AD icon), 'AD Users' (AU icon) with a long GUID, and 'Adam2TestAgain' (AD icon). Below the list, it says 'Selected members:' and 'No members selected'. A 'Select' button is at the bottom of the dialog.

- 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](#)

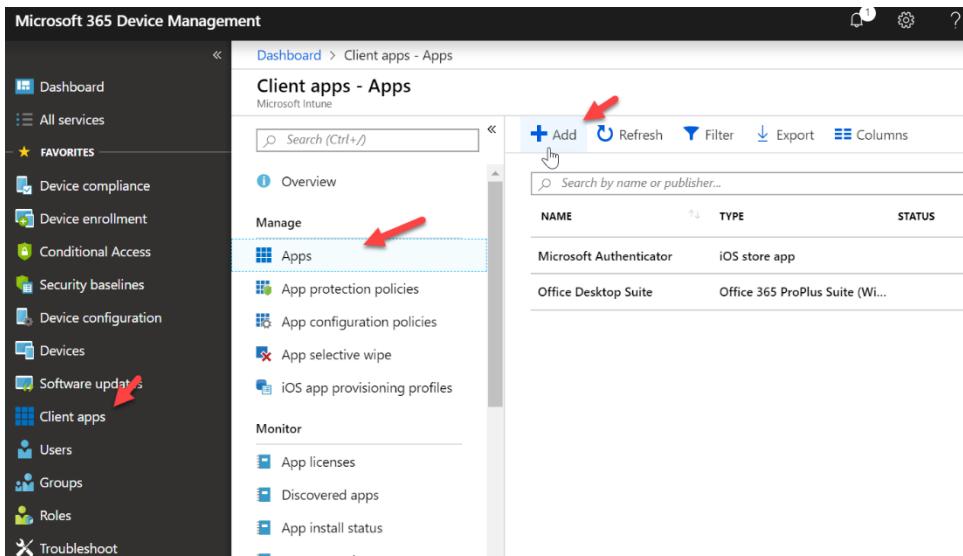
Yes

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:

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



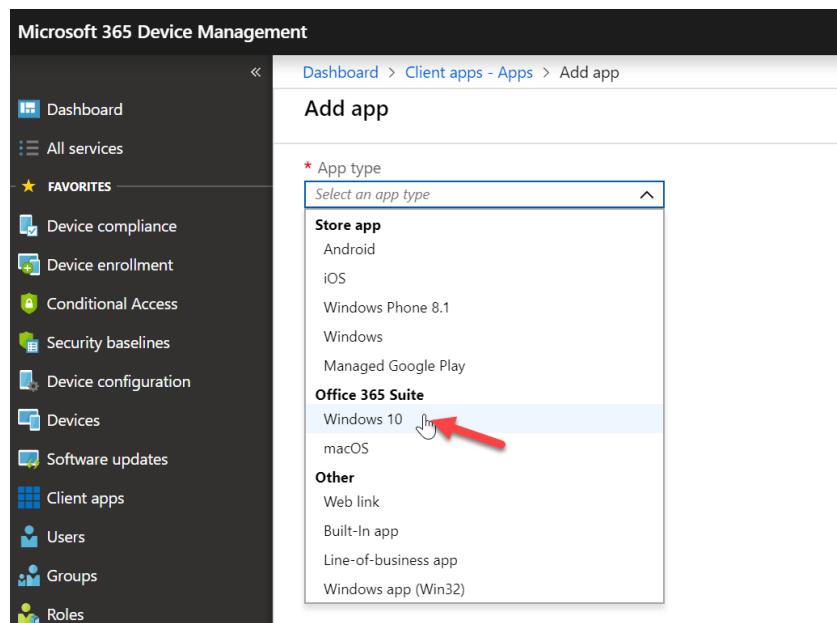
**Microsoft 365 Device Management**

**Client apps - Apps**

**Manage**

NAME	TYPE	STATUS
Microsoft Authenticator	iOS store app	
Office Desktop Suite	Office 365 ProPlus Suite (Wi...)	

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



**Microsoft 365 Device Management**

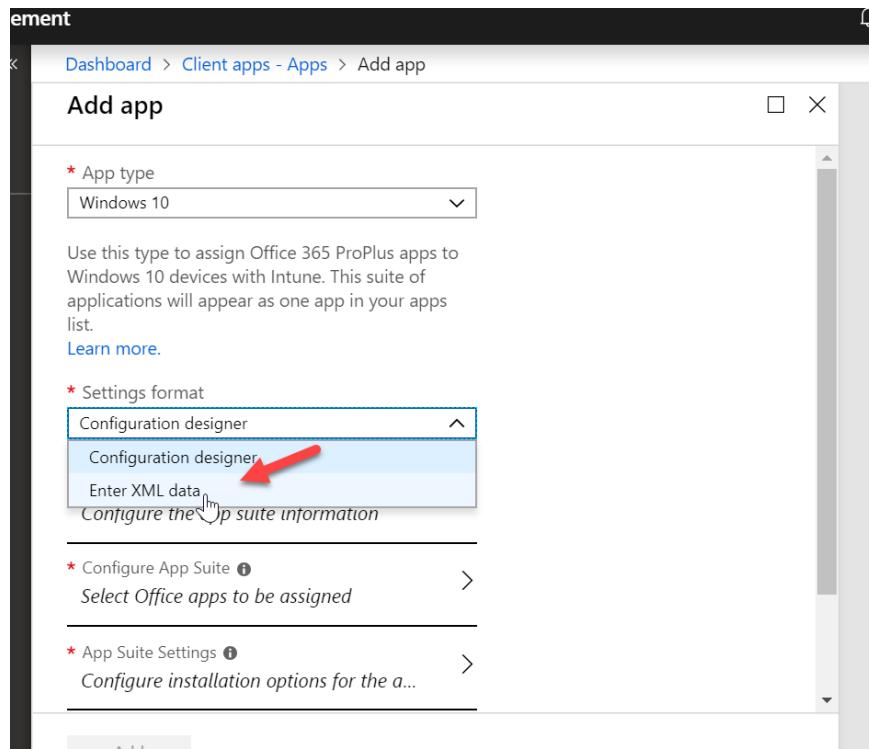
**Add app**

**\* App type**

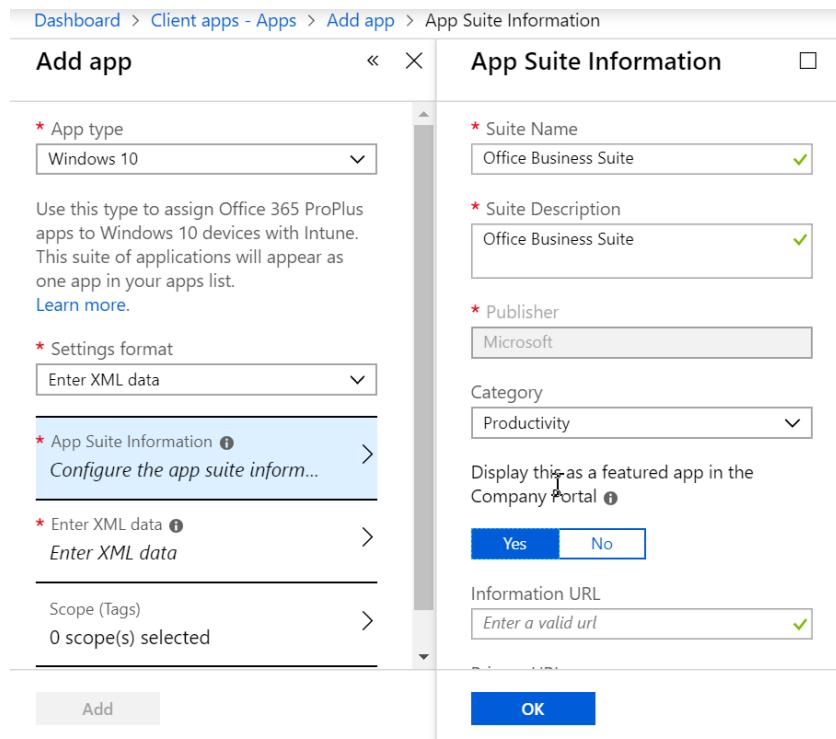
Select an app type

- Store app
  - Android
  - iOS
  - Windows Phone 8.1
  - Windows
  - Managed Google Play
- Office 365 Suite**
  - Windows 10
  - macOS
- Other
  - Web link
  - Built-In app
  - Line-of-business app
  - Windows app (Win32)

- 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:

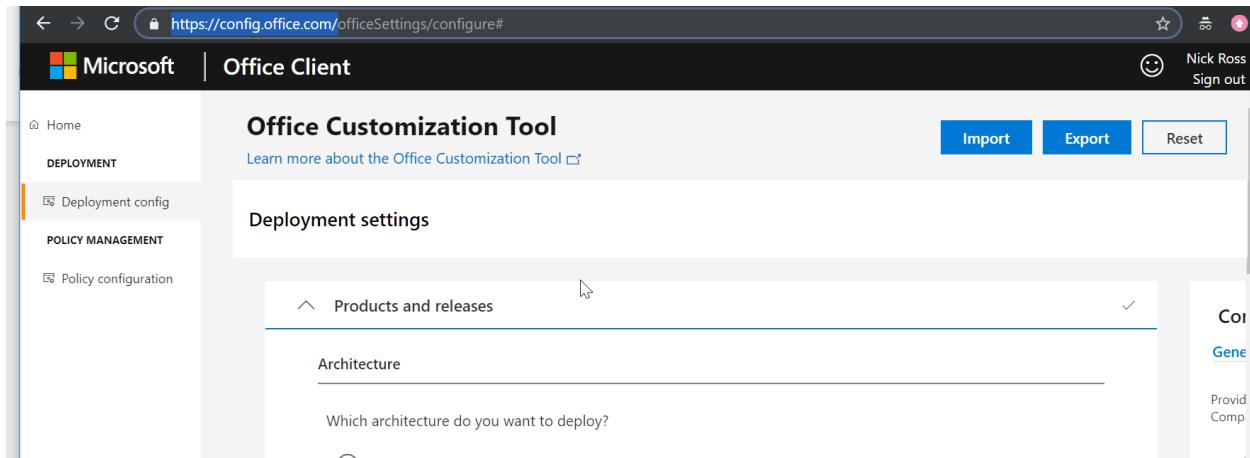


- d. Under **App Suite Information**, configure the following and click ok:



<b>Suite Name</b>	Office Business Suite
<b>Suite Description</b>	Office Business Suite
<b>Publisher</b>	Microsoft
<b>Category</b>	Productivity
<b>Display this as a featured app in the Company Portal</b>	
Yes      No	
<b>Information URL</b>	
Enter a valid url	

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



The screenshot shows the Microsoft Office Client interface for the Office Customization Tool. The URL in the address bar is <https://config.office.com/officeSettings/configure#>. The left sidebar has navigation links: Home, DEPLOYMENT (which is selected), POLICY MANAGEMENT, and Policy configuration. The main content area is titled "Office Customization Tool" with a sub-section "Deployment settings". It features a "Products and releases" dropdown menu with "Architecture" selected. A question "Which architecture do you want to deploy?" is followed by two radio button options: "32-bit" and "64-bit", where "64-bit" is selected.

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

#### Deployment settings

##### Architecture

Which architecture do you want to deploy?

32-bit

64-bit

## 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	
<b>Office 365 Business</b>	
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](#)

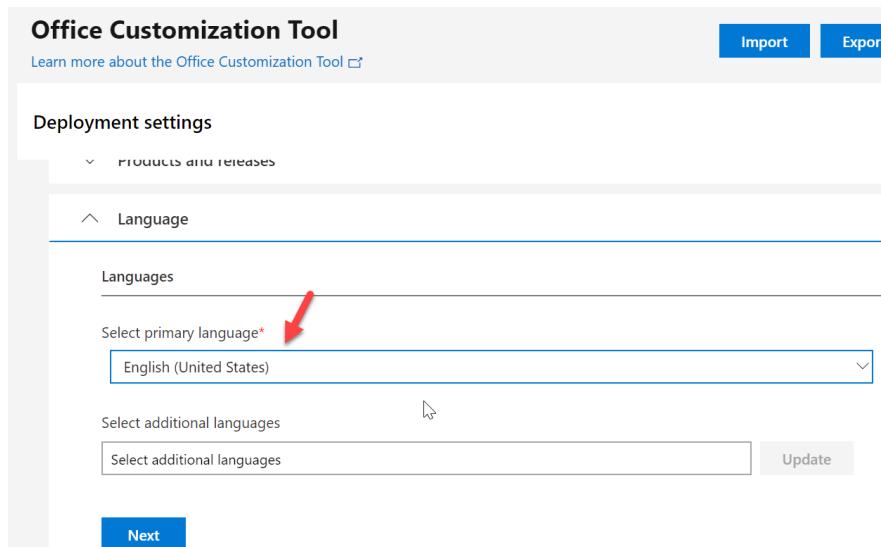
Monthly Channel	▼
-----------------	---

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

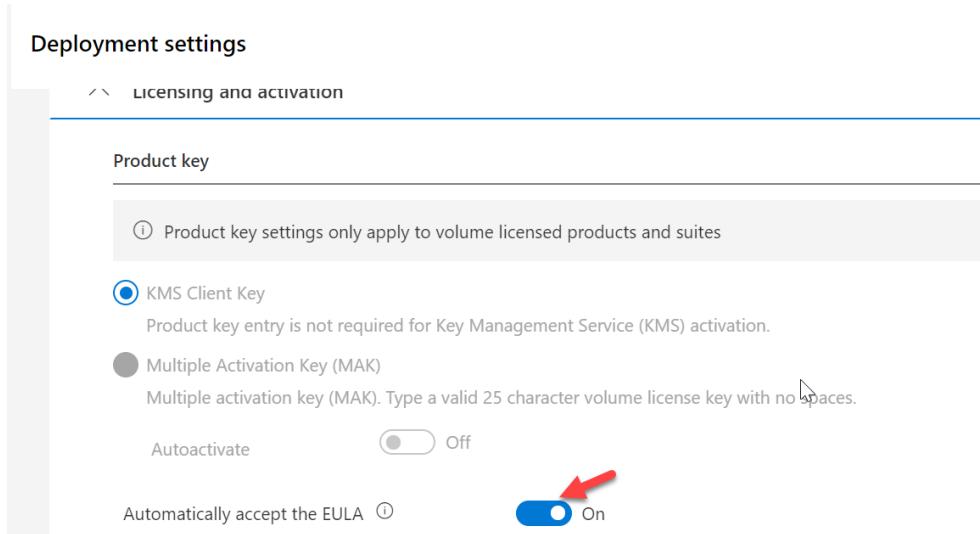
Latest	▼
--------	---

[Next](#)

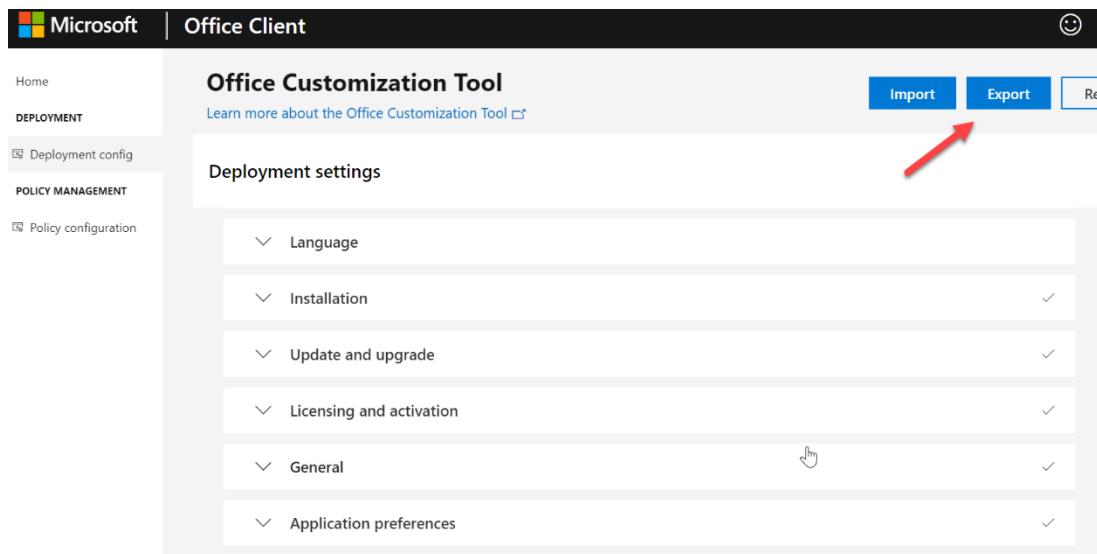
- h. Under **Language** select **English** or your primary language



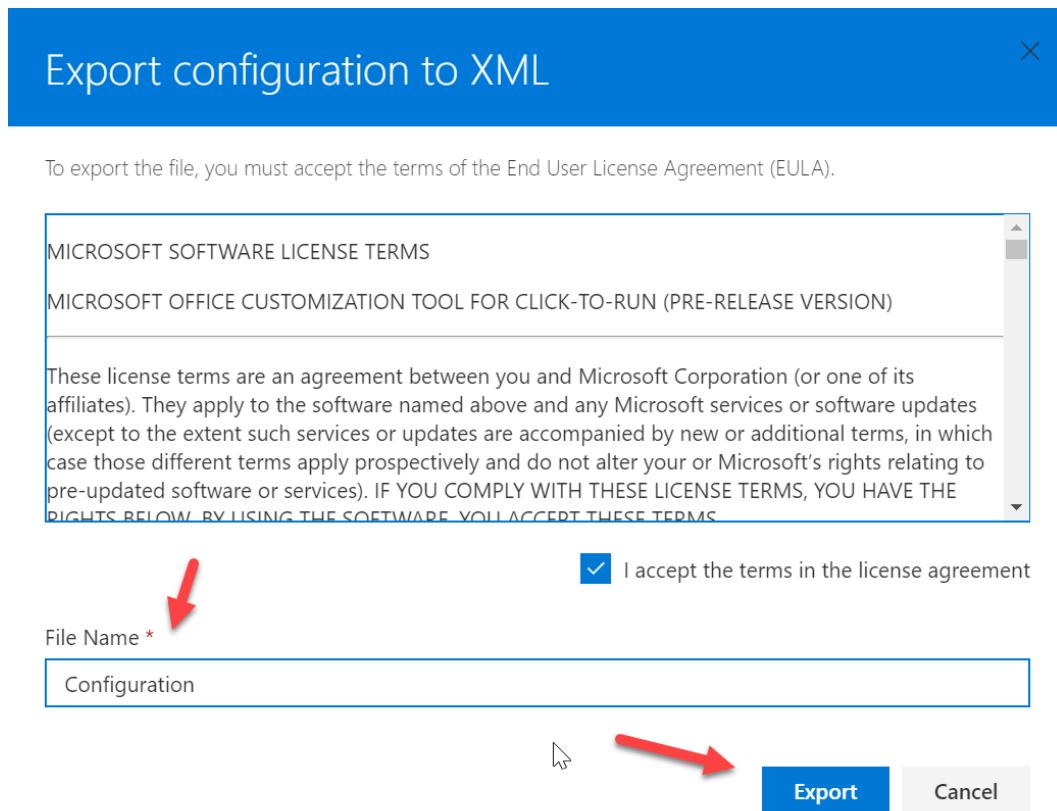
- i. Under the **Licensing and Activation** section turn the **Automatically Accept the EULA** to **On**



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



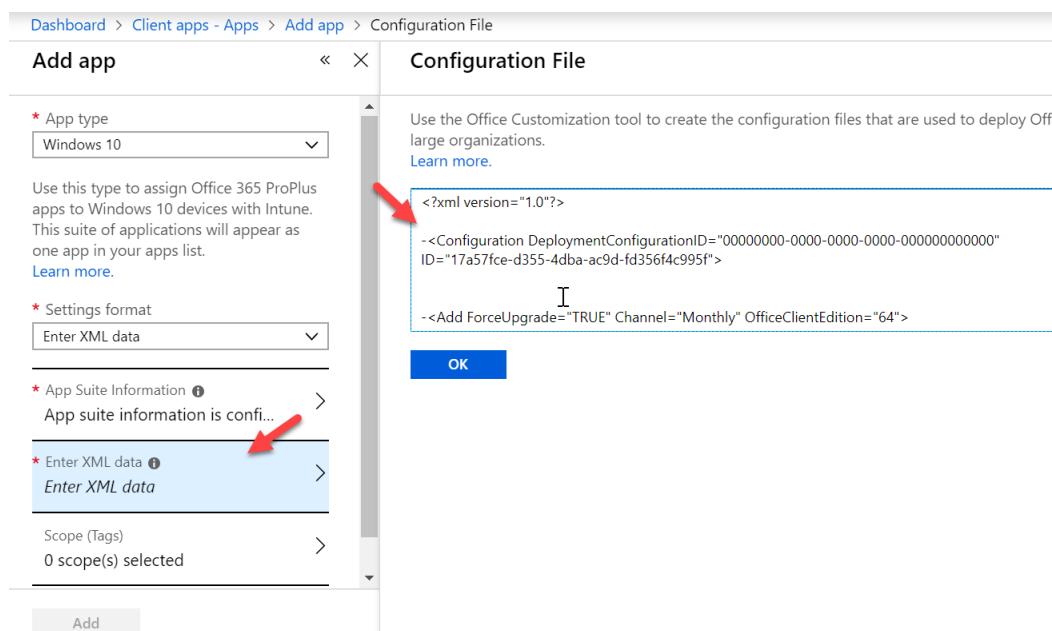
k. Agree to the terms, name your file, and click export



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



The screenshot shows the Microsoft Intune "Add app" configuration page under "Client apps - Apps > Add app > Configuration File". The "App type" is set to "Windows 10". The "Settings format" is set to "Enter XML data". The "Configuration File" section contains the XML code from the previous screenshot. A red arrow points to the "Enter XML data" input field, and another red arrow points to the "OK" button.

n. Click **Add**

Client

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**

Office Desktop Suite - Assignments

Client Apps

Search (Ctrl+ /)

Overview

Manage

Properties

**Assignments**

Monitor

Device install status

User install status

Add group

Save Discard

Add group

GROUP ASSIGNMENT MODE

AVAILABLE FOR ENROLLED DEVICES

No assignments, select 'Add group' to add a ...

REQUIRED

Nicks ... Required Included ...

UNINSTALL

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

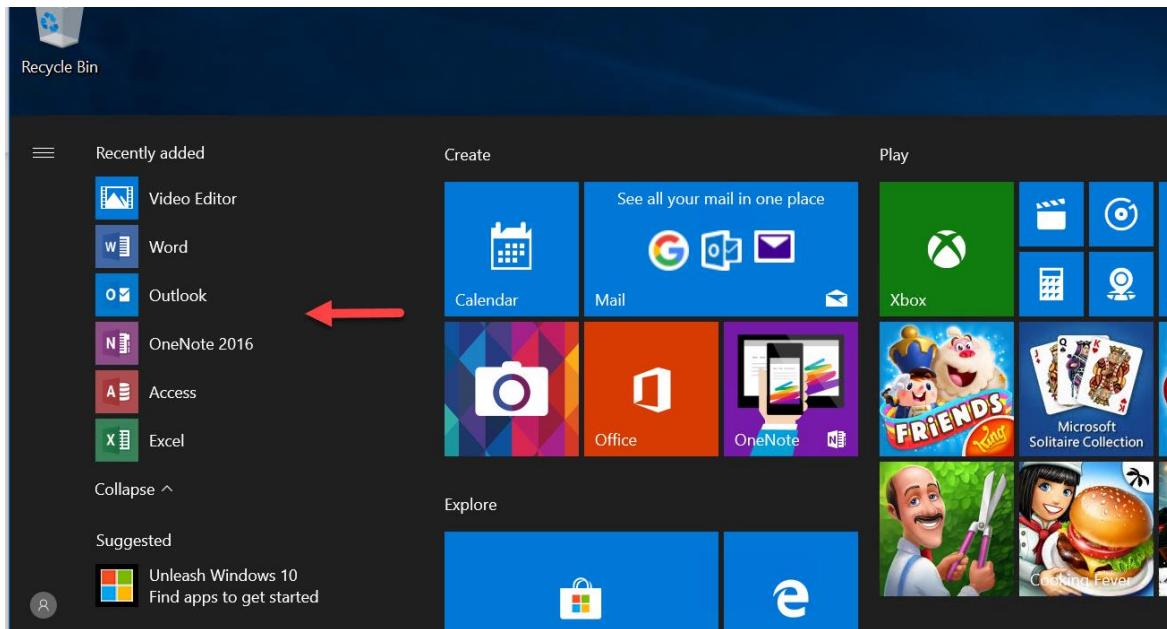
**Required**

Uninstall

No groups selected

Excluded Groups

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

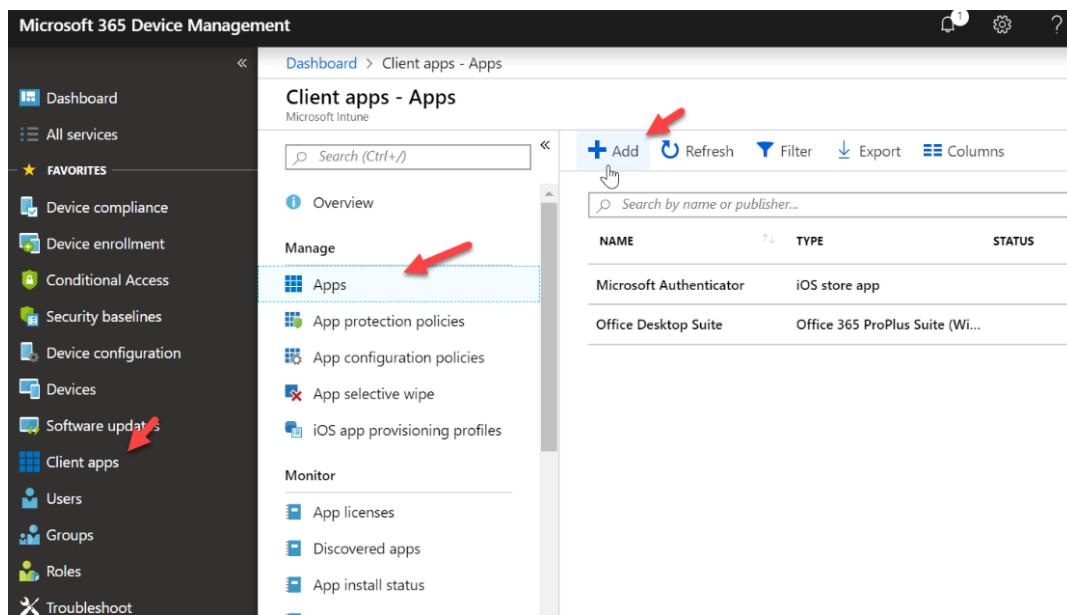


## Adding the Microsoft Authenticator App

The Microsoft Authenticator app is widely used 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.

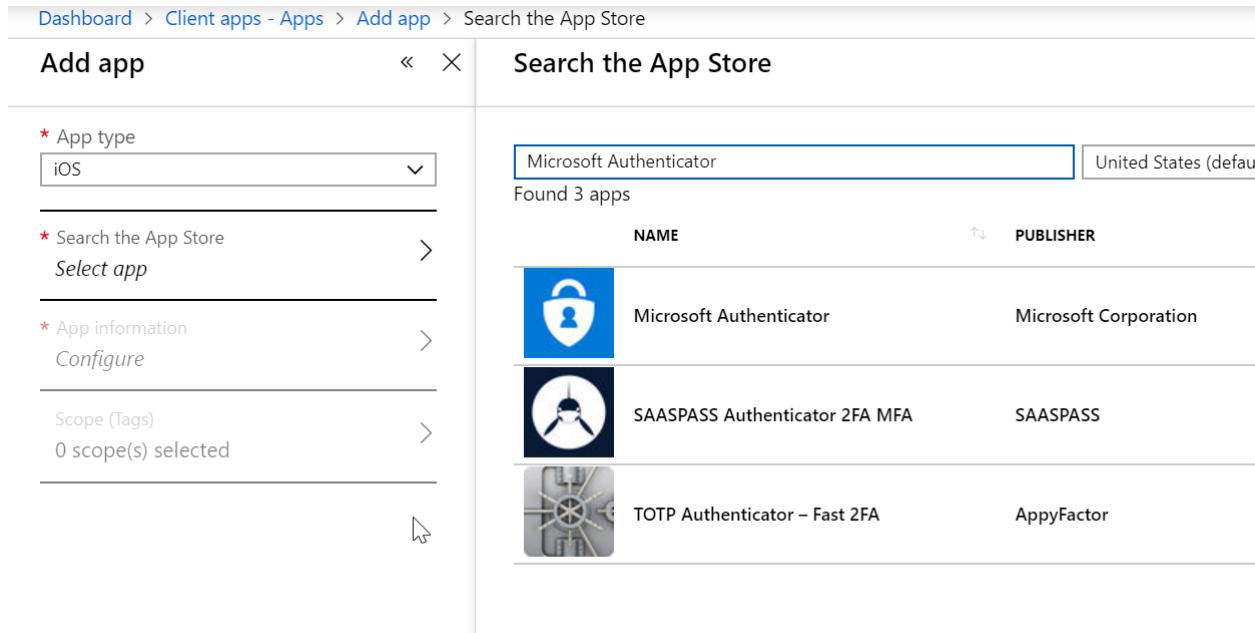
iOS

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



NAME	TYPE	STATUS
Microsoft Authenticator	iOS store app	
Office Desktop Suite	Office 365 ProPlus Suite (Wi...)	

- 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:

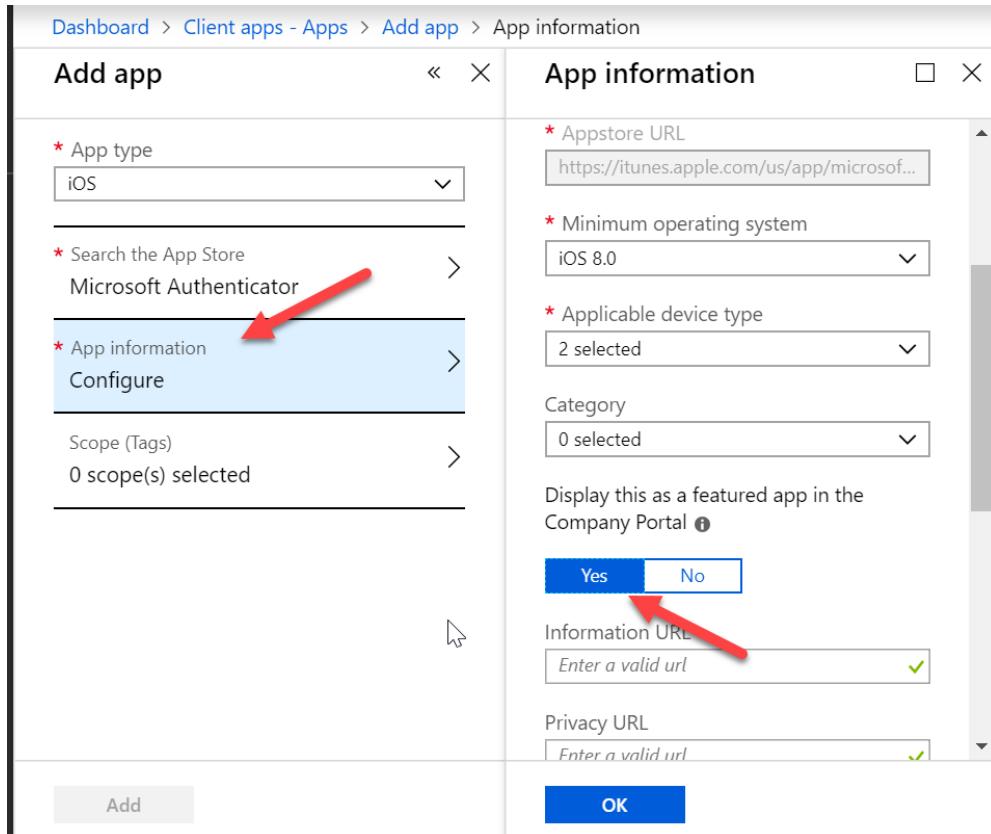


The screenshot shows the 'Add app' wizard with the following steps completed:

- Step 1: Set App type to iOS.
- Step 2: Clicked 'Select app' under 'Search the App Store'.
- Step 3: In the search bar, typed 'Microsoft Authenticator'. The search results show three apps:
 

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

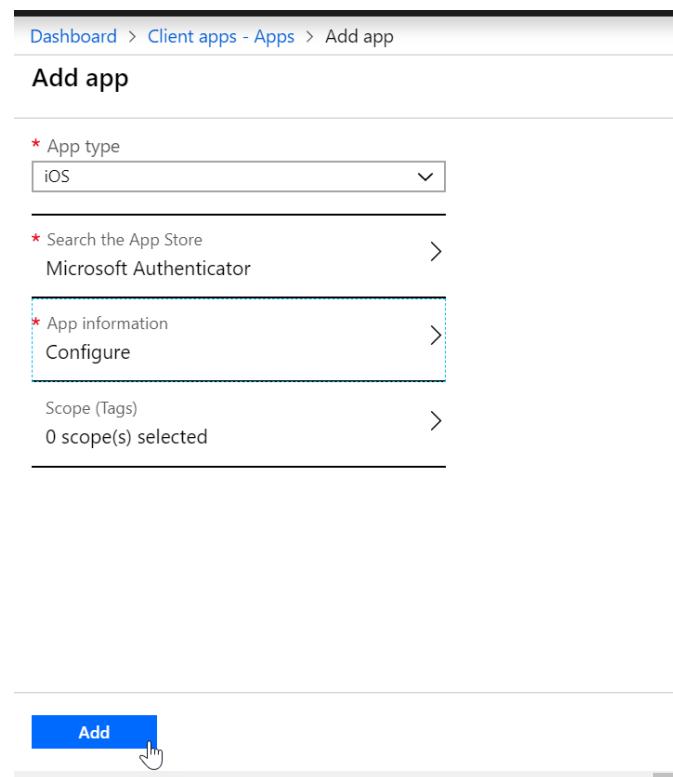
- c. Select the app and click **Configure** under App Information. Say **Yes** for displaying app in Company Portal. Leave all other settings defaulted:



The screenshot shows the 'App information' configuration screen for the Microsoft Authenticator app. The 'Configure' link under 'App information' is highlighted with a red arrow. The 'Display this as a featured app in the Company Portal' section has a 'Yes' button highlighted with a red arrow. Other fields include:

- Appstore URL: https://itunes.apple.com/us/app/microsoft-authenticator/id982339517?mt=8
- Minimum operating system: iOS 8.0
- Applicable device type: 2 selected
- Category: 0 selected
- Information URL: Enter a valid url
- Privacy URL: Enter a valid url

d. Click Add



Dashboard > Client apps - Apps > Add app

### Add app

\* App type  
iOS

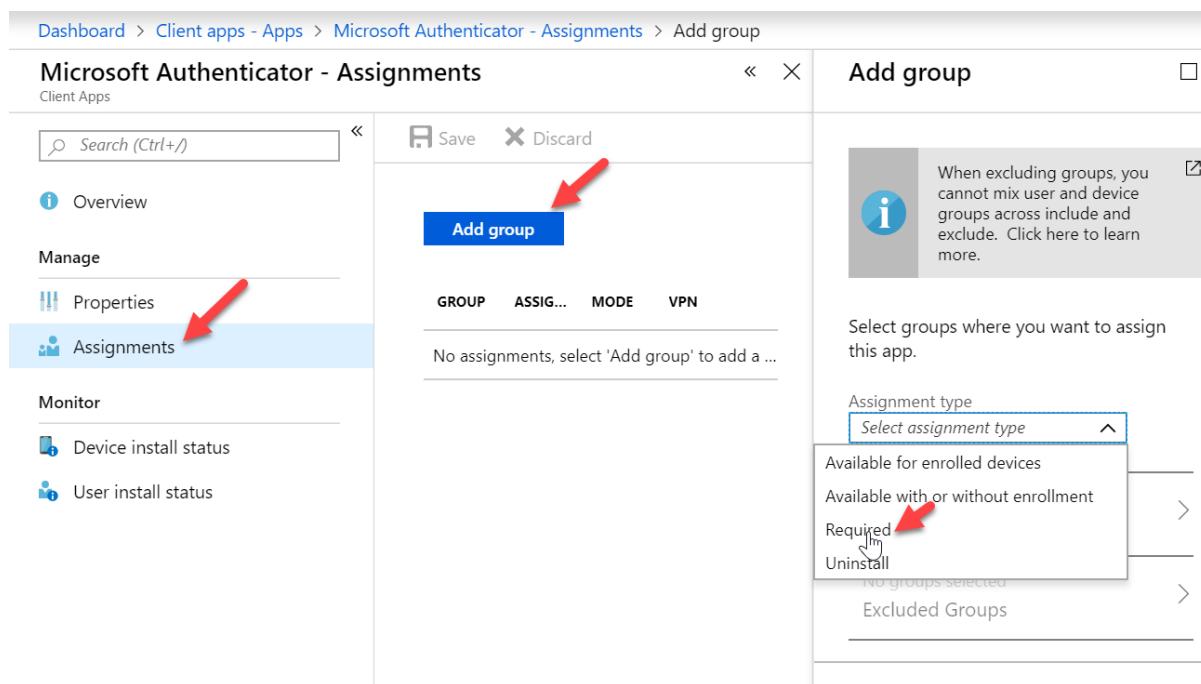
\* Search the App Store  
Microsoft Authenticator

\* App information  
Configure

Scope (Tags)  
0 scope(s) selected

**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** (highlighted with a red arrow)

Monitor

Device install status

User install status

Save Discard

Add group

GROUP ASSIG... MODE VPN

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 (highlighted with a red arrow)

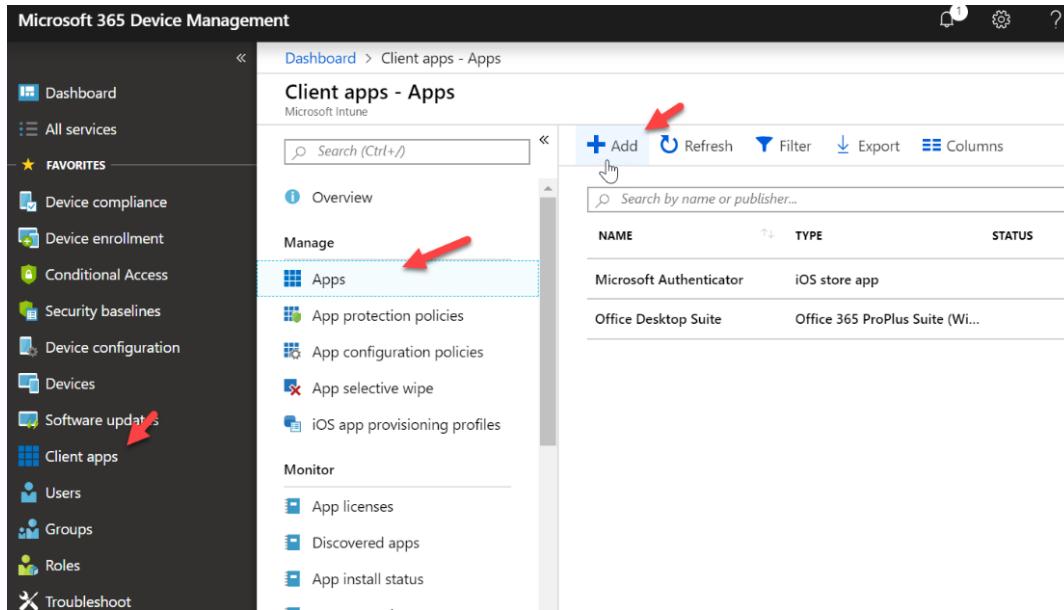
Uninstall

No groups selected

Excluded Groups

## Android

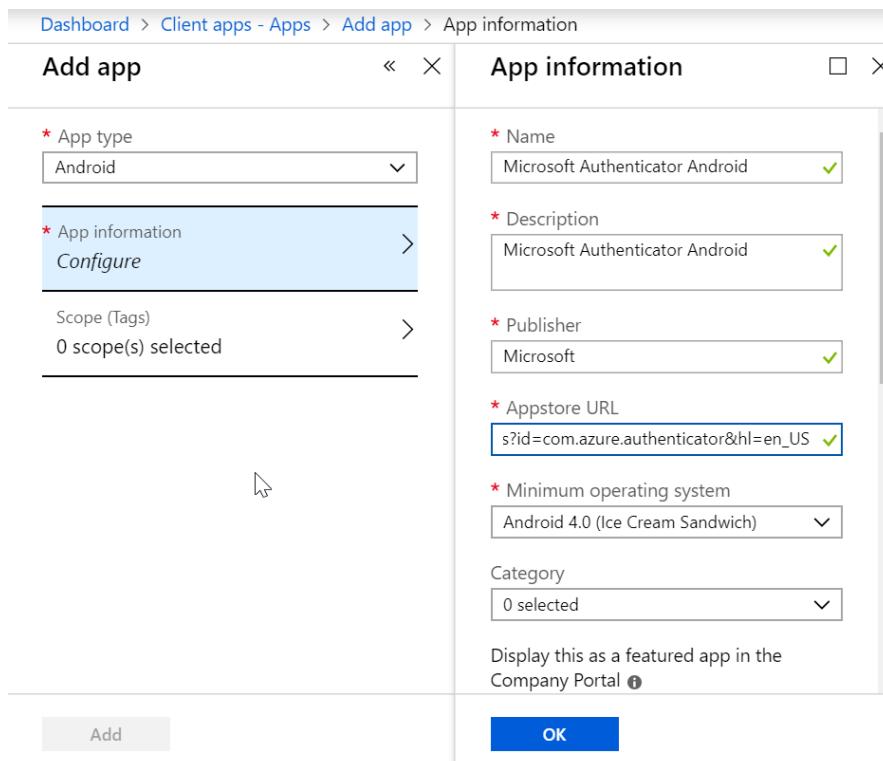
- a. In the Device Management Admin center>Client Apps>Apps>Add



The screenshot shows the Microsoft 365 Device Management Admin center interface. The left sidebar includes 'Dashboard', 'All services', 'Favorites' (with 'Client apps' selected), 'Device compliance', 'Device enrollment', 'Conditional Access', 'Security baselines', 'Device configuration', 'Devices', 'Software updates' (highlighted with a red arrow), 'Client apps' (selected and highlighted with a red arrow), 'Users', 'Groups', 'Roles', and 'Troubleshoot'. The main area is titled 'Client apps - Apps' and shows a table with two rows: 'Microsoft Authenticator' (iOS store app) and 'Office Desktop Suite' (Office 365 ProPlus Suite). The top right features a toolbar with 'Add' (highlighted with a red arrow), 'Refresh', 'Filter', 'Export', and 'Columns'.

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

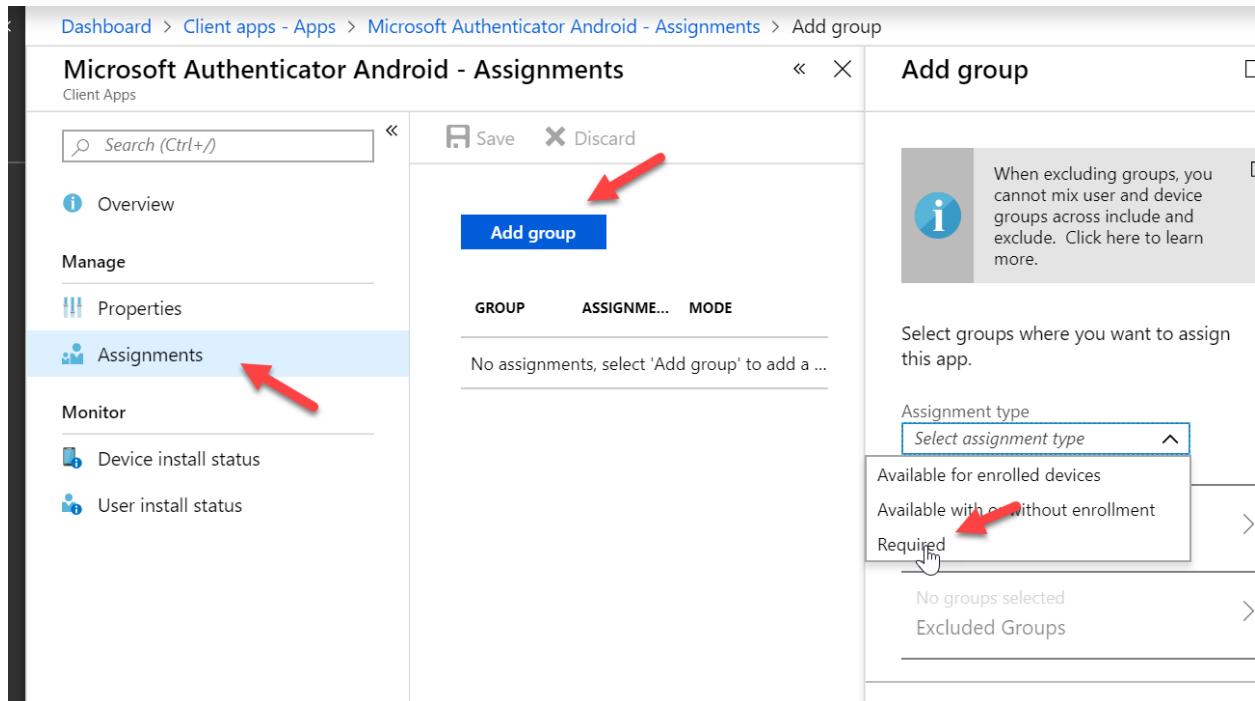
[https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en\\_US](https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US)



The screenshot shows the 'Add app' and 'App information' forms. The 'Add app' form on the left has 'App type' set to 'Android'. The 'App information' form on the right has the following fields filled: 'Name' (Microsoft Authenticator Android), 'Description' (Microsoft Authenticator Android), 'Publisher' (Microsoft), 'Appstore URL' ([https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en\\_US](https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US)), 'Minimum operating system' (Android 4.0 (Ice Cream Sandwich)), and 'Category' (0 selected). A note at the bottom says 'Display this as a featured app in the Company Portal'.

c. Click **Add**

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

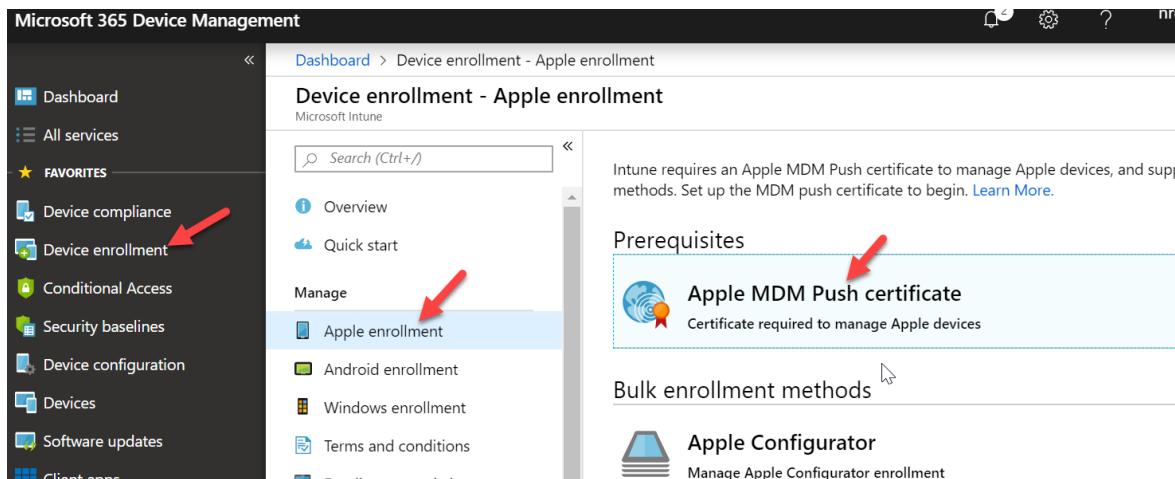


The screenshot shows the 'Microsoft Authenticator Android - Assignments' page in the Azure portal. On the left, there's a navigation menu with 'Overview', 'Properties', 'Assignments' (which is selected and highlighted in blue), 'Monitor', 'Device install status', and 'User install status'. In the main content area, there's a 'Save' and 'Discard' button at the top. Below it is a large blue 'Add group' button with a red arrow pointing to it. To the right of the 'Add group' button is a note: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.' Further down, there's a section titled 'Assignment type' with a dropdown menu set to 'Select assignment type'. The dropdown menu has three options: 'Available for enrolled devices', 'Available with or without enrollment', and 'Required'. A red arrow points to the 'Required' option. At the bottom of the page, there are sections for 'No groups selected' and '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.

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



The screenshot shows the Microsoft 365 Device Management interface. The left sidebar has a 'FAVORITES' section with 'Device compliance' checked, 'Device enrollment' highlighted with a red arrow, and other options like 'Conditional Access', 'Security baselines', etc. The main content area is titled 'Device enrollment - Apple enrollment'. It shows a 'Prerequisites' section with 'Apple MDM Push certificate' highlighted with a red arrow. Below it is a 'Bulk enrollment methods' section with 'Apple Configurator'.

- 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

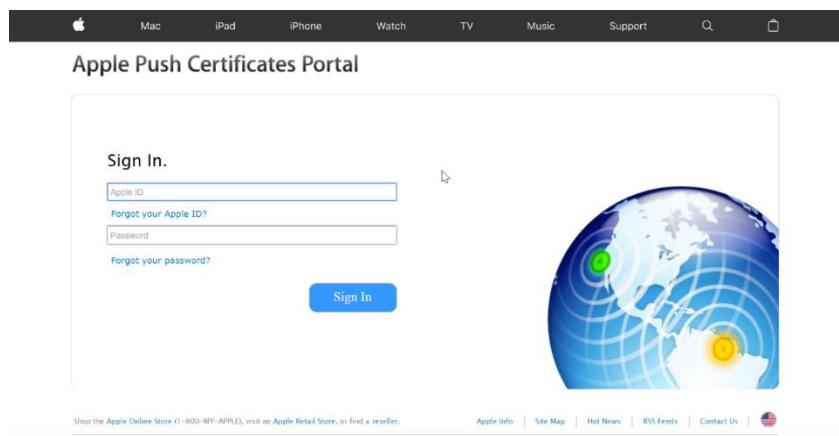
HIPAABusinessAssociateAgr(WW)(ENG)(Februar...	9/30/2018 1:54 PM	Microsoft Word Doc...	51 KB	
IMG_1436	10/28/2018 8:18 PM	JPG File	53 KB	
IntuneCSR.csr	11/2/2018 12:43 PM	CSR File	10 KB	
invoice-48363	10/24/2018 4:32 PM	PDF File	59 KB	
invoice-51422	10/4/2018 1:19 PM	PDF File	42 KB	
invoice-51913	10/4/2018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

**Configure MDM Push Certificate**

**Steps:**

1. I grant Microsoft permission to send both user and device information to Apple. [More information.](#)  \* I agree. 
2. Download the Intune certificate signing request required to create an Apple MDM push certificate. [Download your CSR](#) 
3. Create an Apple MDM push certificate. [More information.](#) [Create your MDM push Certificate](#) 
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)



- 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

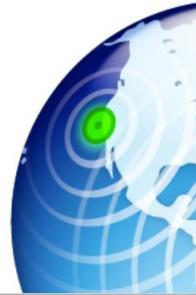
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

Choose File IntuneCSR.csr 





## Apple Push Certificates Portal

nross@wrajrecords.com [Sign out](#)

### 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

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



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  
nross@wrrajrecords.com 

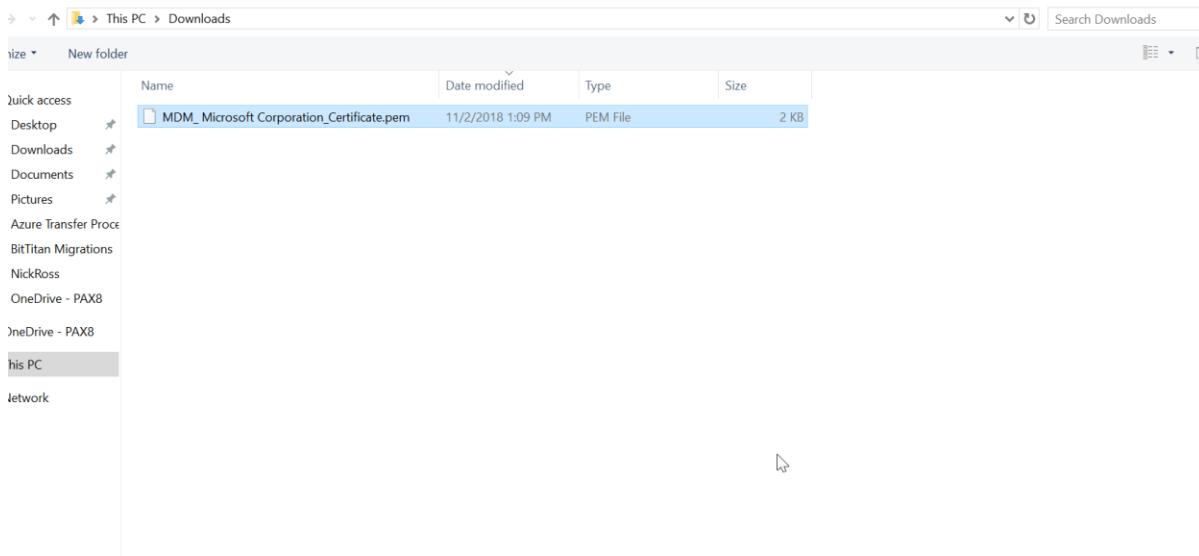
---

5. Browse to your Apple MDM push certificate to upload

\* Apple MDM push certificate  
"MDM\_Microsoft Corporation\_Certificate.pem" 

---

**Upload**



f. You will see the status as active

Configure MDM Push Certificate

Delete	
Status:	<input checked="" type="checkbox"/> 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.

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

Microsoft 365 Device Management

Dashboard > Device enrollment - Android enrollment

Device enrollment - Android enrollment

By default, all Android devices, including those that support Android Enterprise, can be managed using conventional Android devices. To enable management of the Work Profile and other functionality, configure Managed Google Play below. [Learn More](#).

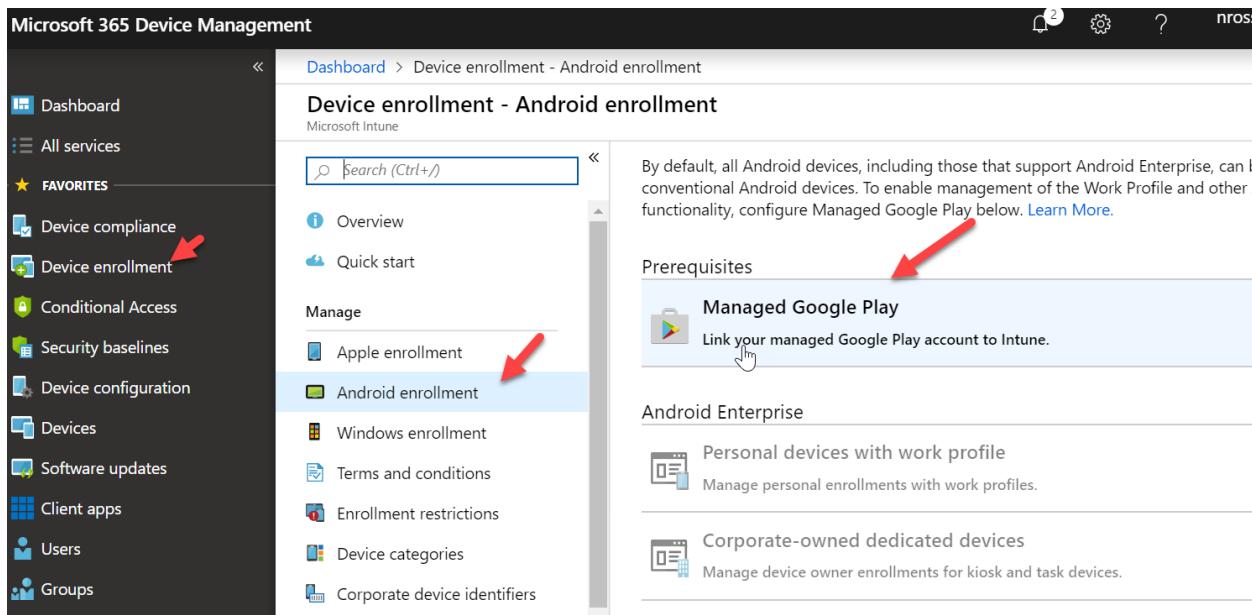
Prerequisites

**Managed Google Play**

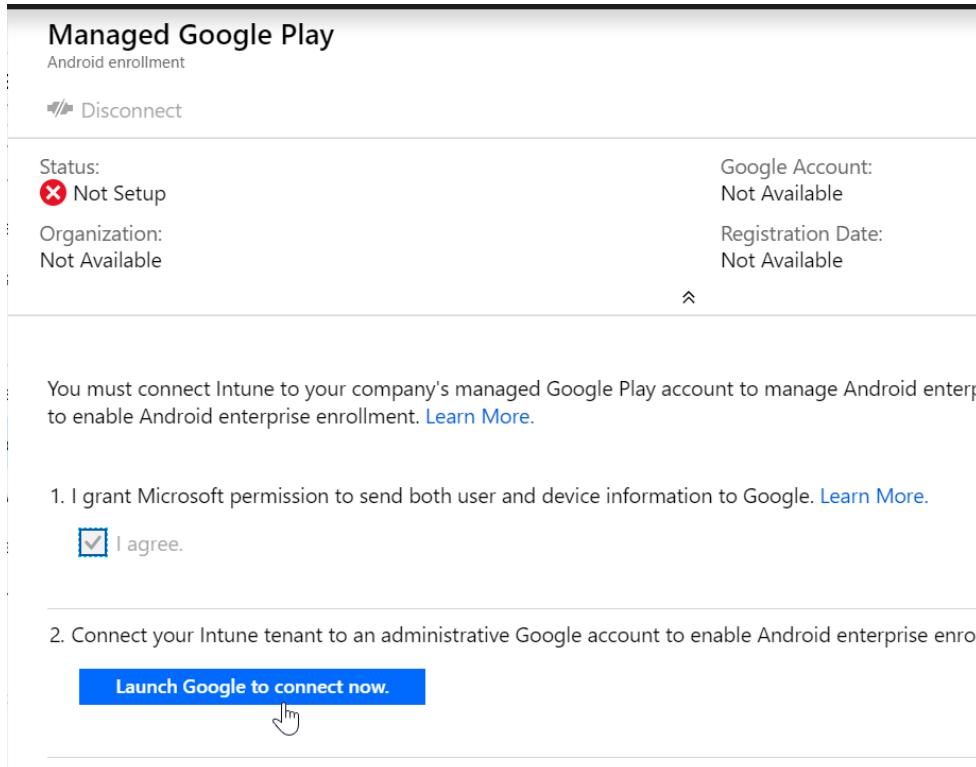
Link your managed Google Play account to Intune.

Android Enterprise

- Personal devices with work profile
- Corporate-owned dedicated devices



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



**Managed Google Play**  
Android enrollment

 Disconnect

Status:  Not Setup	Google Account: Not Available
Organization: Not Available	Registration Date: Not Available

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:



- d. Enter your Business Name and click Next

# Business name

We need some details about your business

Business name

Your answer

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:

Phone

---

EU Representative

Name

---

Email

---

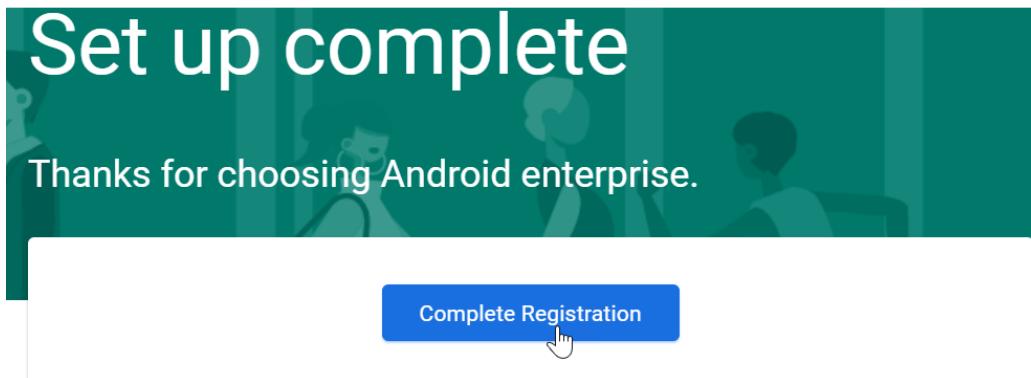
Phone

---

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.

### Managed Google Play

Android enrollment

 Disconnect

Status:	 Setup
Organization:	TMinus365

 Managed Google Play successfully config  
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.

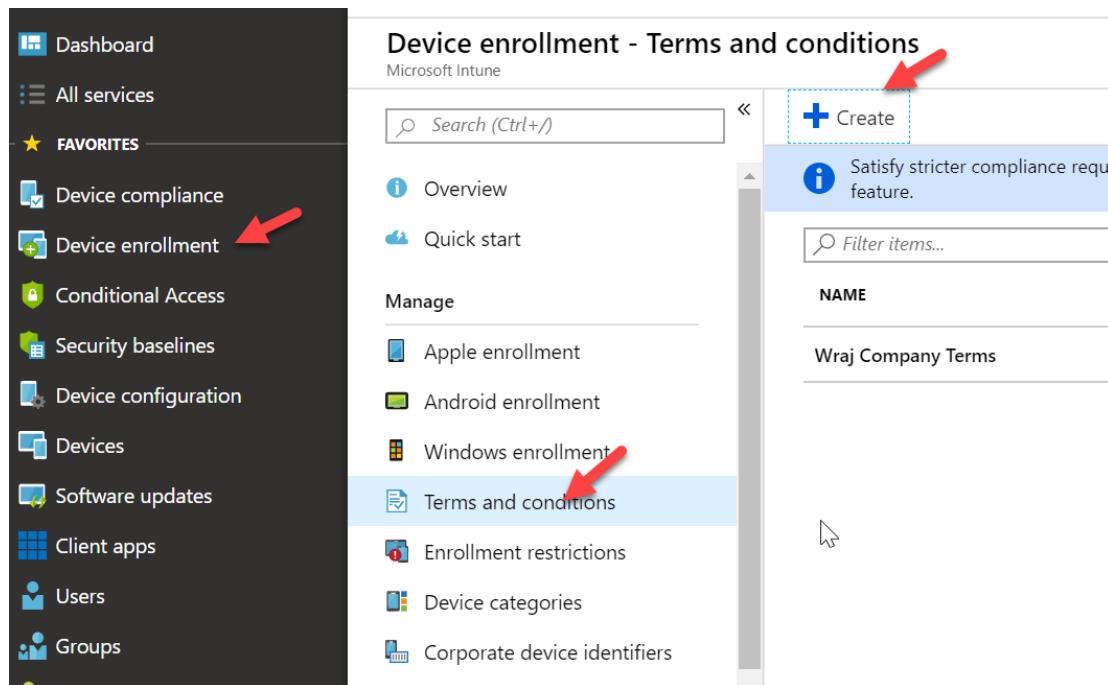
[Launch Google to connect now.](#)

## 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:

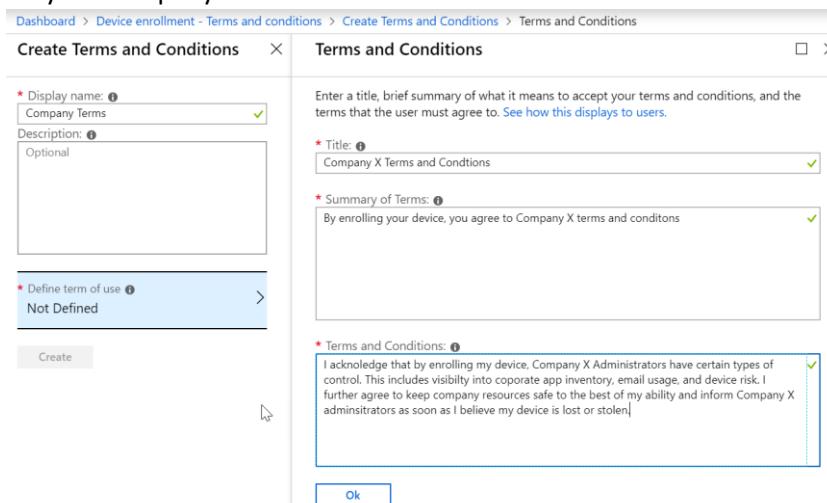
- enroll devices
- Access resources like company apps and email.

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



The screenshot shows the Microsoft Intune Device Enrollment - Terms and Conditions interface. On the left, there's a sidebar with various navigation options. The 'Device enrollment' option is highlighted with a red arrow. The main content area has a heading 'Device enrollment - Terms and conditions'. Below it, there's a 'Create' button with a plus sign, also highlighted with a red arrow. A tooltip for the 'Create' button says 'Satisfy stricter compliance requirements'. The 'NAME' field contains 'Wraj Company Terms'. The 'Manage' section includes links for Apple enrollment, Android enrollment, Windows enrollment, and Terms and conditions, which is also highlighted with a red arrow. Other links in the 'Manage' section include Enrollment restrictions, Device categories, and Corporate device identifiers.

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



The screenshot shows two adjacent tabs: 'Create Terms and Conditions' on the left and 'Terms and Conditions' on the right.

**Create Terms and Conditions Tab:**

- \* Display name: Company Terms
- Description: Optional
- \* Define term of use: Not Defined
- Buttons: Create, >

**Terms and Conditions Tab:**

- Enter a title, brief summary of what it means to accept your terms and conditions, and the terms that the user must agree to. See how this displays to users.
- \* Title: Company X Terms and Conditions
- \* Summary of Terms: By enrolling your device, you agree to Company X terms and conditons
- \* 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.
- Buttons: ok

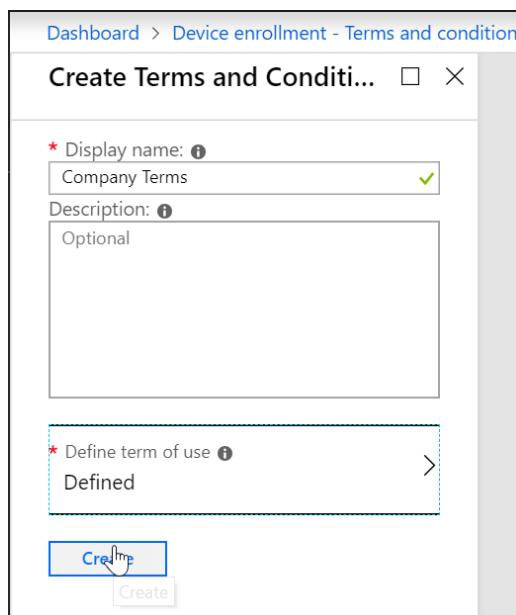
**Ex. Summary of Terms**

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****

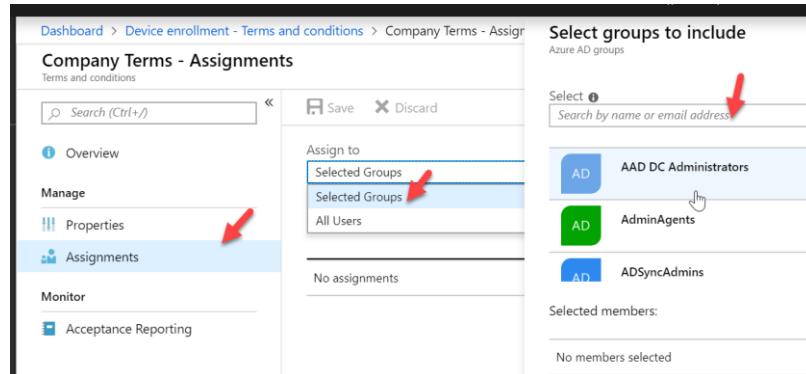


The screenshot shows the 'Create Terms and Conditions' tab with the following fields:

- \* Display name: Company Terms
- Description: Optional
- \* Define term of use: Defined

At the bottom, there are two buttons: a blue 'Create' button with a hand cursor icon, and a grey 'Create' button.

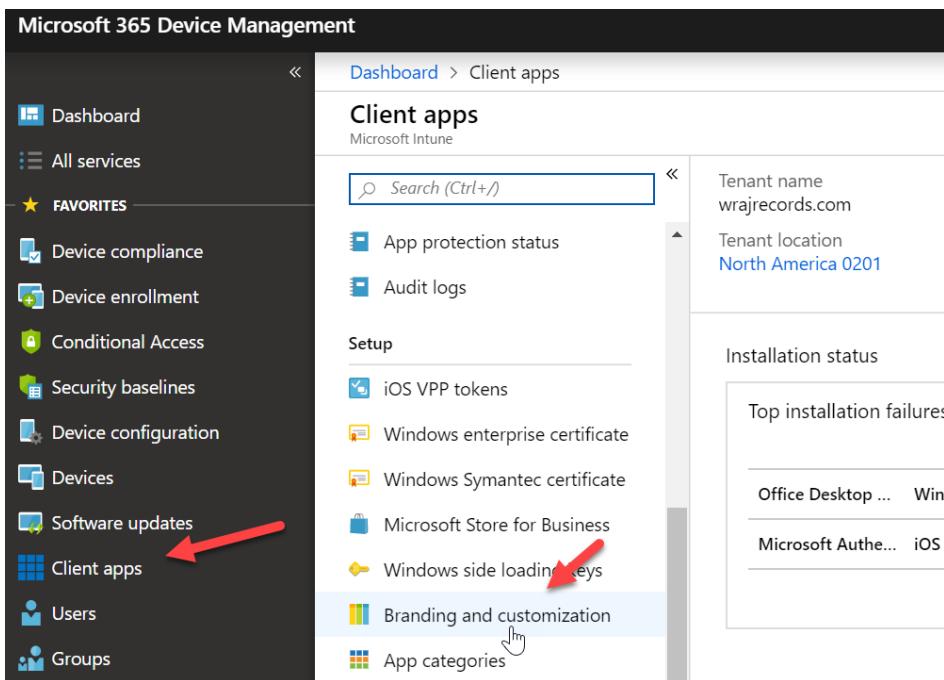
- d. Click on the Policy after creation and click **Assignments** to assign the Terms to All Users or a select group:



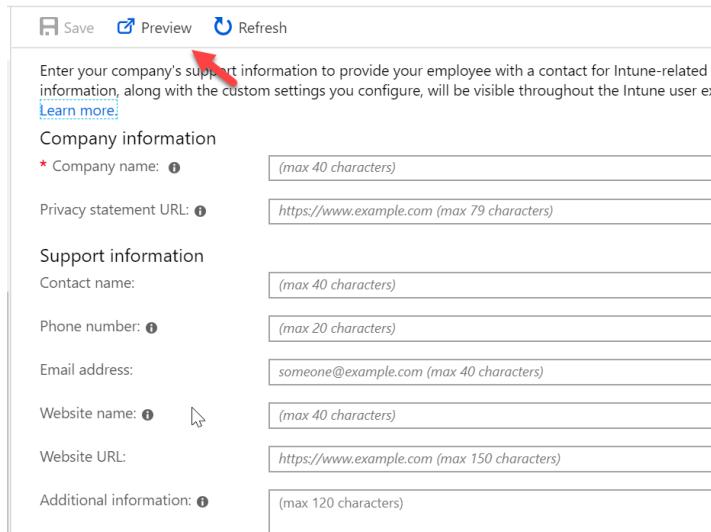
## Add Company Branding

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 c  
[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  Blue

Display



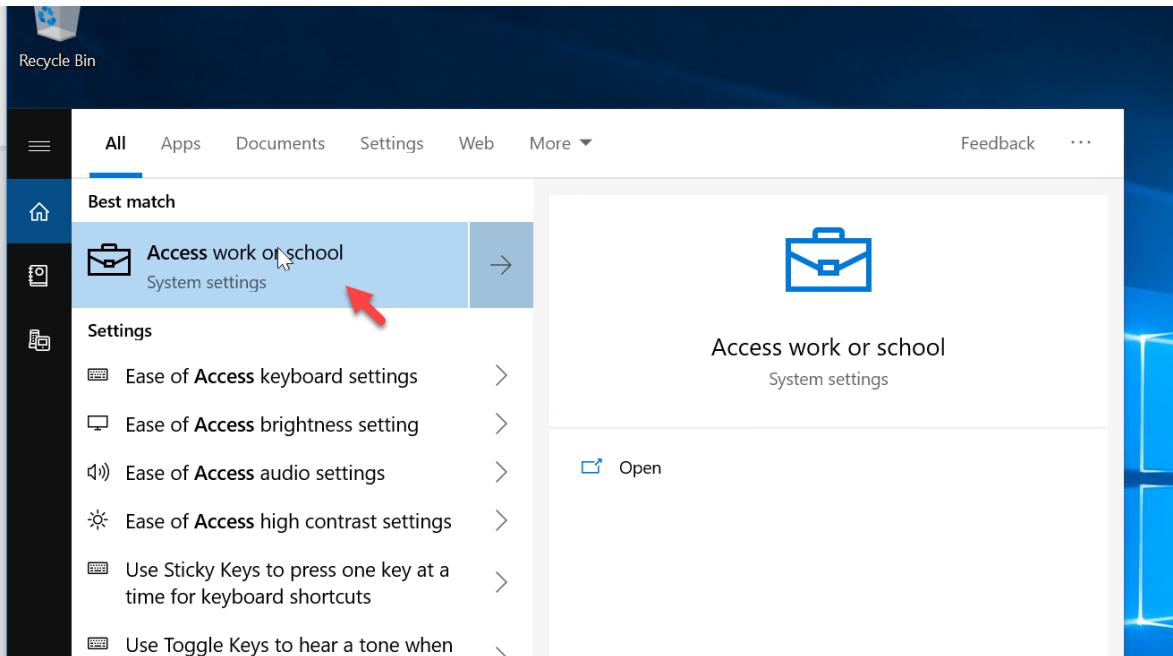
Text color: White

^ Logo to use on white or light background 

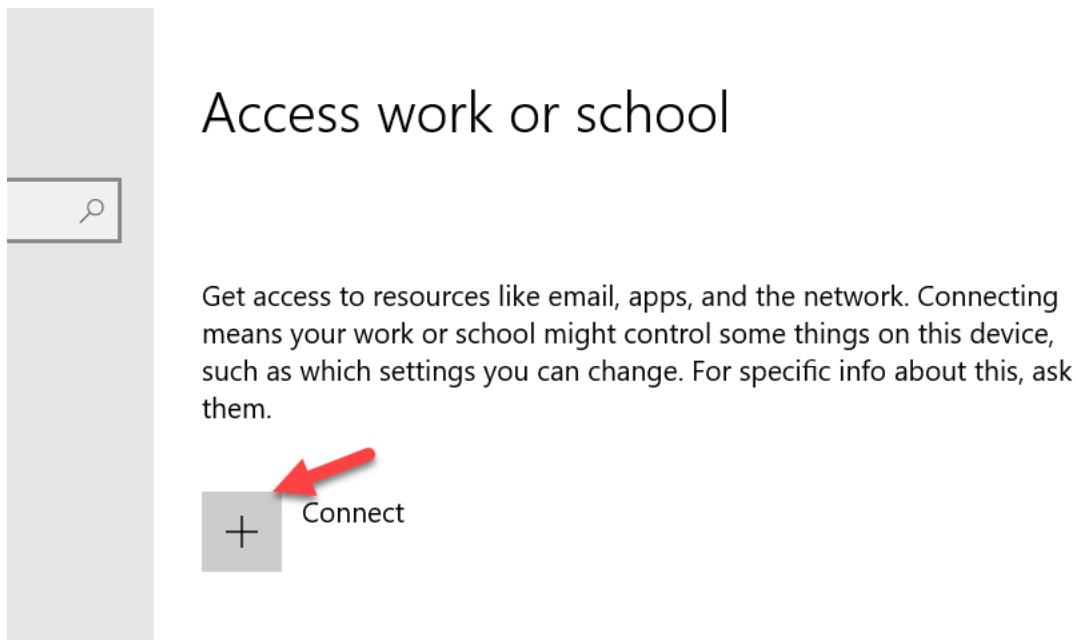
Upload your logo

## 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

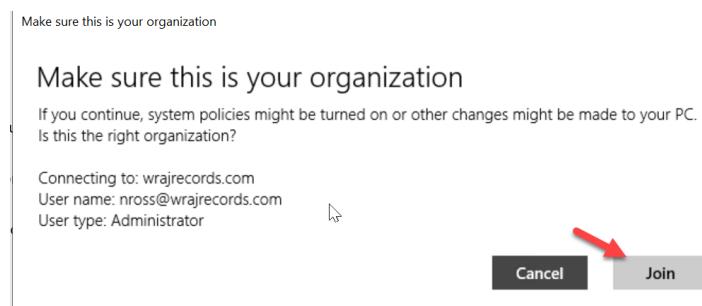
Which account should I use?

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

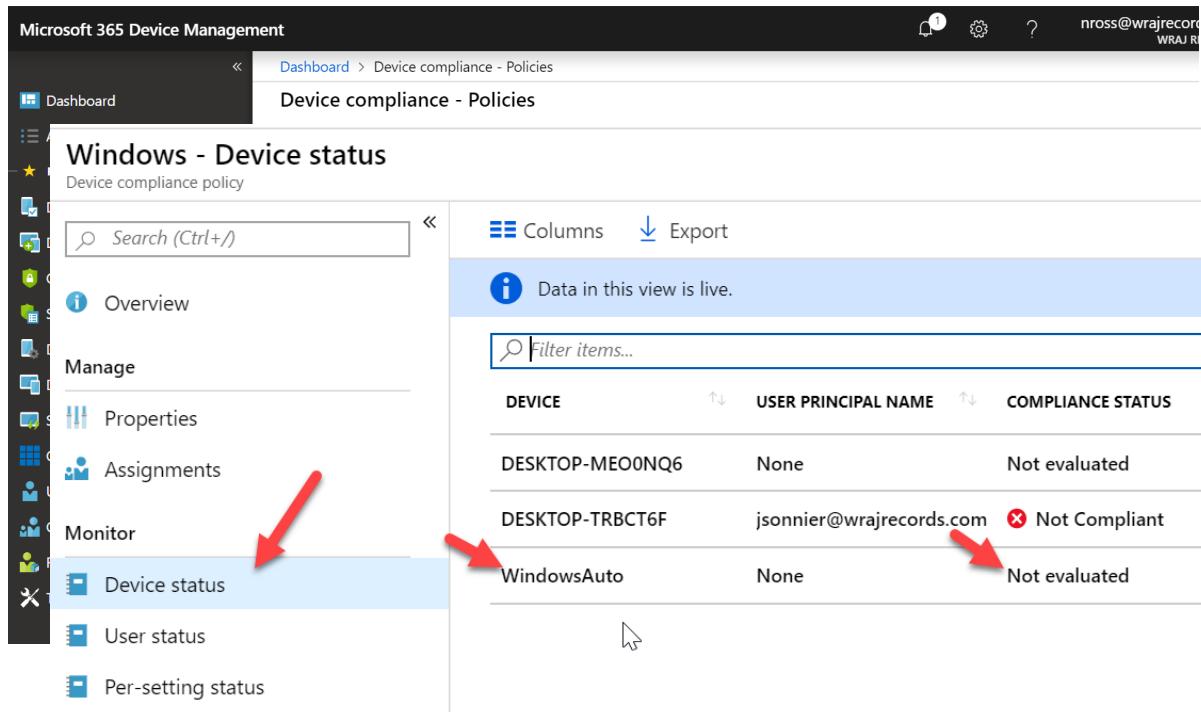
You're all set!

This device is connected to wraj 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 nrross@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)

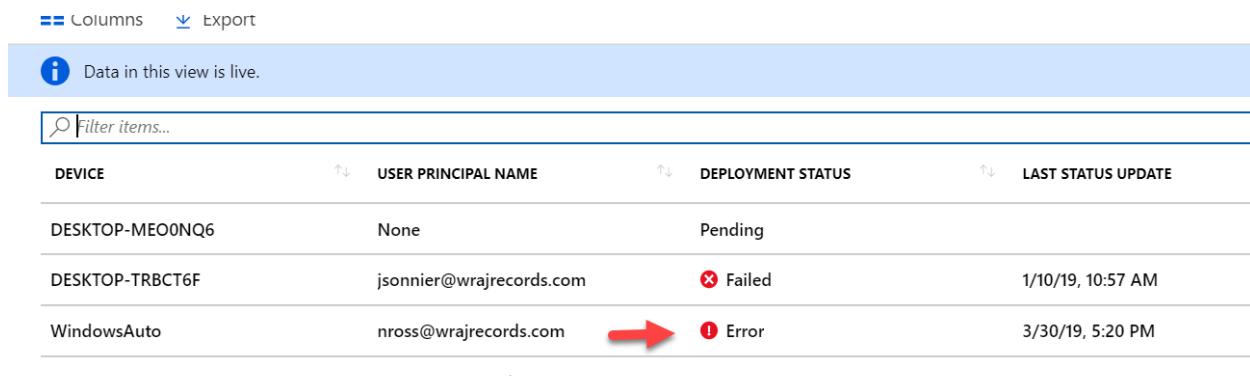


DEVICE	USER PRINCIPAL NAME	COMPLIANCE STATUS
DESKTOP-MEO0NQ6	None	Not evaluated
DESKTOP-TRBCT6F	jsonnierz@wrajrecords.com	<span style="color:red;">✖ Not Compliant</span>
WindowsAuto	None	Not evaluated

- 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:



DEVICE	USER PRINCIPAL NAME	DEPLOYMENT STATUS	LAST STATUS UPDATE
DESKTOP-MEO0NQ6	None	Pending	
DESKTOP-TRBCT6F	jsonnierz@wrajrecords.com	<span style="color:red;">✖ Failed</span>	1/10/19, 10:57 AM
WindowsAuto	nross@wrajrecords.com	<span style="color:red;">✖ Error</span>	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

		Retire     Wipe     Delete     Remote lock     Sync     Reset passcode     Restart																				
<b>Overview</b>  <b>Manage</b>  <b>Properties</b>  <b>Monitor</b> 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	<a href="#">See more</a>		Device actions status		<table border="1"> <thead> <tr> <th>ACTION</th> <th>STATUS</th> <th>DATE/TIME</th> </tr> </thead> <tbody> <tr> <td colspan="3">No results</td> </tr> </tbody> </table>		ACTION	STATUS	DATE/TIME	No results		
	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																				
	<a href="#">See more</a>																					
	Device actions status																					
	<table border="1"> <thead> <tr> <th>ACTION</th> <th>STATUS</th> <th>DATE/TIME</th> </tr> </thead> <tbody> <tr> <td colspan="3">No results</td> </tr> </tbody> </table>		ACTION	STATUS	DATE/TIME	No results																
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 

- 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		
<a href="#">Export</a>		
SETTING	STATE	STATE DETAILS
Antispyware	✓ Compliant	
Number of non-alphanumeric characters in password	✓ 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

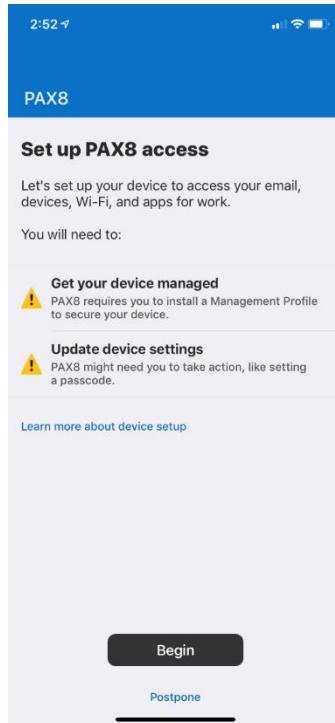
Microsoft Corporation

#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

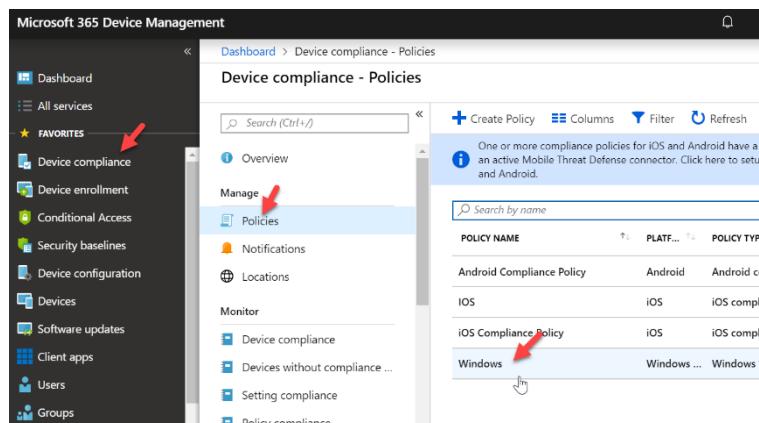
- End User Experience for Communications to Broad audience
- Common Troubleshooting Techniques for each platform

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

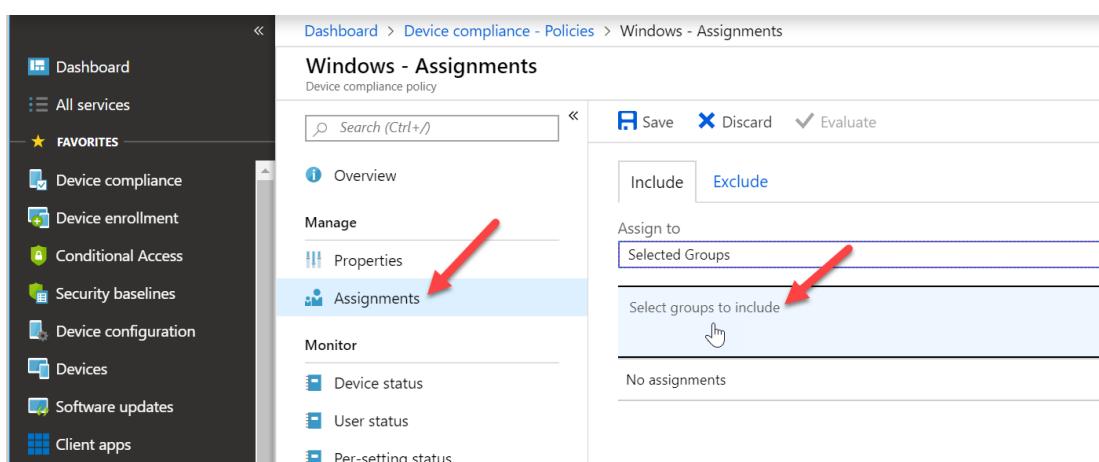
Lastly, after we have this pushed out and a target date for deployment, we can go back into the Device Management Admin Center and begin to add our groups to our policies and profiles:

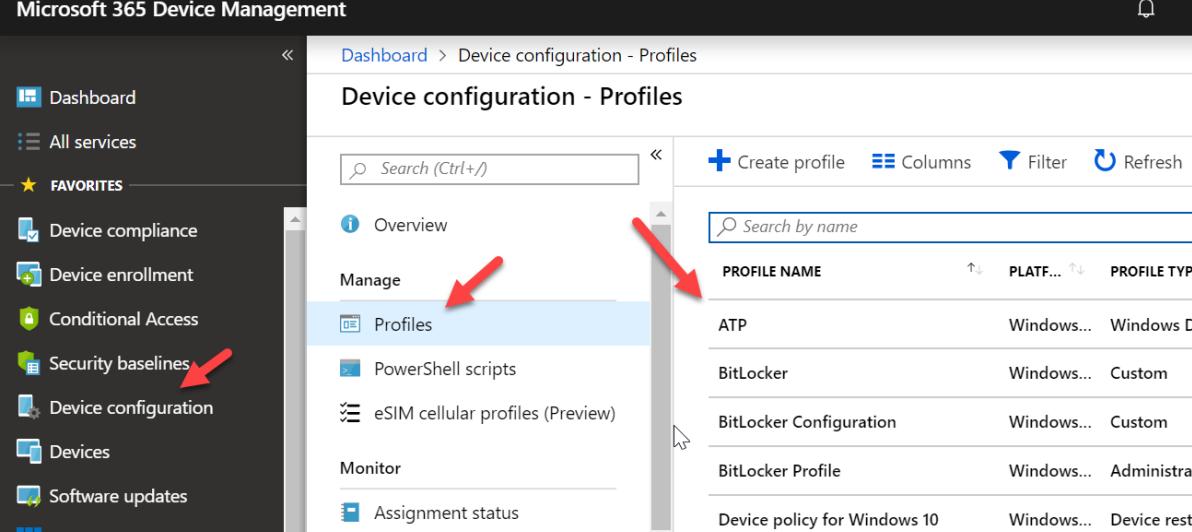
- a. Go to Device Compliance and click on policy you want to add a group to:



POLICY NAME	PLATF...	POLICY TYP...
Android Compliance Policy	Android	Android compl...
iOS	iOS	iOS compl...
iOS Compliance Policy	iOS	iOS compl...
<b>Windows</b>	Windows	Windows

- 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





**Microsoft 365 Device Management**

Dashboard > Device configuration - Profiles

## Device configuration - Profiles

Search (Ctrl+ /) Create profile Columns Filter Refresh

**OVERVIEW**

**Manage**

- Profiles** (selected) (Red arrow pointing here)
- PowerShell scripts
- eSIM cellular profiles (Preview)

**Monitor**

Assignment status

PROFILE NAME	PLATF...	PROFILE TYP...
ATP	Windows...	Windows D...
BitLocker	Windows...	Custom
BitLocker Configuration	Windows...	Custom
BitLocker Profile	Windows...	Administrat...
Device policy for Windows 10	Windows...	Device restri...

## 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](mailto:Msp4msps@tminus365.com)

