Intune Implementation Guide

Guide Description

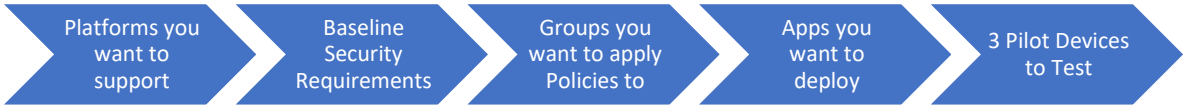
*The purpose of this guide is to lay out the steps for implementing Intune. This guide is assuming you have the **M365 Business** License. It can apply to EMS licenses but some features will not be covered such as Conditional Access and Windows Autopilot. After you complete this guide you will have:*

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

Disclaimer

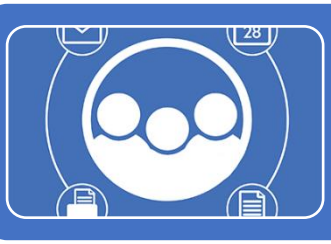
This guide is meant to provide best practices for policy creation and implementation of Intune. It is meant to be used as a template, but the policies defined will not be the same in all use cases. You must access to policies and configuration you will need for your customers environment and make changes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

Pre-Flight Checklist



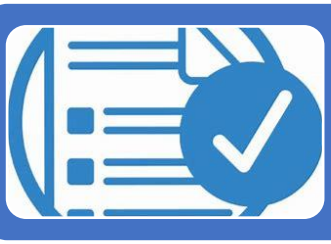
a. Determine Platforms that you will support
    i. IOS/Android
    ii. MAC/Windows
b. Have baseline security requirements complied that you want to implement
    i. Min/Max OS versions
    ii. Password Requirements
    iii. Encryption Enabled
c. Determine if there will be separate groups for separate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

Table of Contents



Phase 1: Groups and Licensing

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

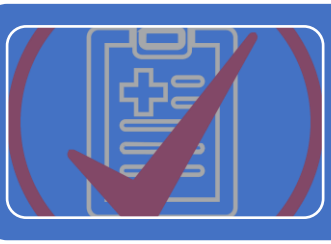


Phase 2: Polciy and Profile Creatation

- Configure Device Polcies
  - 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: Windwos
- Enroll Devices: iOS and Android

Phase 6: Testing and Broad Deployment

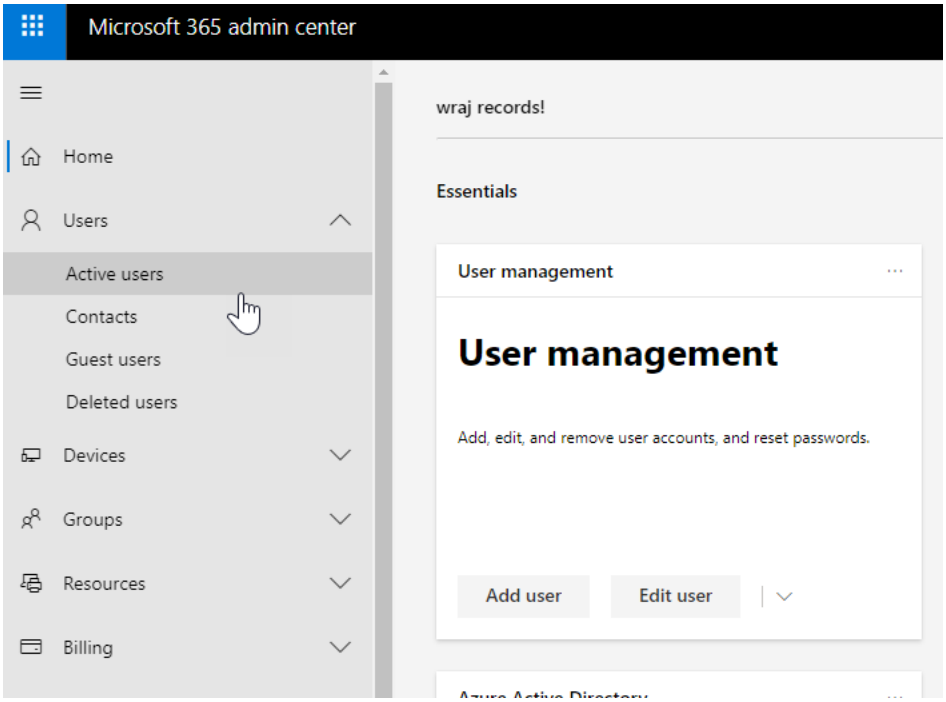
- Pilot Testing and Remediation
- Broad Deployment

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

Licensing Users

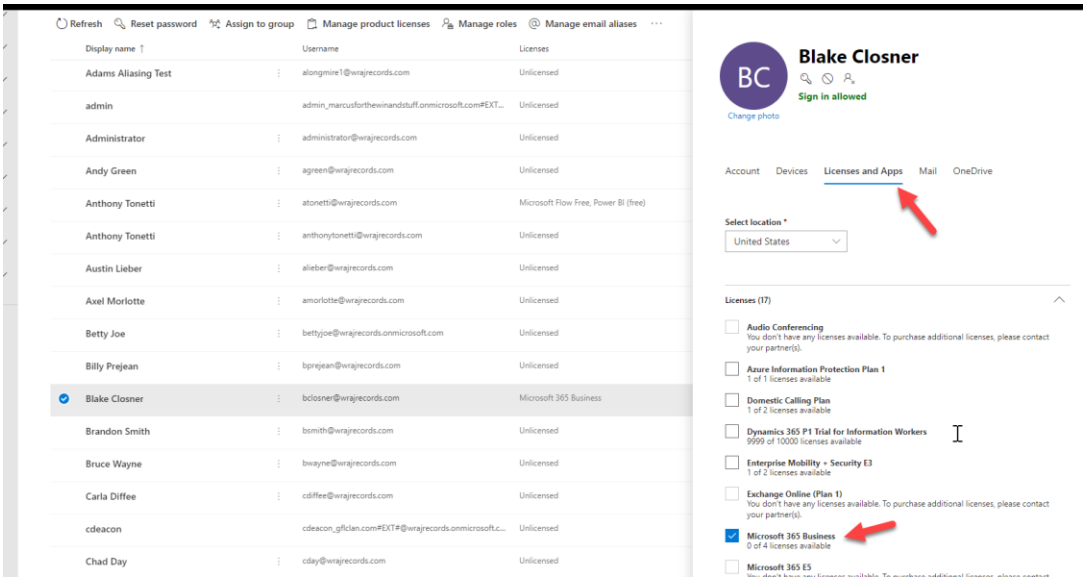
1. Ensure All appropriate Users are Licensed

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



.

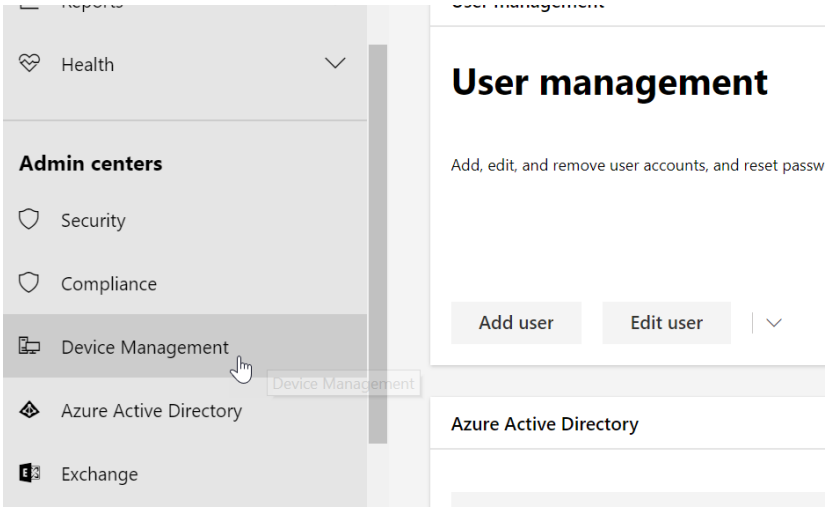
    b. Select a User>Click **Licenses and Apps**>Ensure an M365 License is Assigned



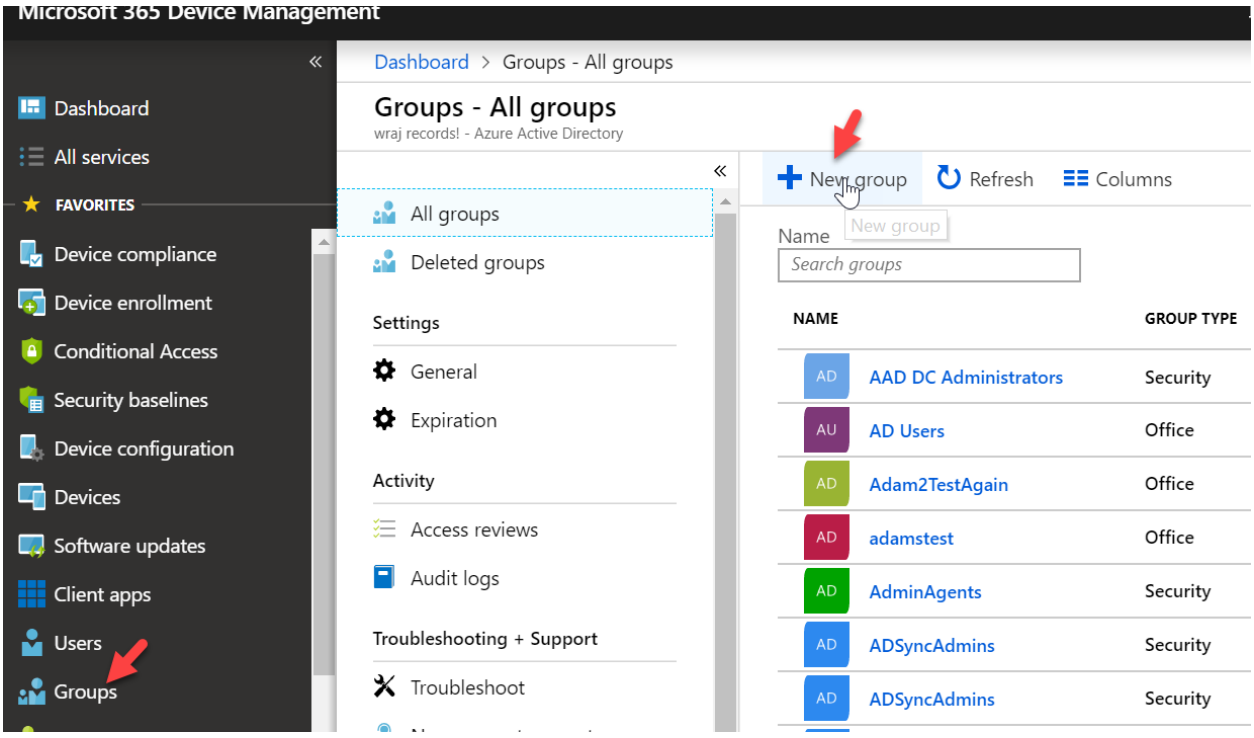
Create Groups

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

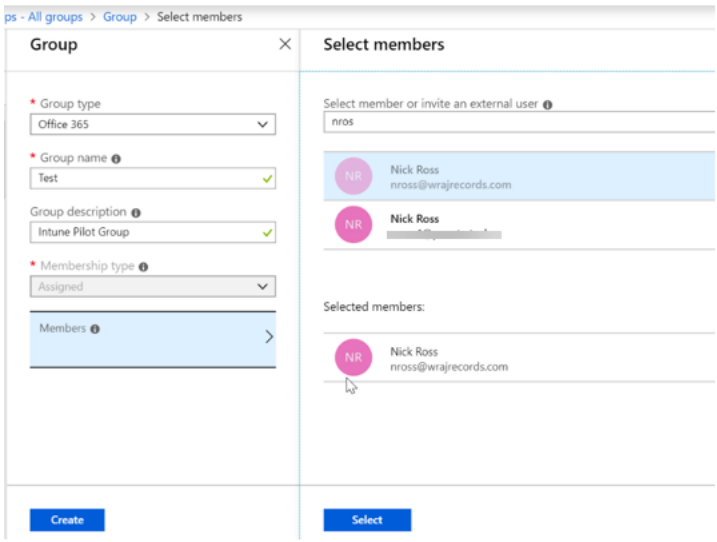
a. Scroll Down in the 365 Admin Portal and Go to the **Device Management Portal**



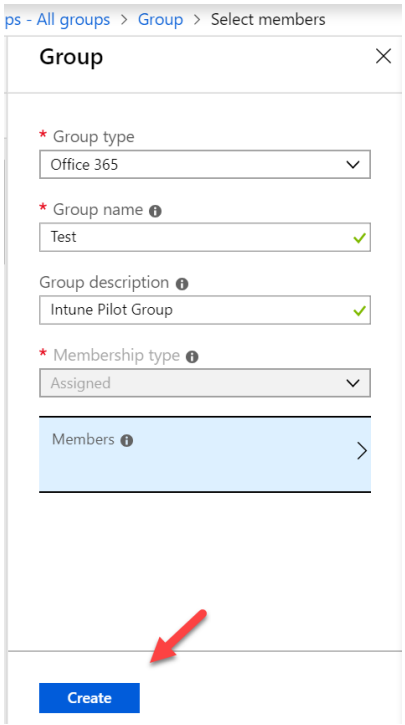
b. Click on **Groups** and click **New Group**



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



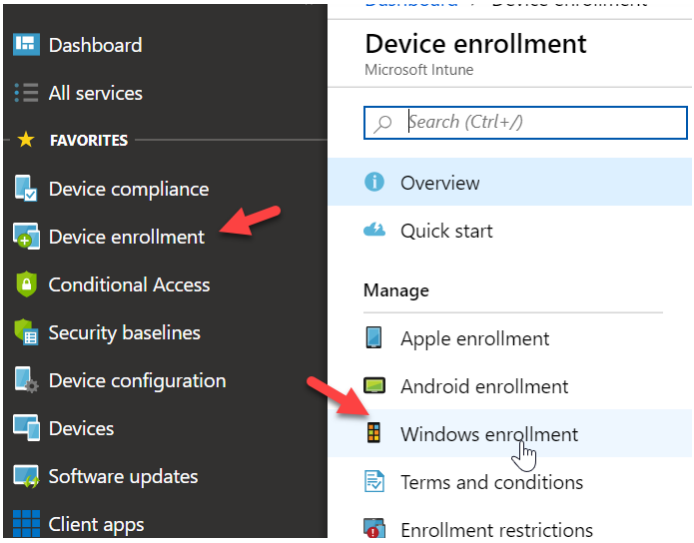
d. Click **Create** when finished



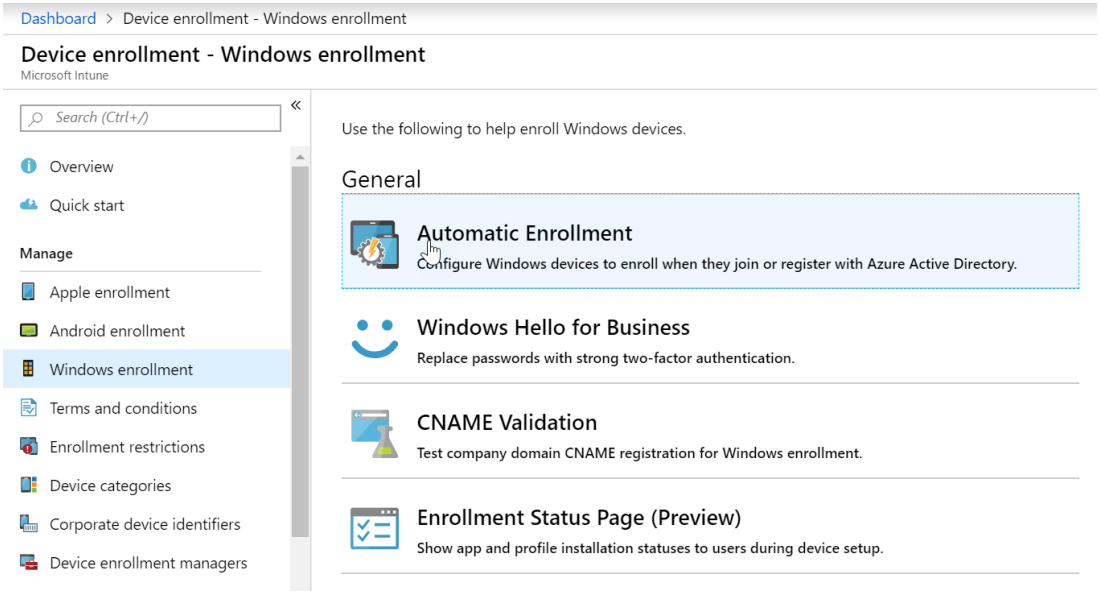
Device Autoenrollment

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:

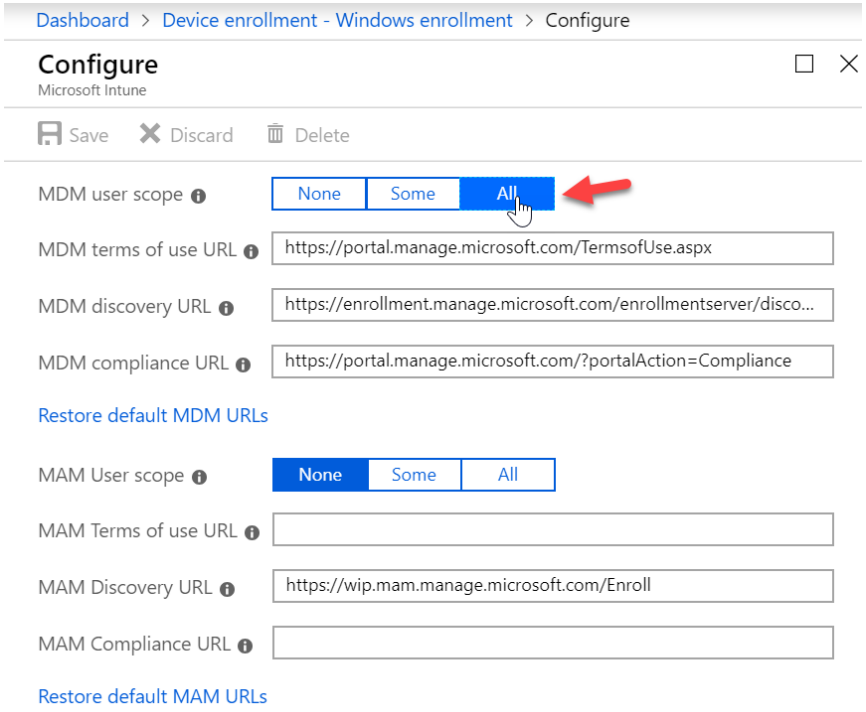
a. Go to **Device Enrollment** and click **Windows Enrollment**



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

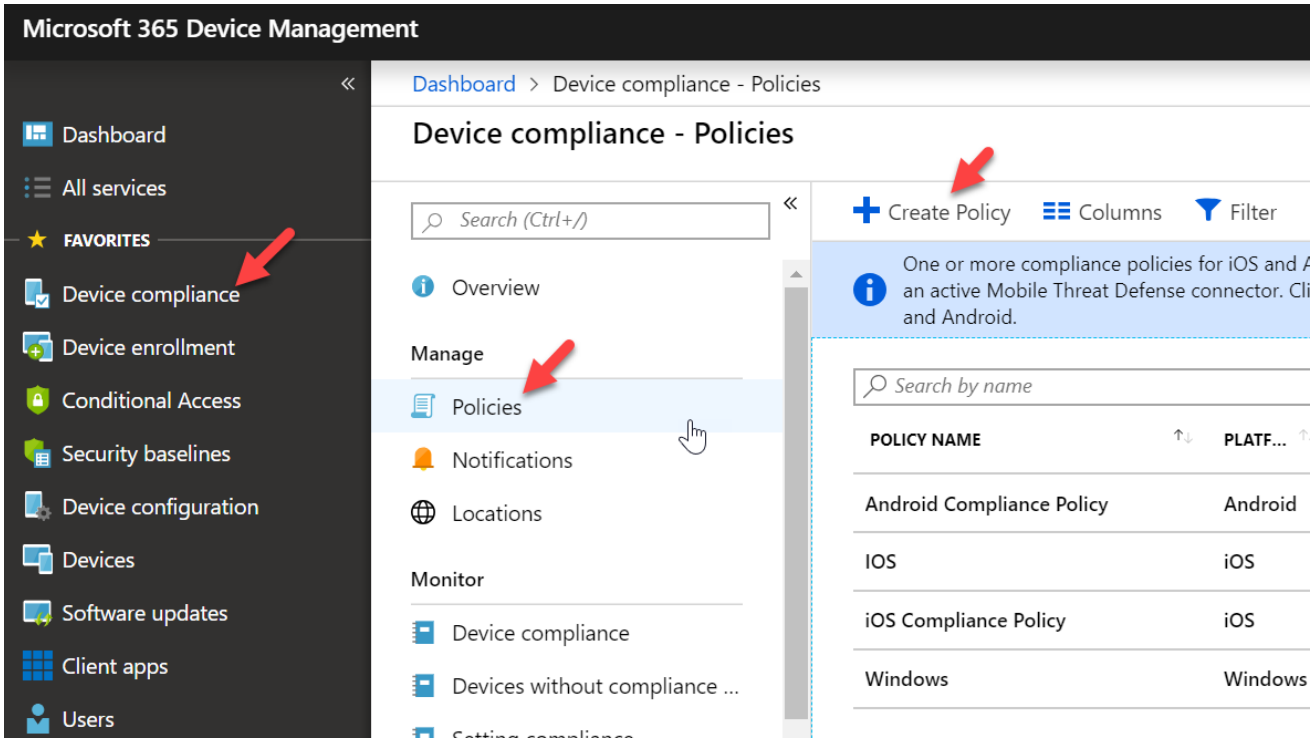


Configure Device Policies

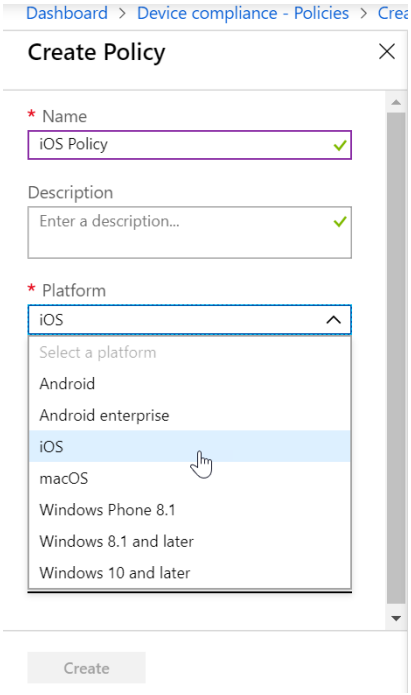
Device Policies designate which devices are compliant and non-compliant. When we join devices to Intune after configuring these policies, we will be able to see why the devices are not compliant. You will want to create a device policy for every platform you wish to support in your organization

IOS

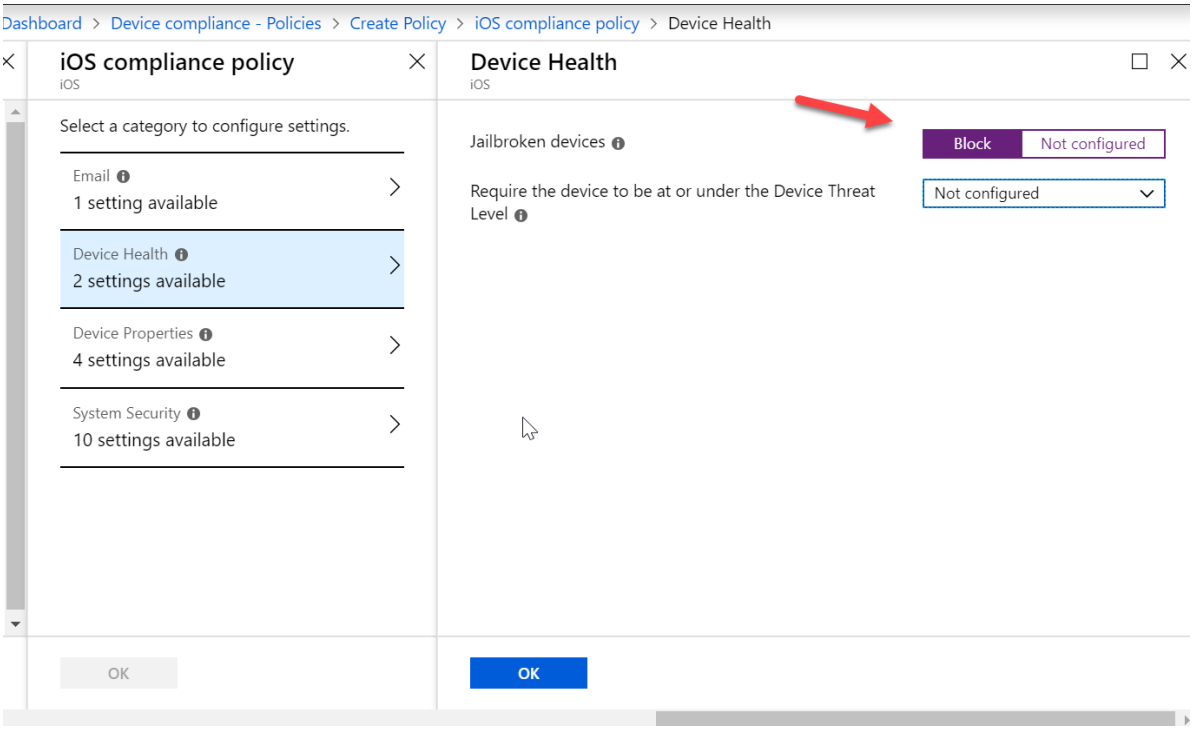
a. In the Device Management admin portal, go to **Device Compliance**>**Policies**>**Create Policy**



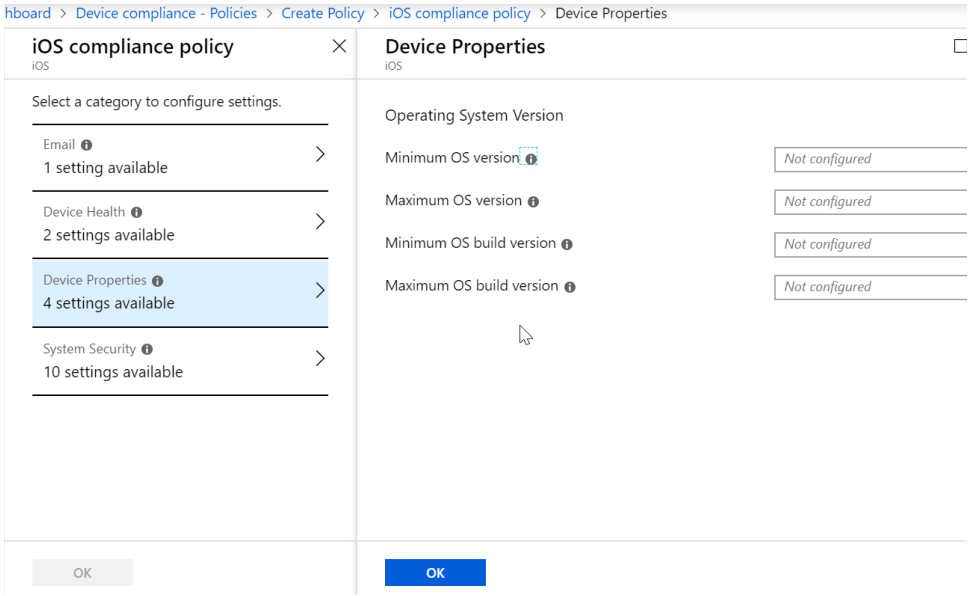
b. The first policy we will create is for iOS. Select a **Name** and **Description** (if applicable) and choose **iOS** from the **Platform** dropdown list



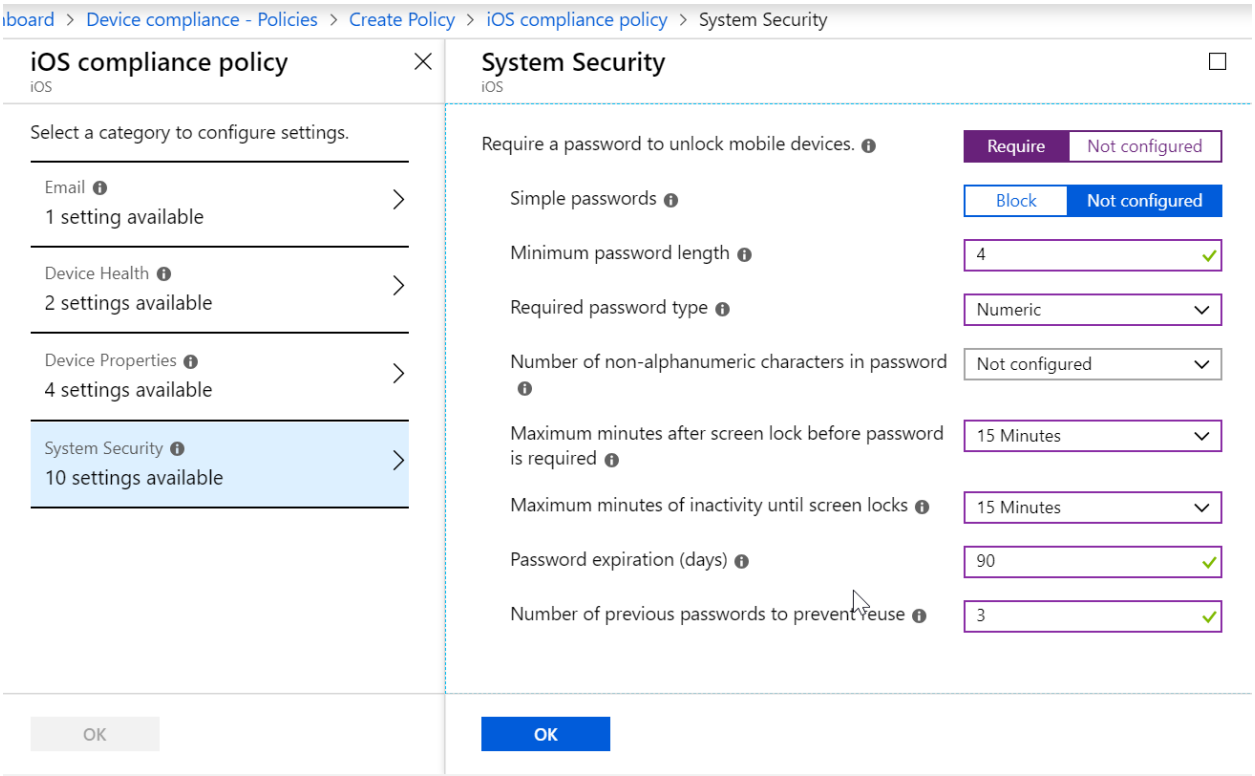
c. Under the **Device Health** Section for settings, **block Jailbroken Devices**



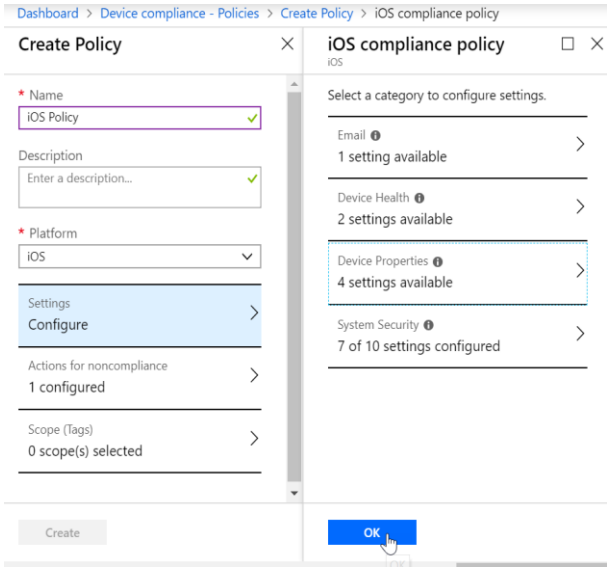
d. Under **Device Properties**, configure **Min/Max OS versions** if applicable. If you do not what to define these settings leave them blank

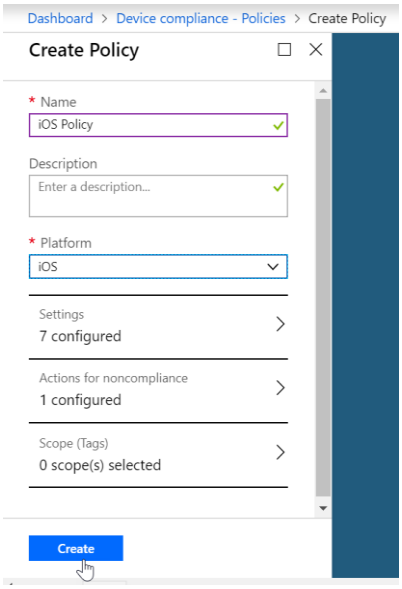


e. Under System Security, enter the values as follows:

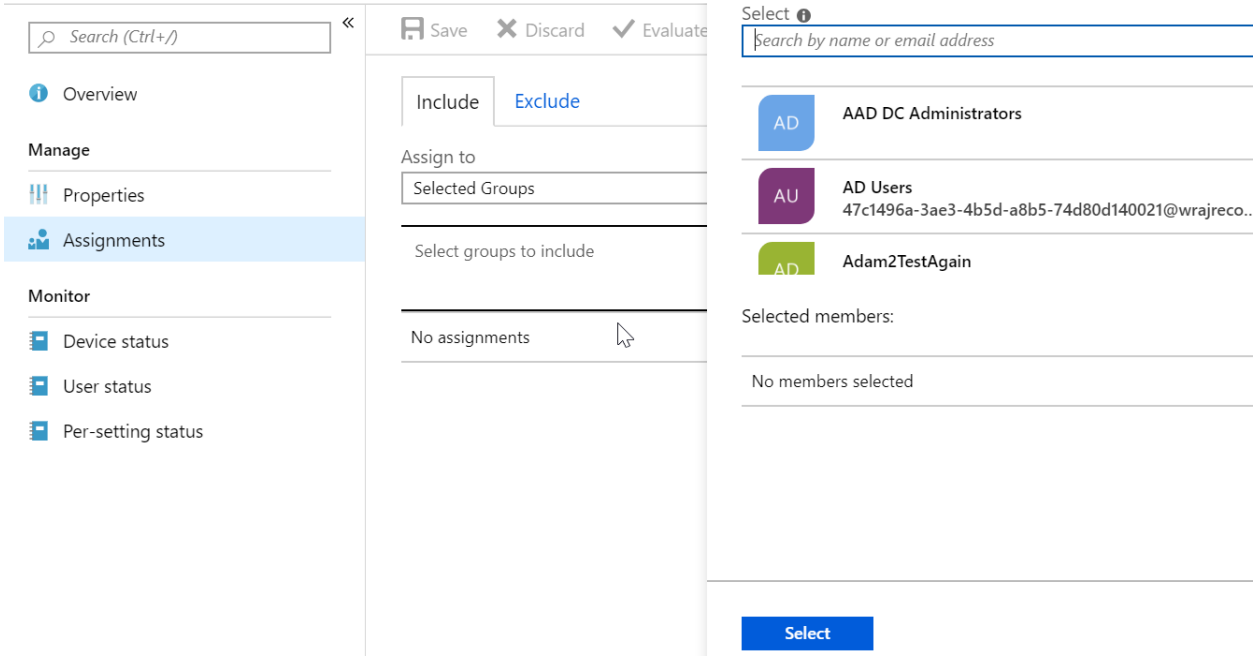


f. Click **ok** and then **Create**



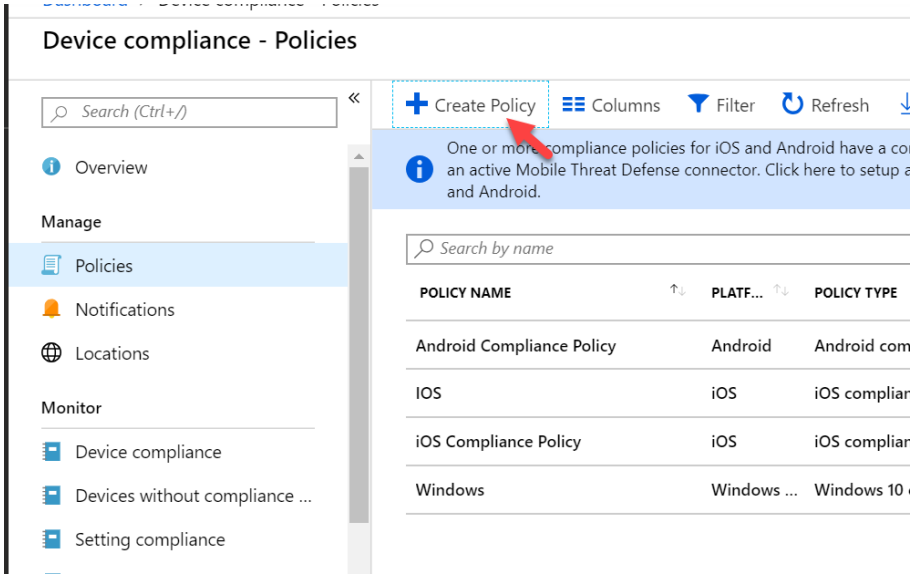


g. Select Assignments and select the group of users you want this policy applied to:

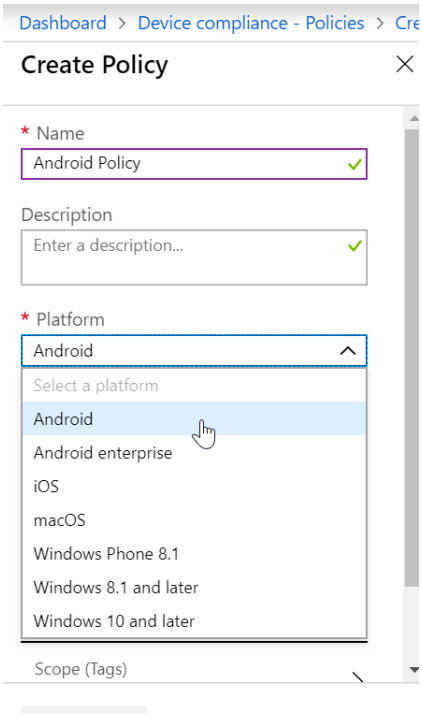


Android

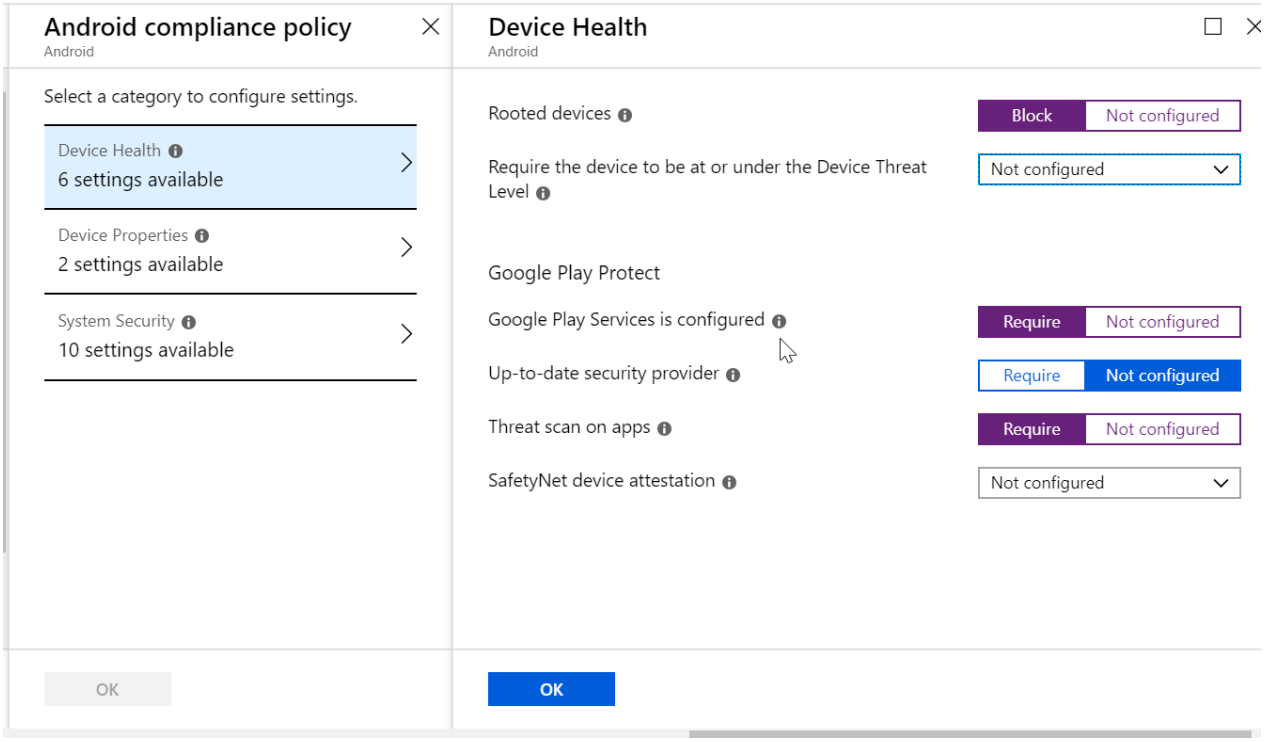
a. Click Create Policy



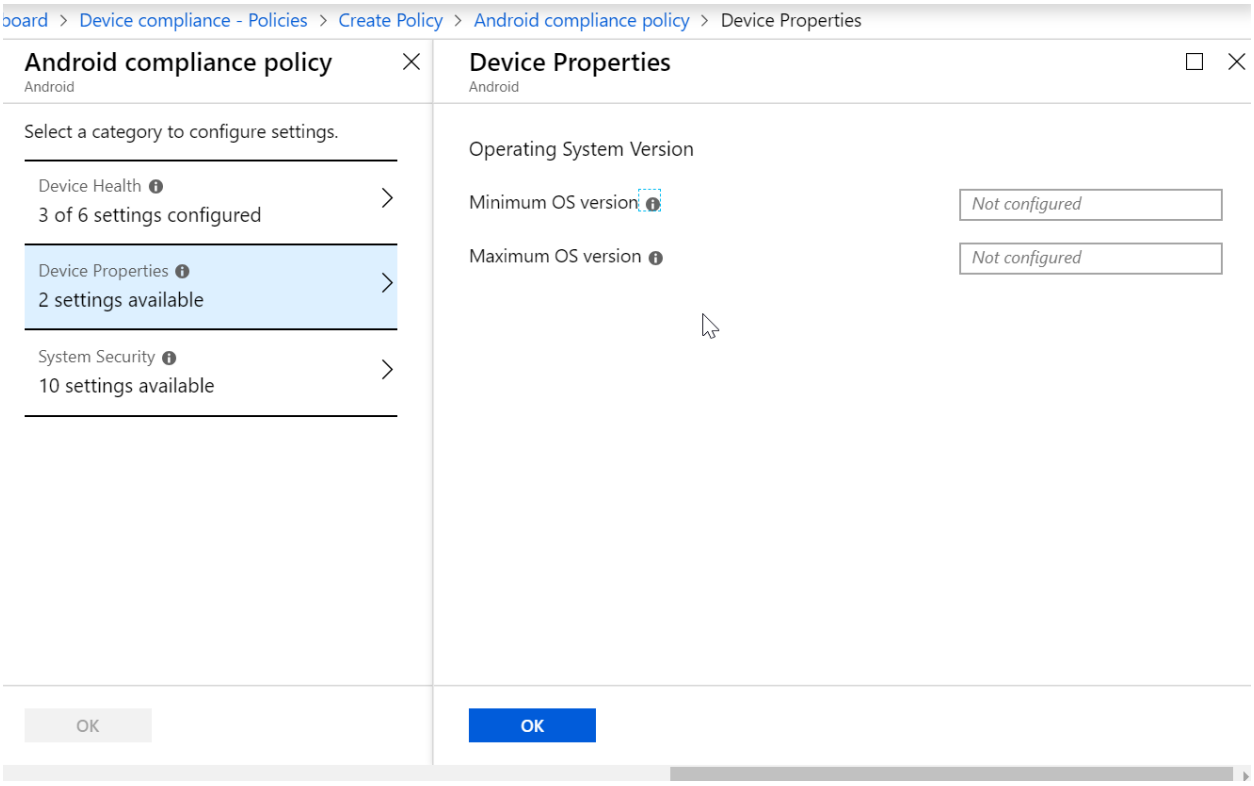
b. Select the **Name**, enter **description** (if applicable), and choose **Android** from Platform dropdown



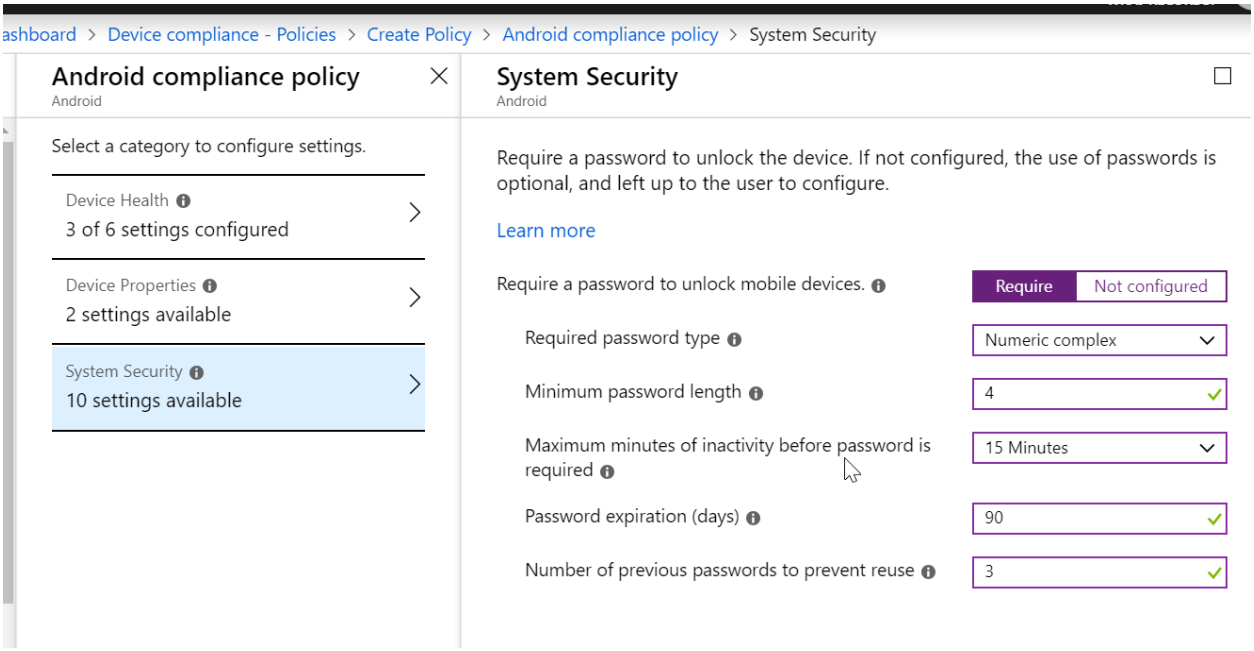
c. Under Settings>Device Health, configure the following:

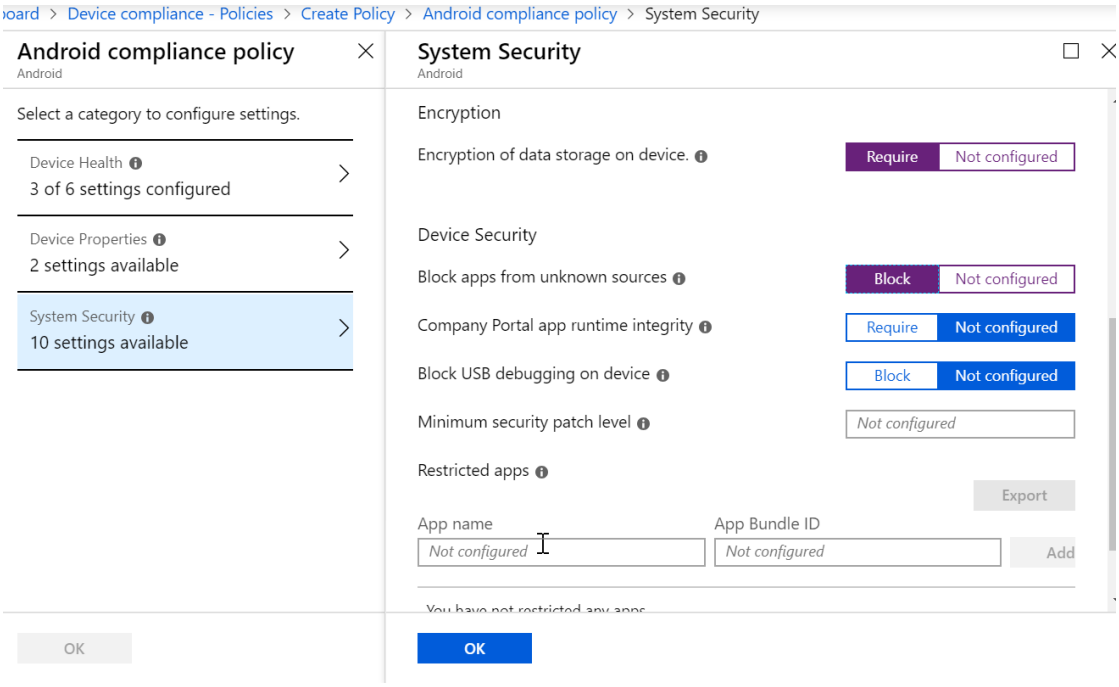


d. Under Device Properties, configure the Min/Max OS version if applicable. If you do not want to configure, leave blank

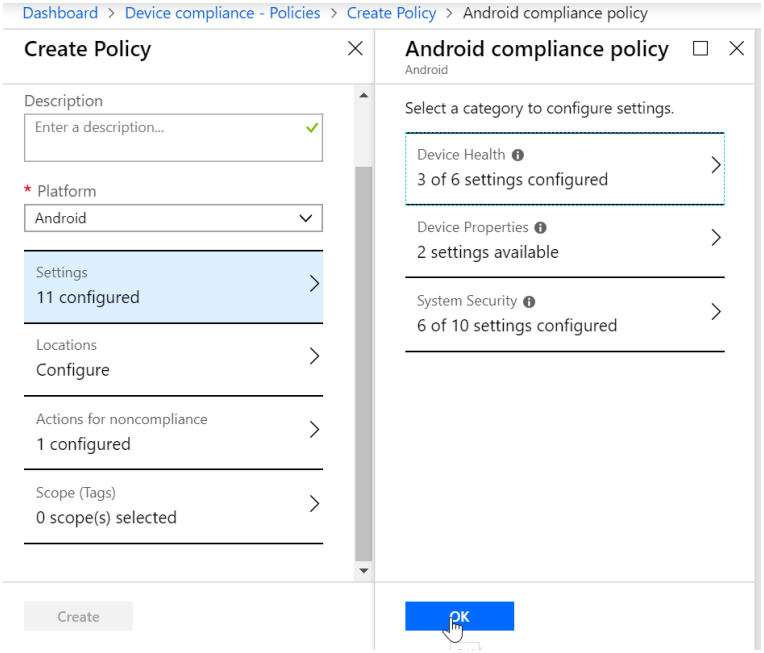


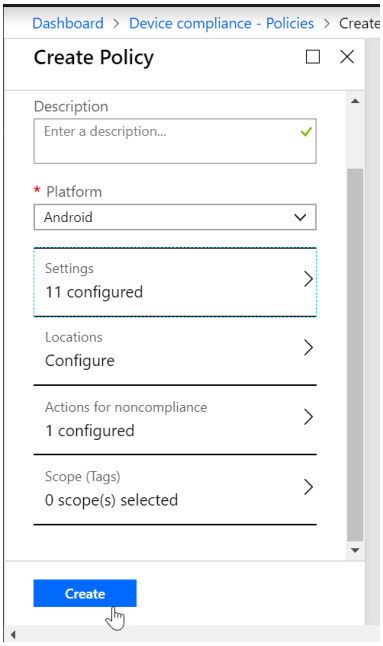
e. Under **System Security**, configure as follows:



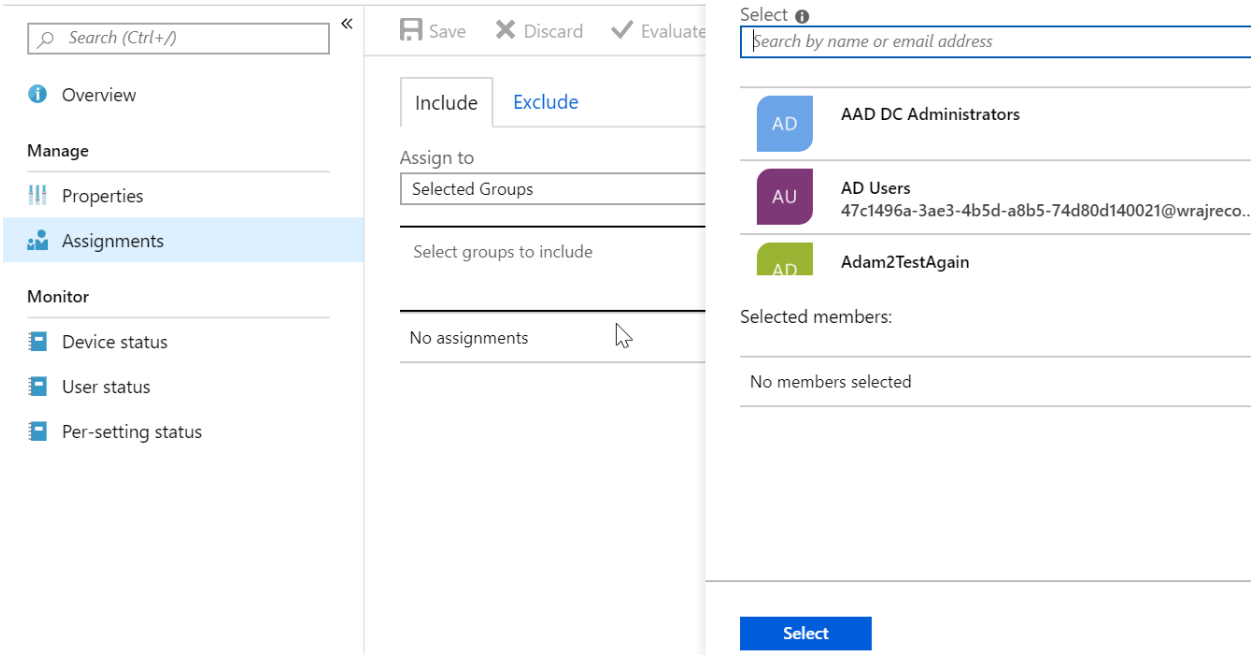


f. Click **OK** and **Create**



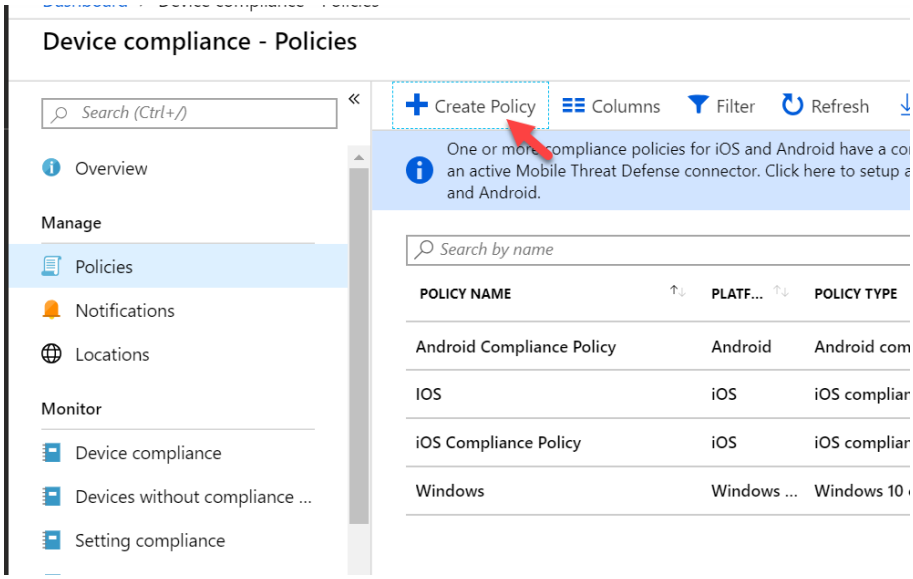


g. Select Assignments and select the group of users you want this to apply to:

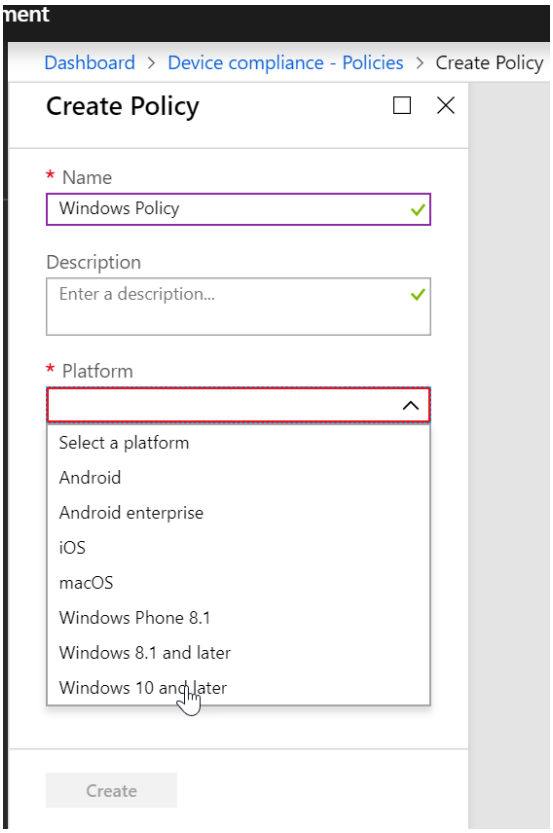


Windows

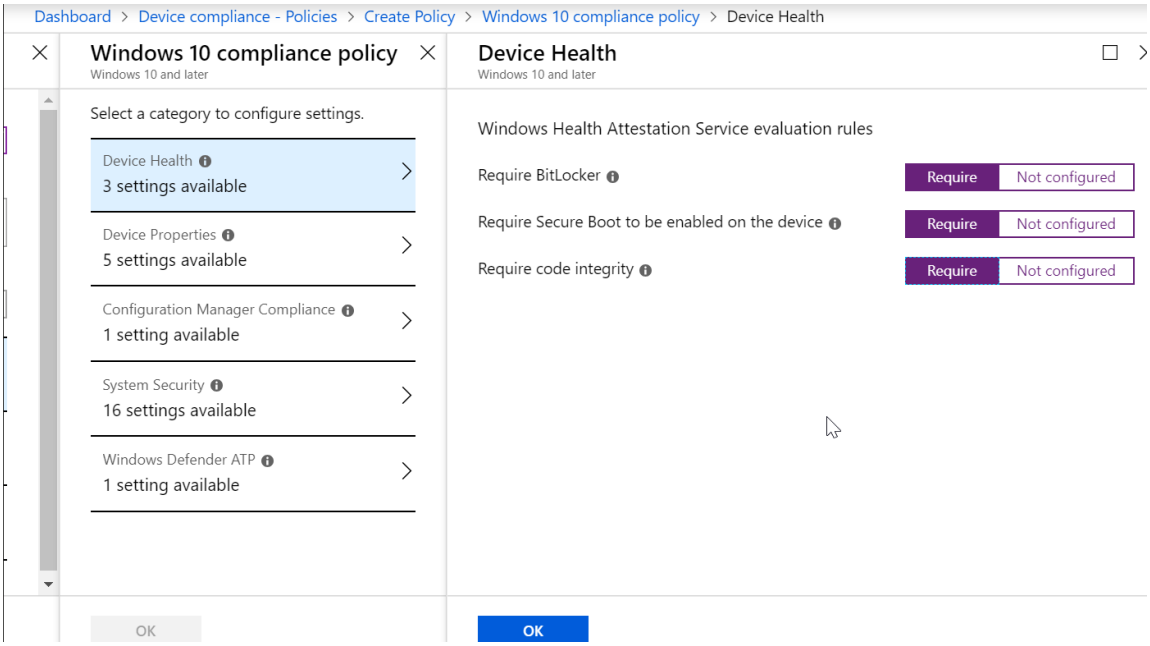
a. Click Create Policy



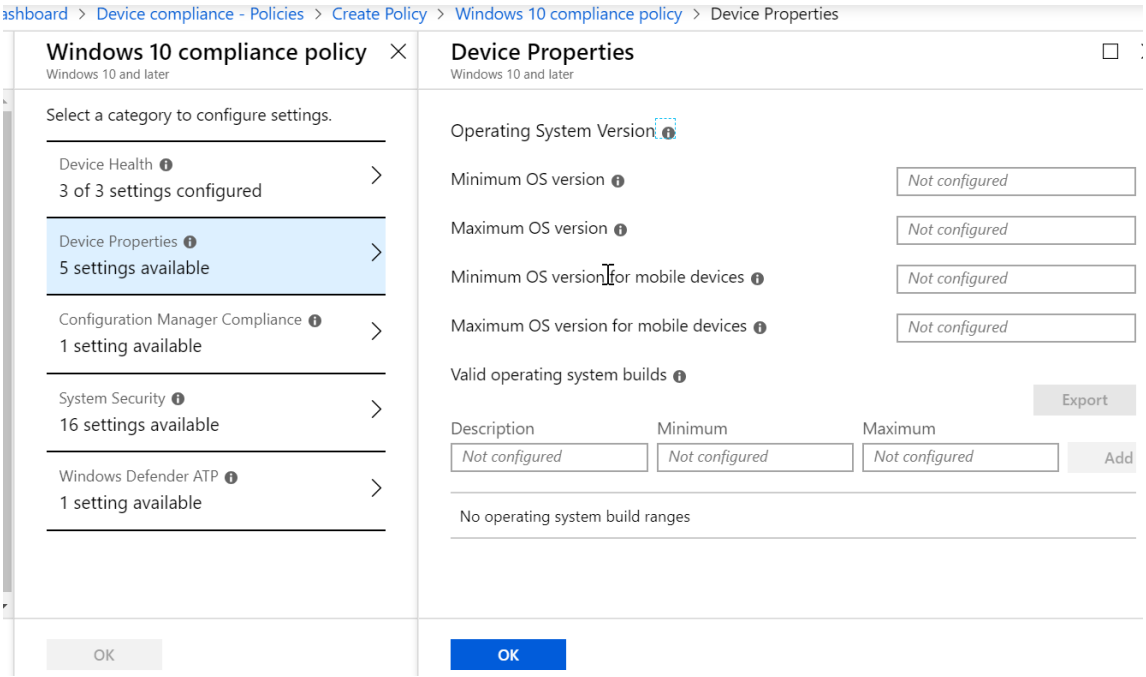
b. Select a **Name**, **Description** (if applicable), and Choose **Windows 10 or later** from the Platform dropdown



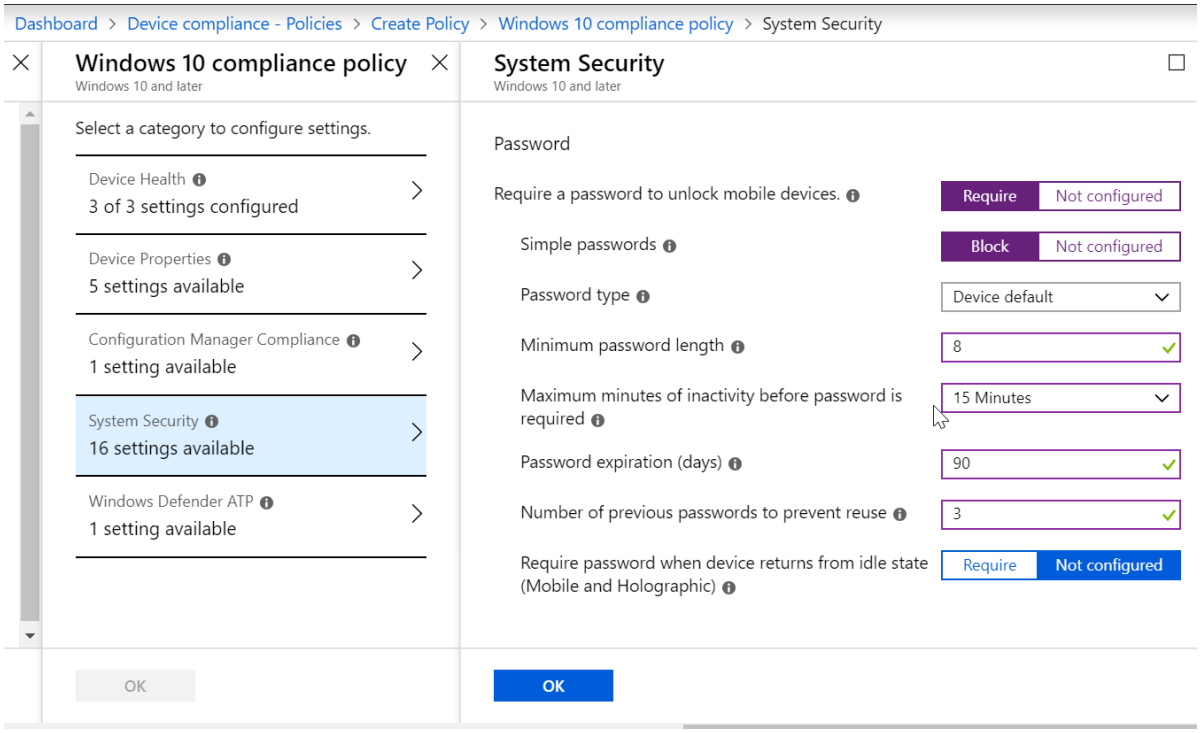
c. Under **Settings>Device Health**, configure the following

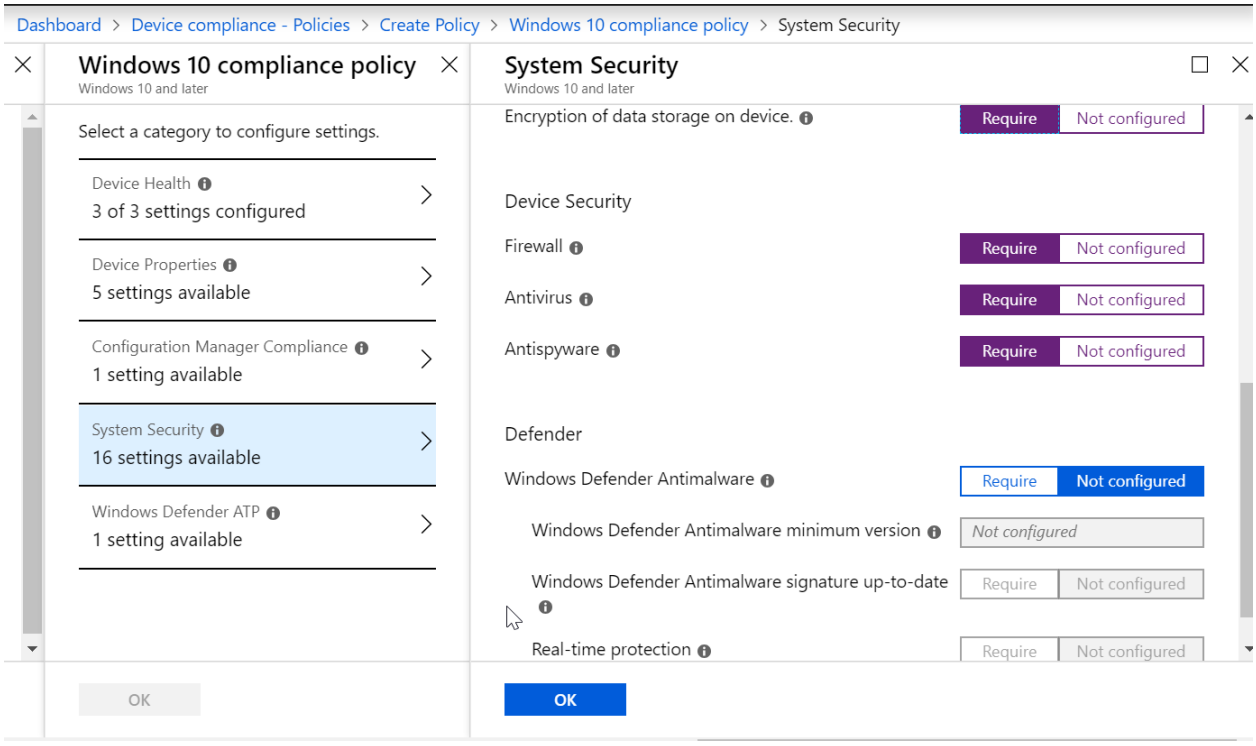


d. Under Device Properties, configure the Min/Max OS version if applicable. If you do not want to configure, leave blank

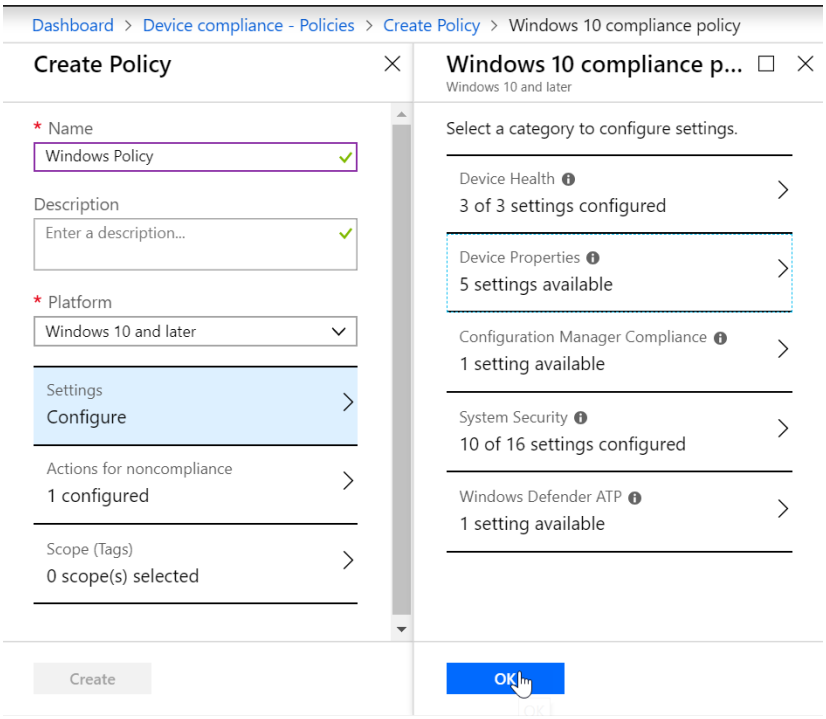


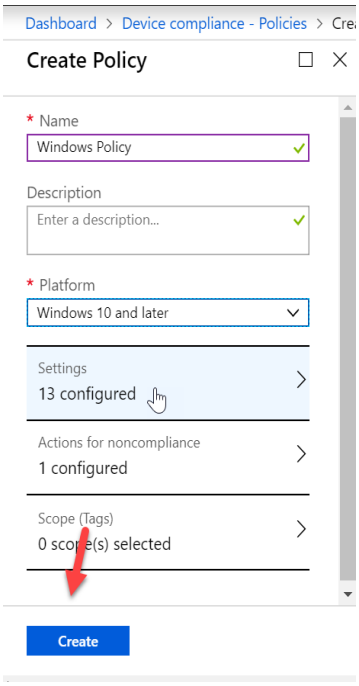
e. Under **System Security**, configure the following:



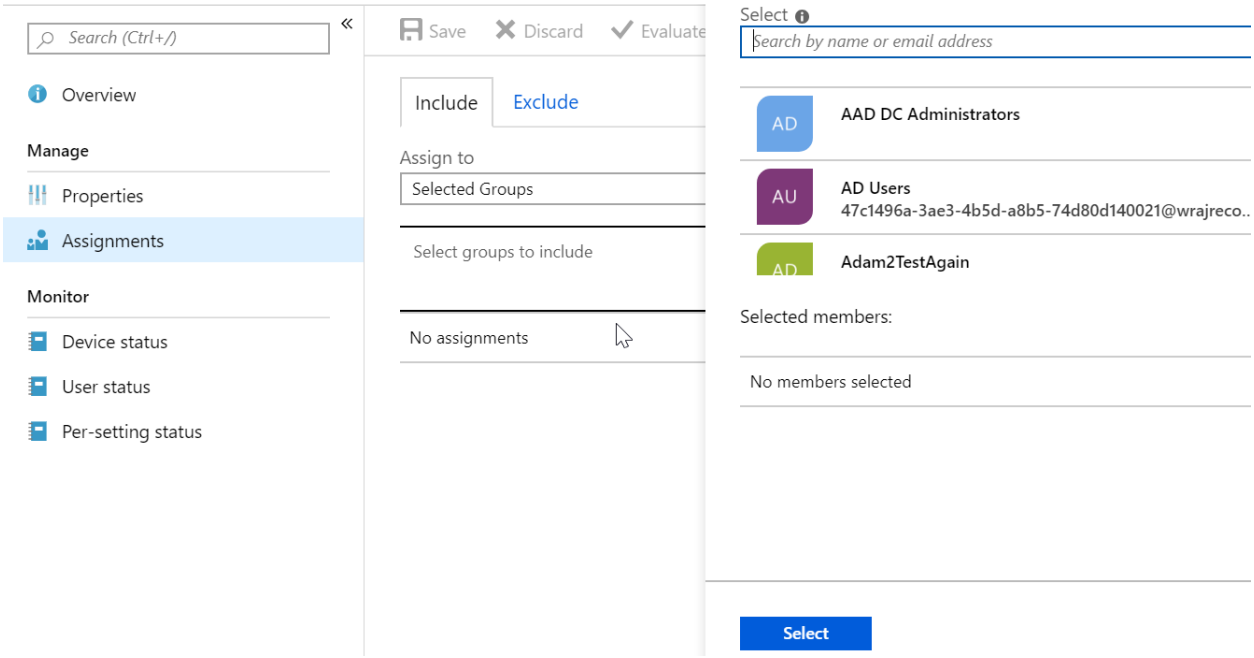


f. Click **Ok** and **Create**





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



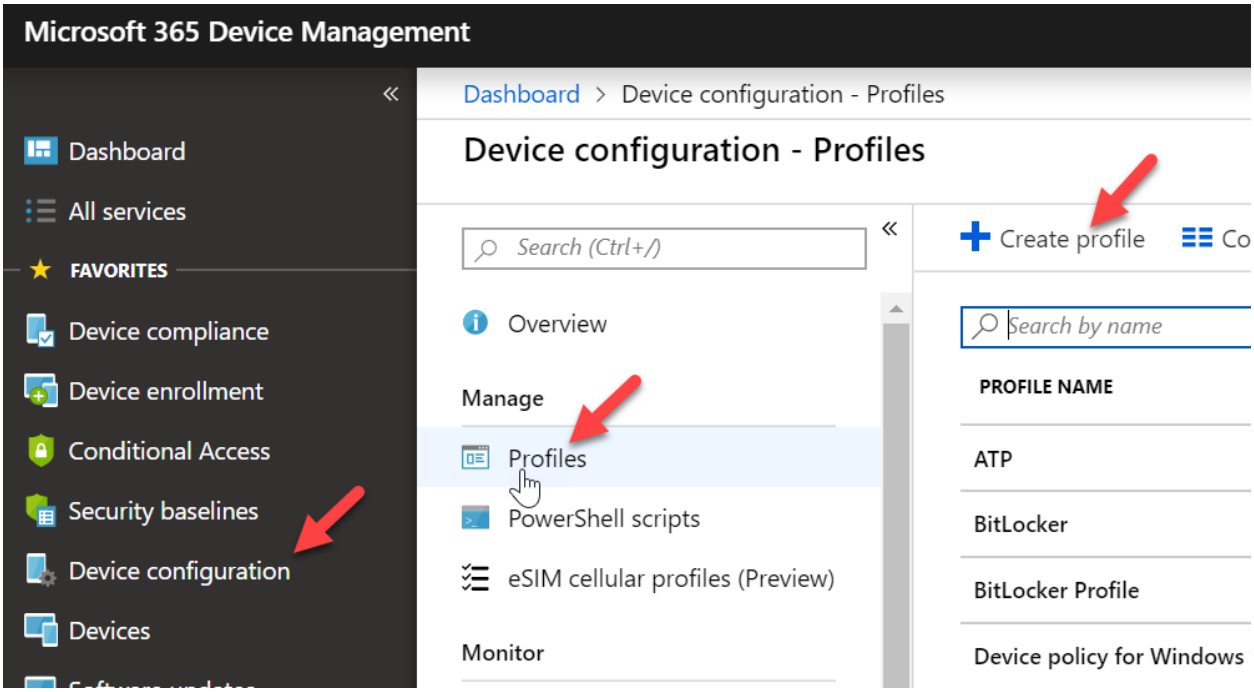
Create Device Profile

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

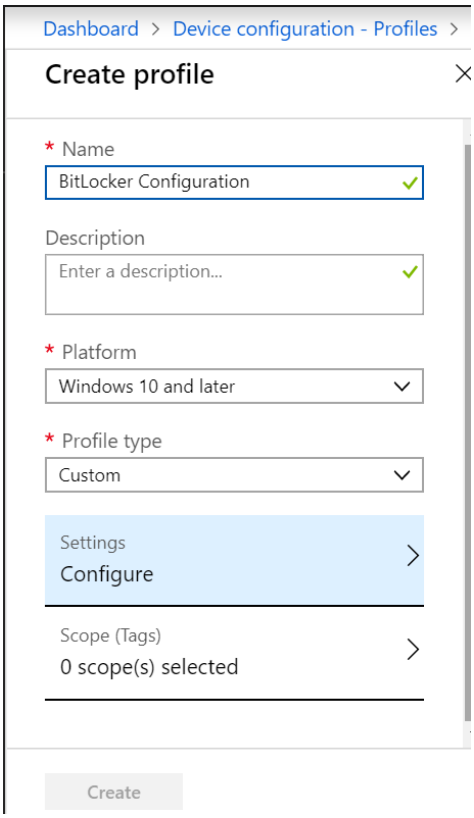
- You create a wifi profile that automatically configures the wifi on device that are enrolled with Intune
- Assume that you want to provision all iOS devices with the settings required to connect to a file share on the corporate network. You create a VPN profile that contains the settings to connect 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.

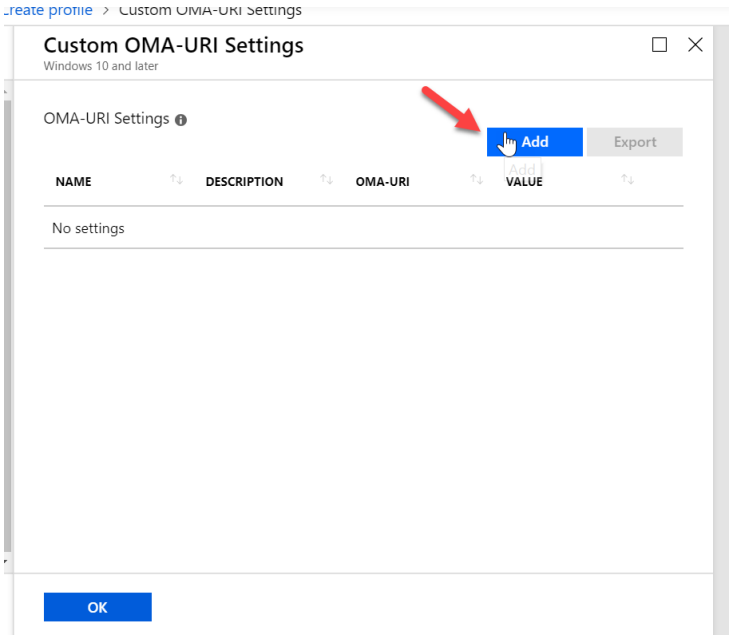
a. Go to the **Device Management Admin Portal>Device Configuration>Profiles>Create Profile**



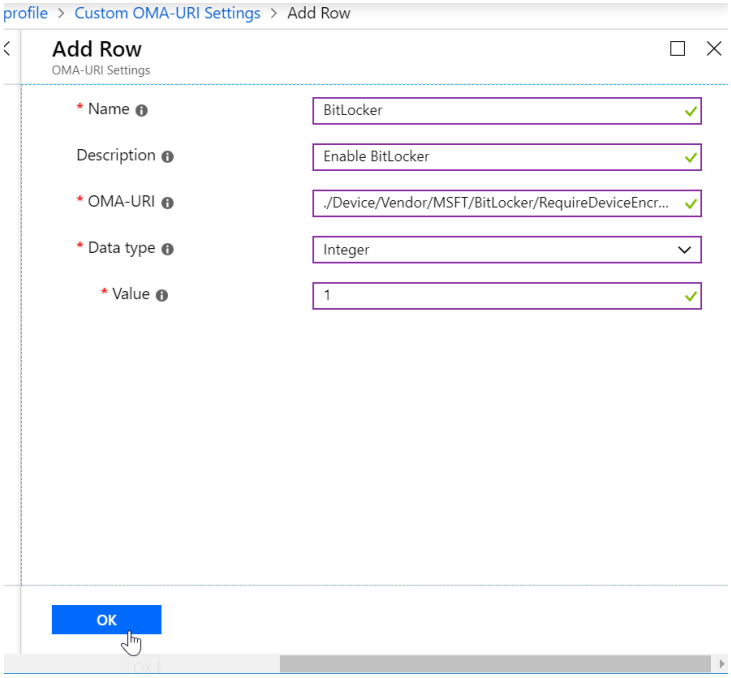
b. Enter a **Name**, **Description** (if applicable), choose **Windows 10 or later** from the platform, and select **Custom** from Profile Type



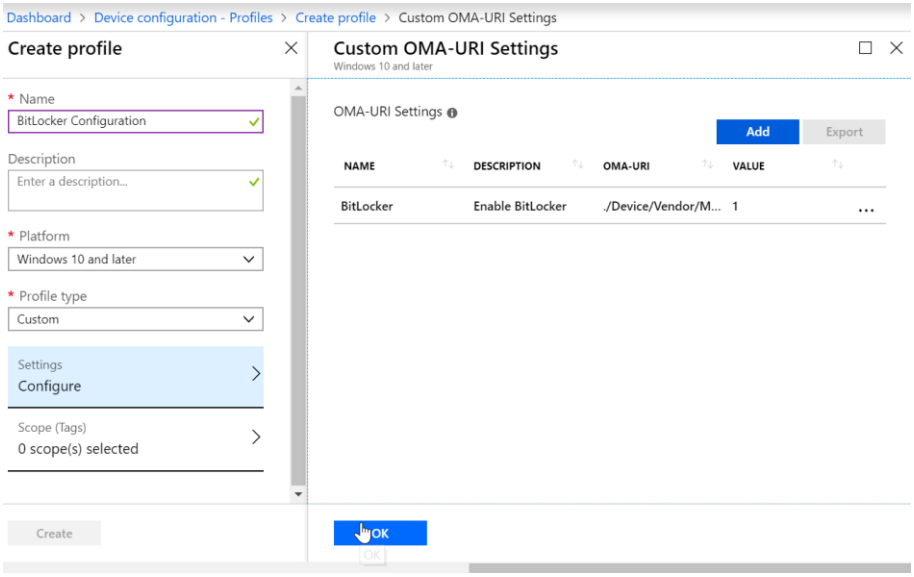
c. Click **Add**

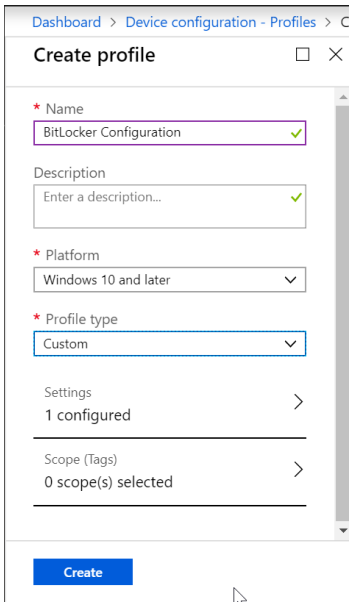


d. Enter the following, including: ./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption

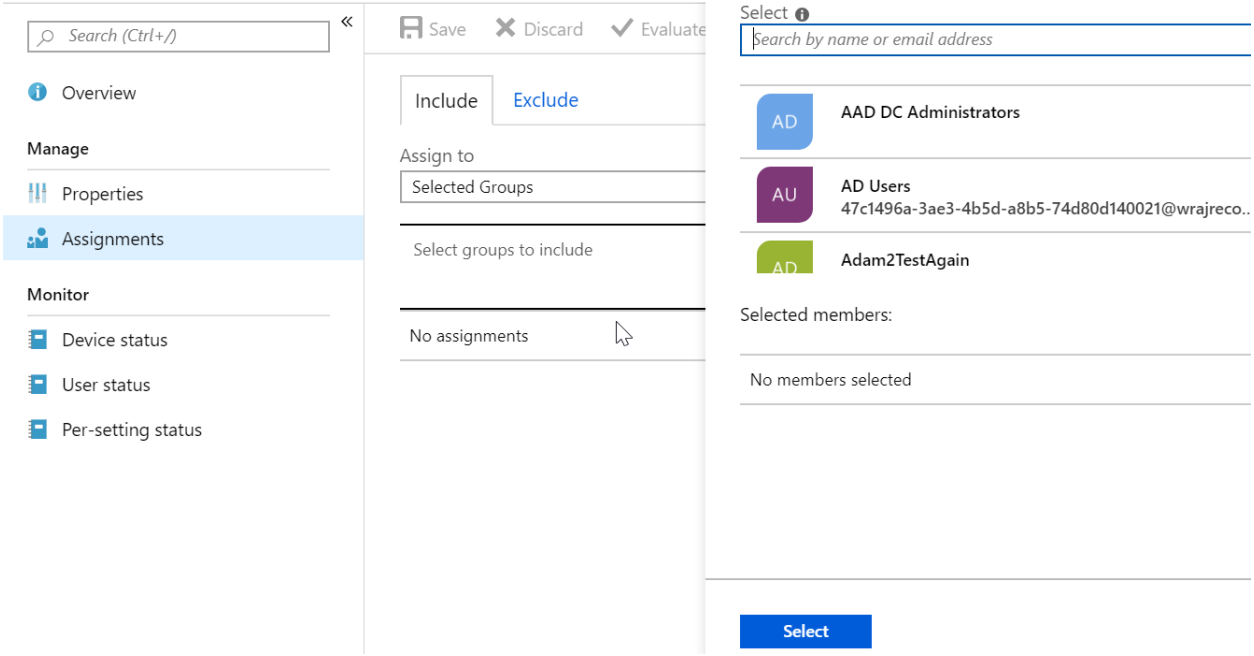


e. Click Ok and Create





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

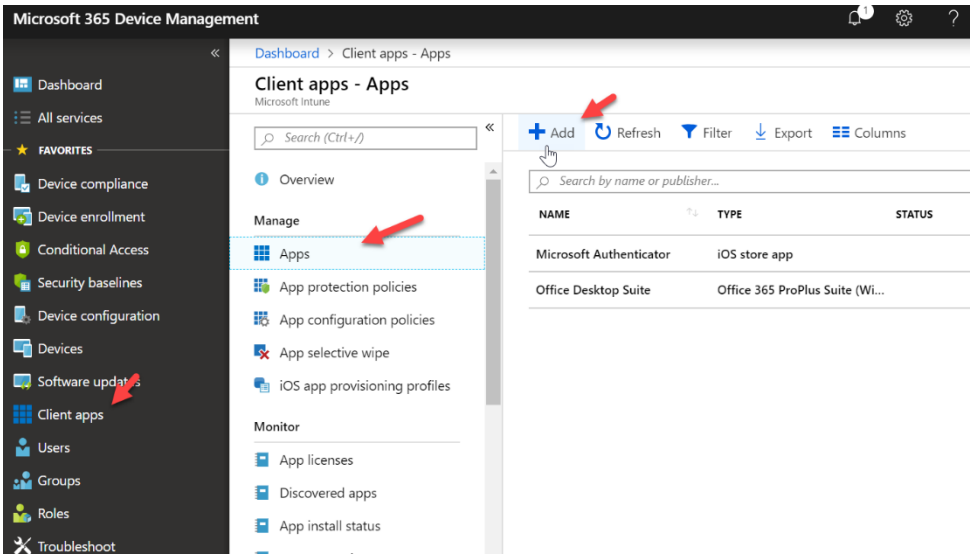


g. End users enrolled in Intune will get a notification to set up BitLocker

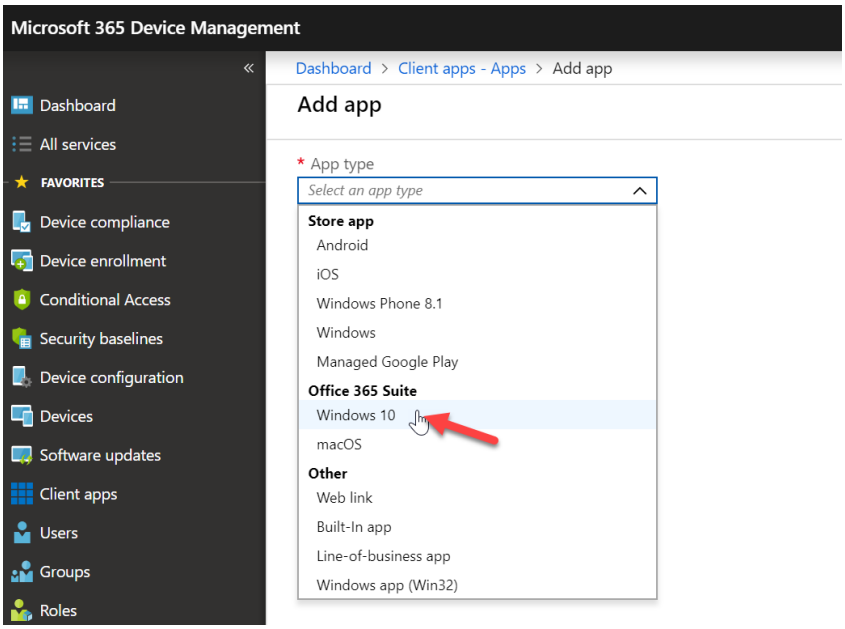
Add an Application

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:

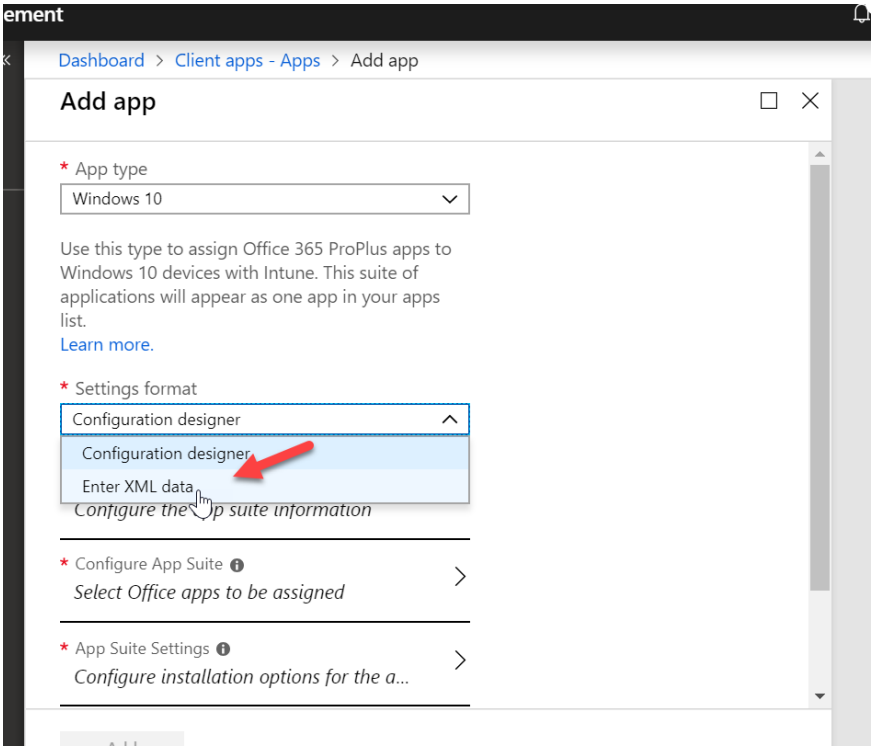
a. In the Device Management Admin center go to **Client Apps>Apps>Add**



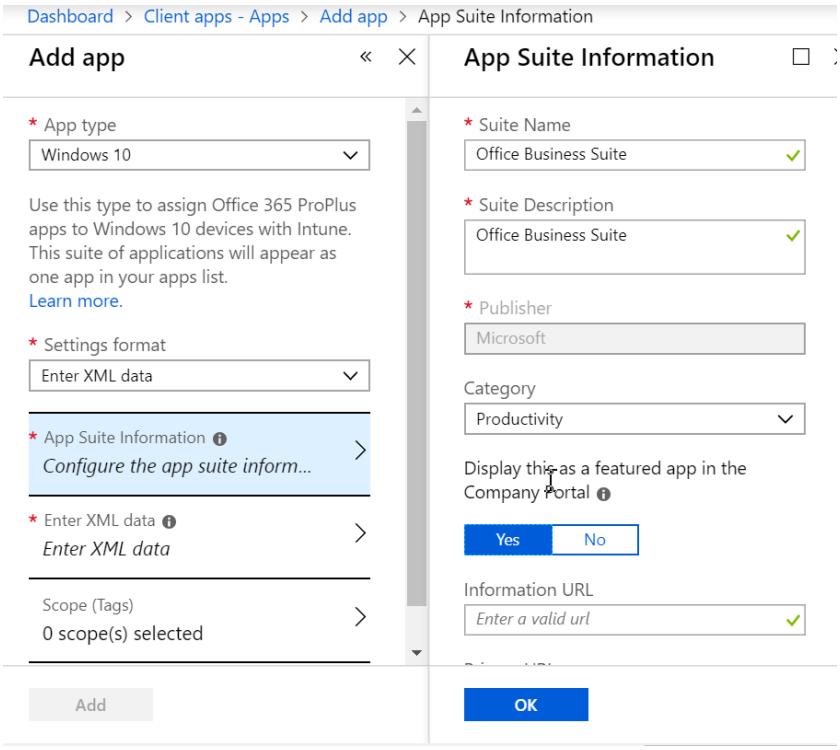
b. Select Windows 10 under Office 365 Suite from the dropdown list:



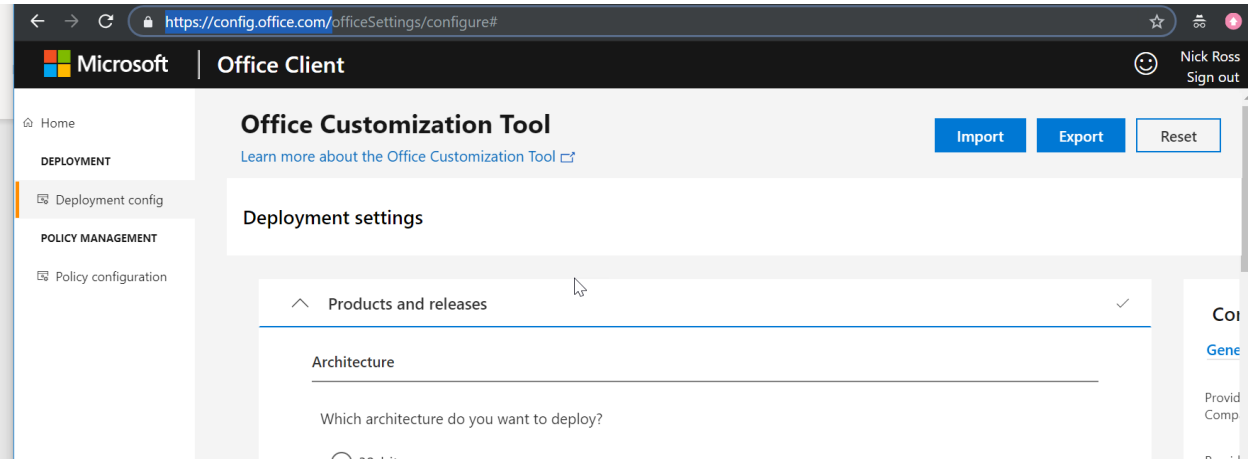
c. Under **Settings Format** select **Enter XML data** *Note* We are making this selection because we have M365 Business Plan. If we have a plan that comes with Proplus (E3,E5, M365 E3, M365 E5) we would select Configuration Designer:



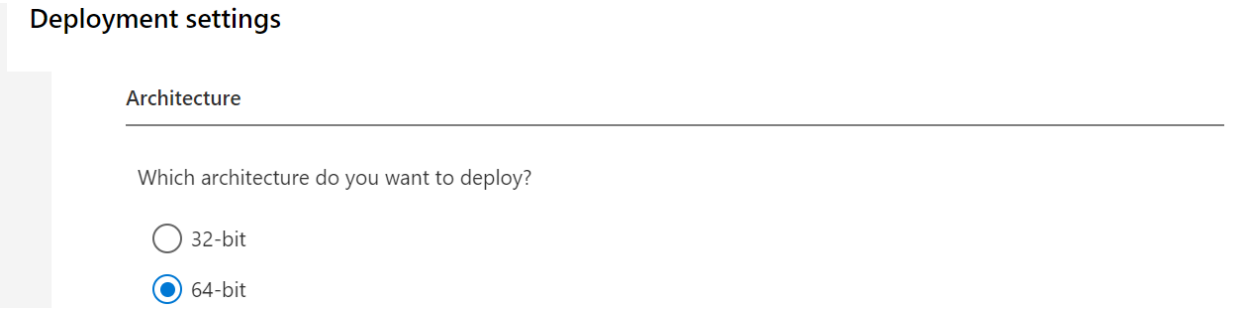
d. Under **App Suite Information,** configure the following and click ok:

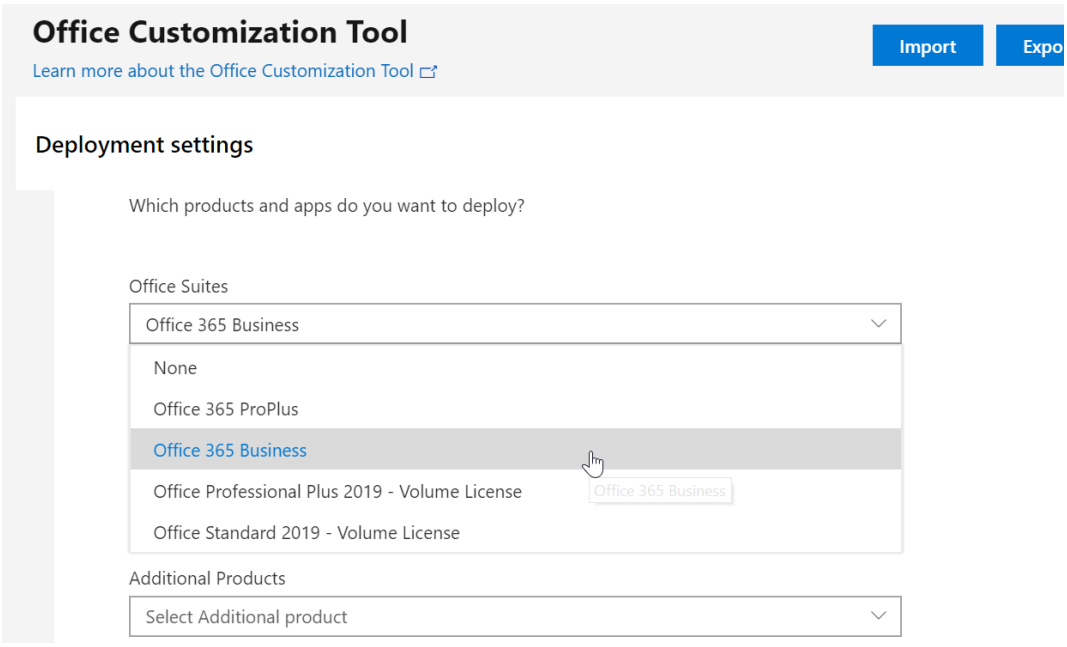


e. Go to https://config.office.com/ and sign in with your admin credentials

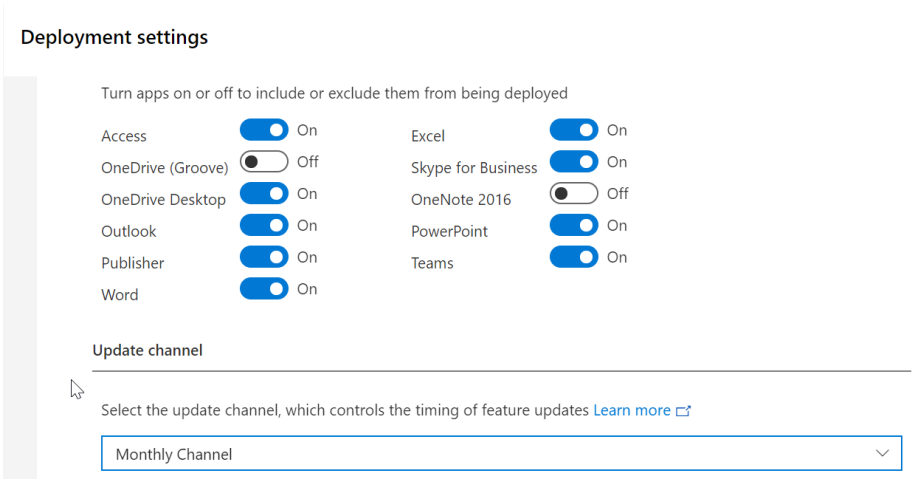


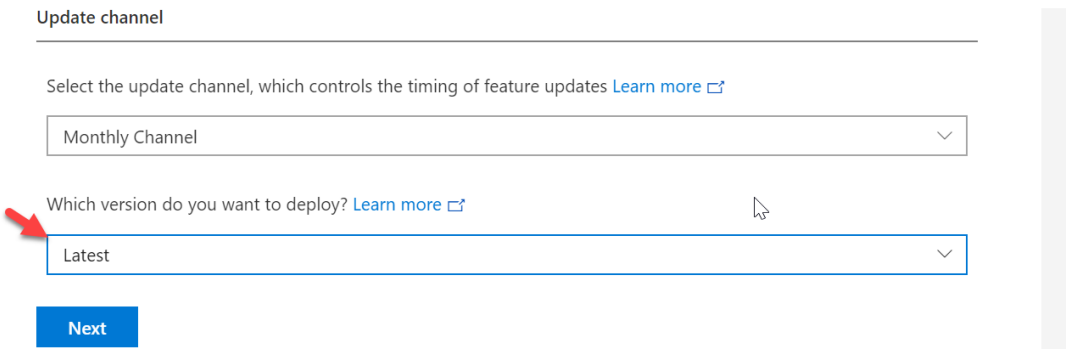
f. Select your appropriate architecture and select **Office 365 Business** from the dropdown:



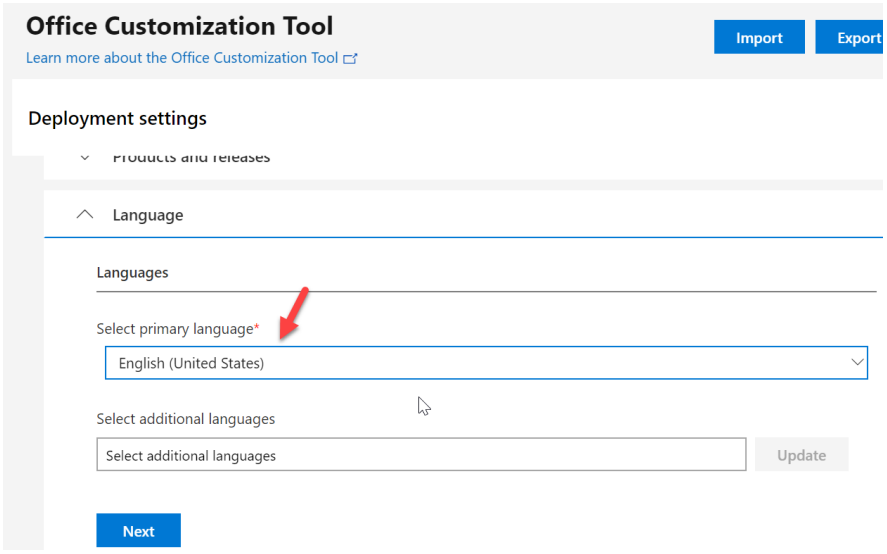


g. De-select any apps you do not want to deploy and choose **Monthly** for the update channel and **Latest** for the version

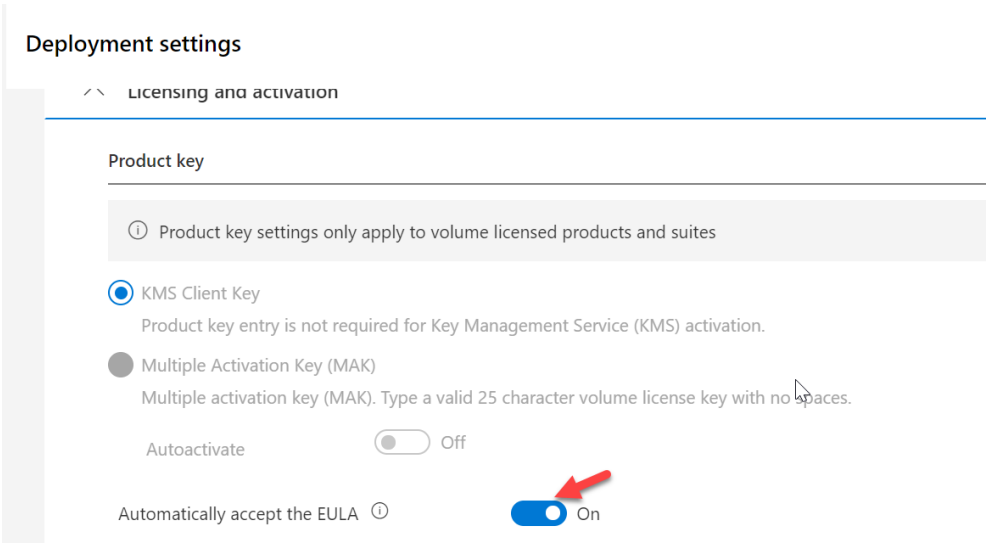




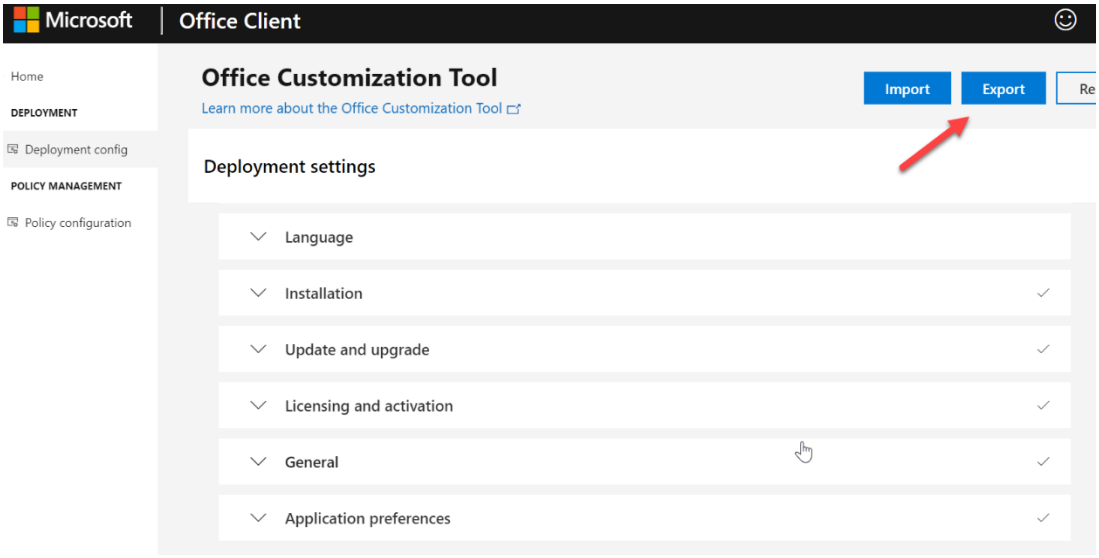
h. Under **Language** select **English** or your primary language



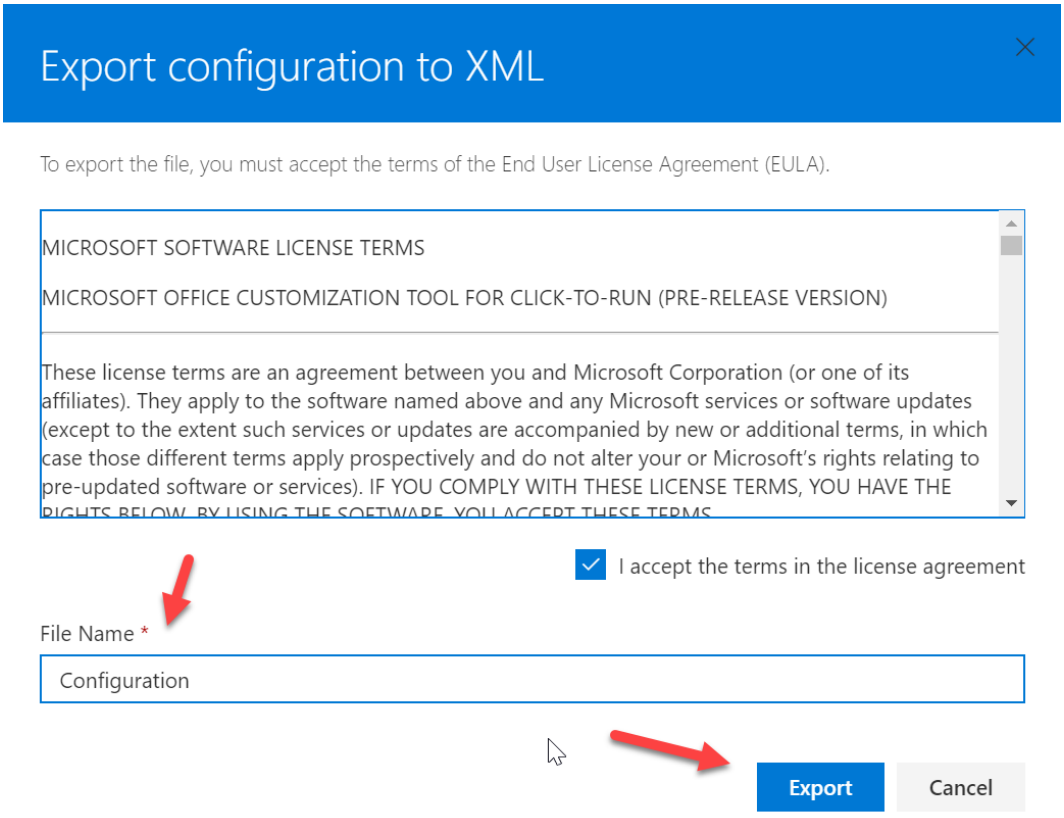
i. Under the **Licensing and Activation** section turn the **Automatically Accept the EULA** to **On**



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

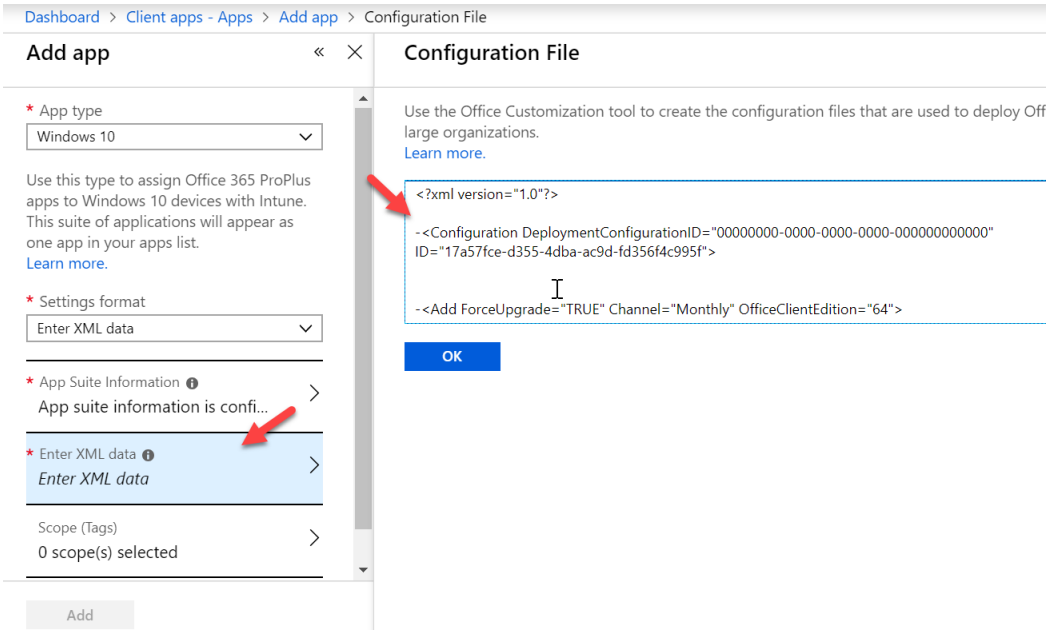


k. Agree to the terms, name your file, and click export

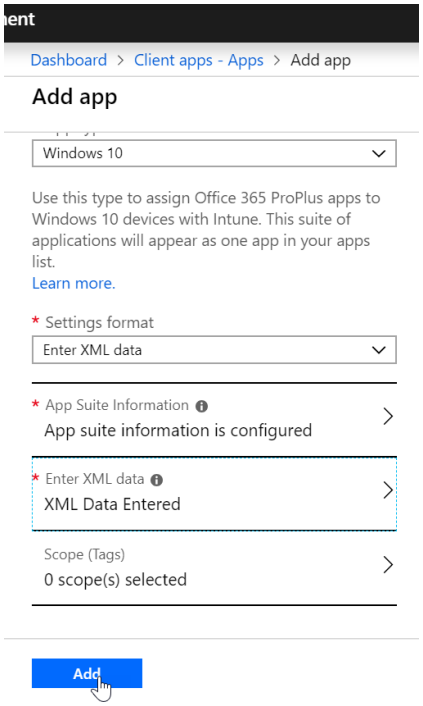


l. Open the XML file and copy the text:

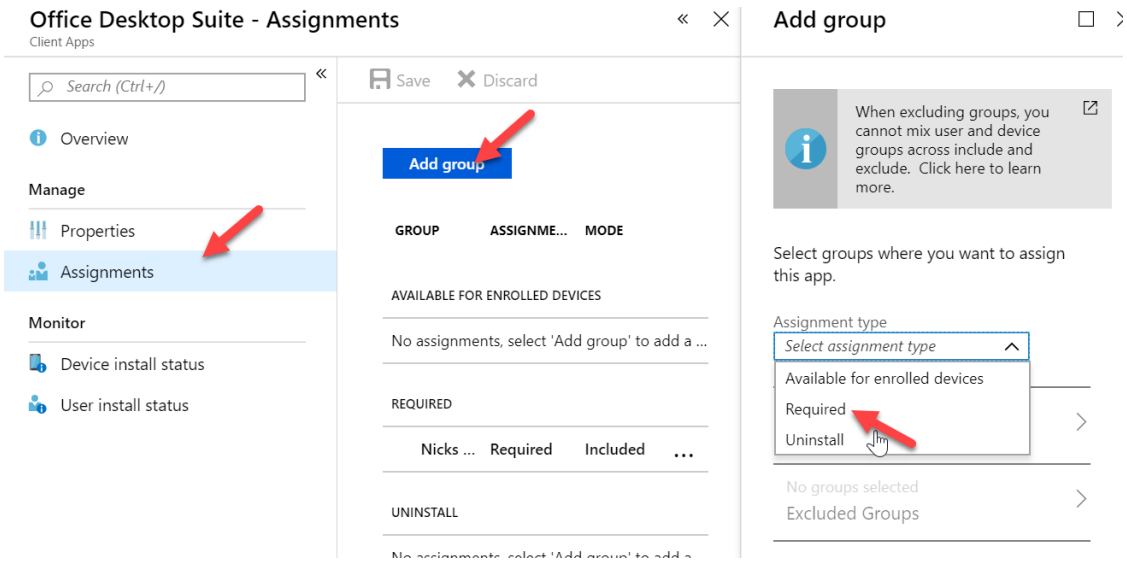
m. Back in the Microsoft portal, click **Enter XML Data**, paste the text, and click ok



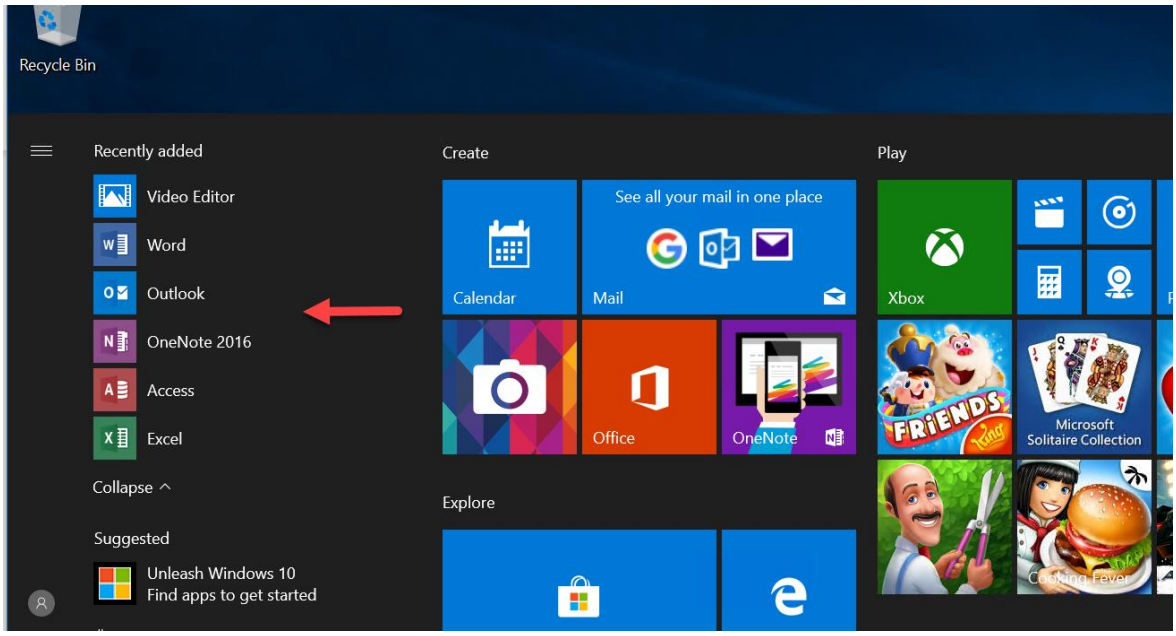
n. Click **Add**



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



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

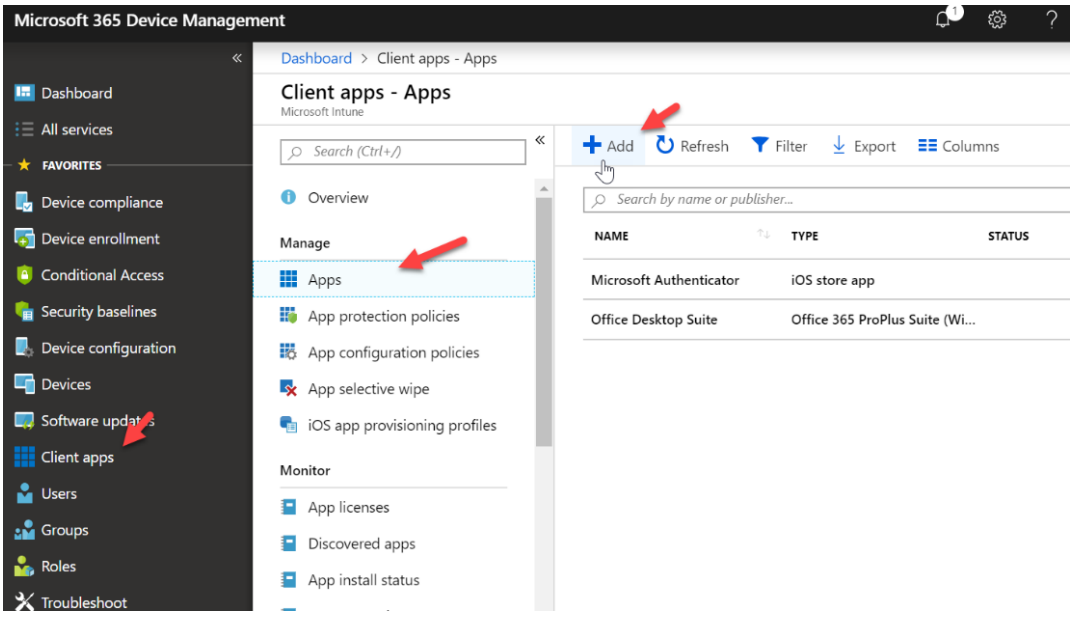


Adding the Microsoft Authenticator App

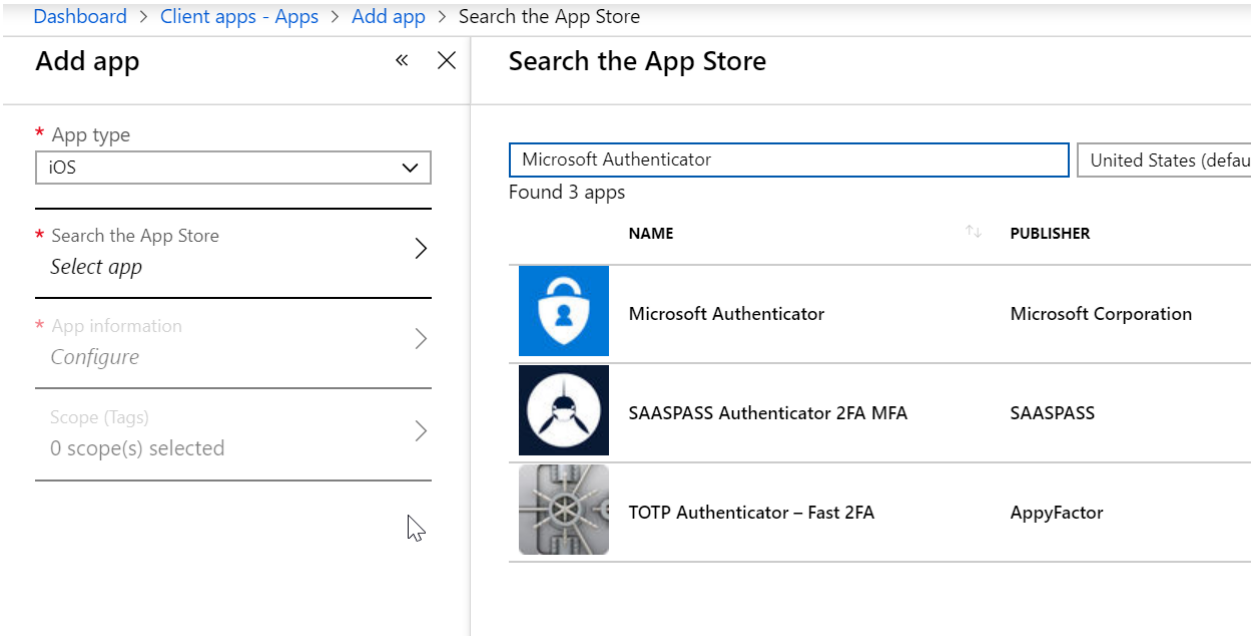
The Microsoft Authenticator app is widely using for MFA that comes with M365 Business. You can add this app in Intune so that it is immediately available for download for your clients.

iOS

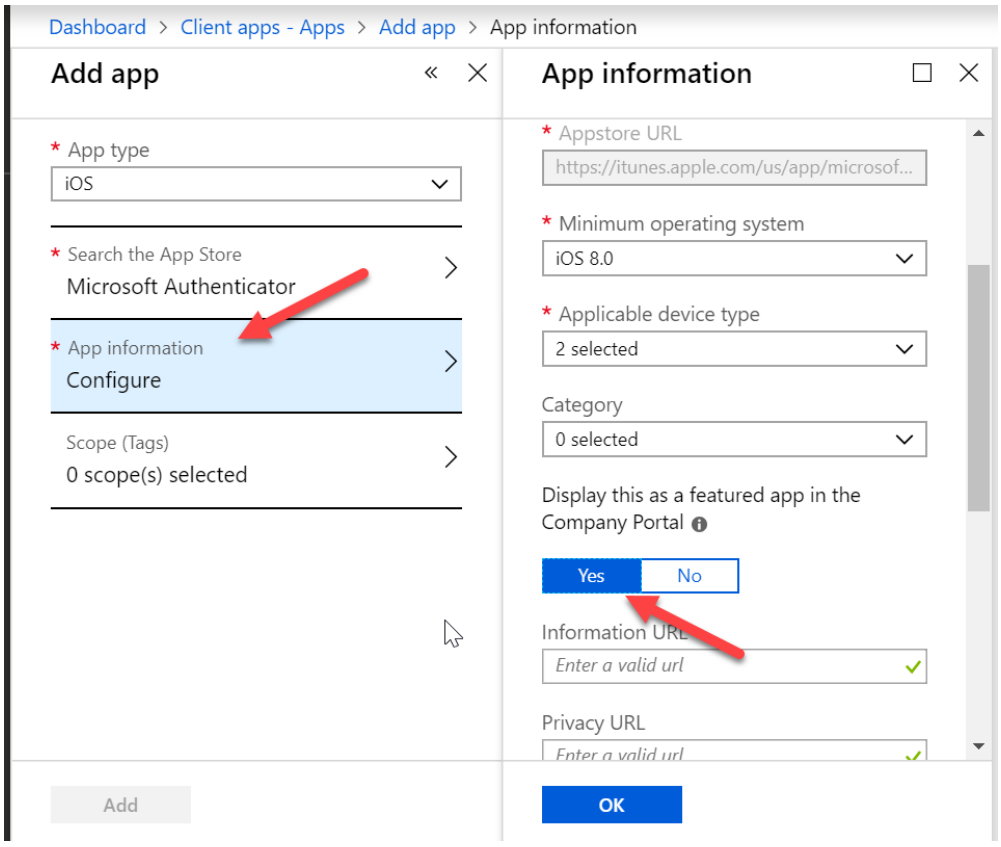
a. In the Device Management Admin center go to **Client Apps>Apps>Add**



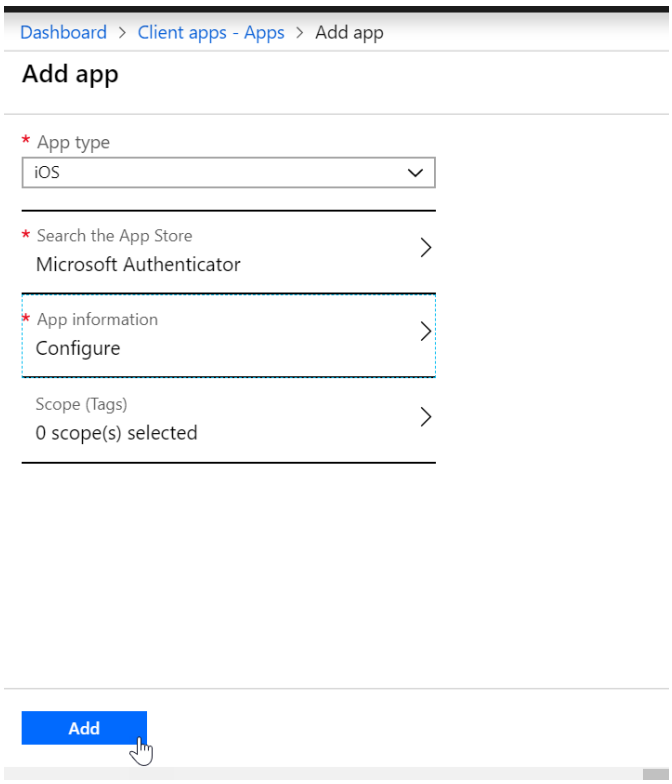
b. Under App Type select **iOS**, then click **Select App,** then search for **Microsoft Authenticator** *NOTE* You will have to search for this text in its entirety for it to find this app:



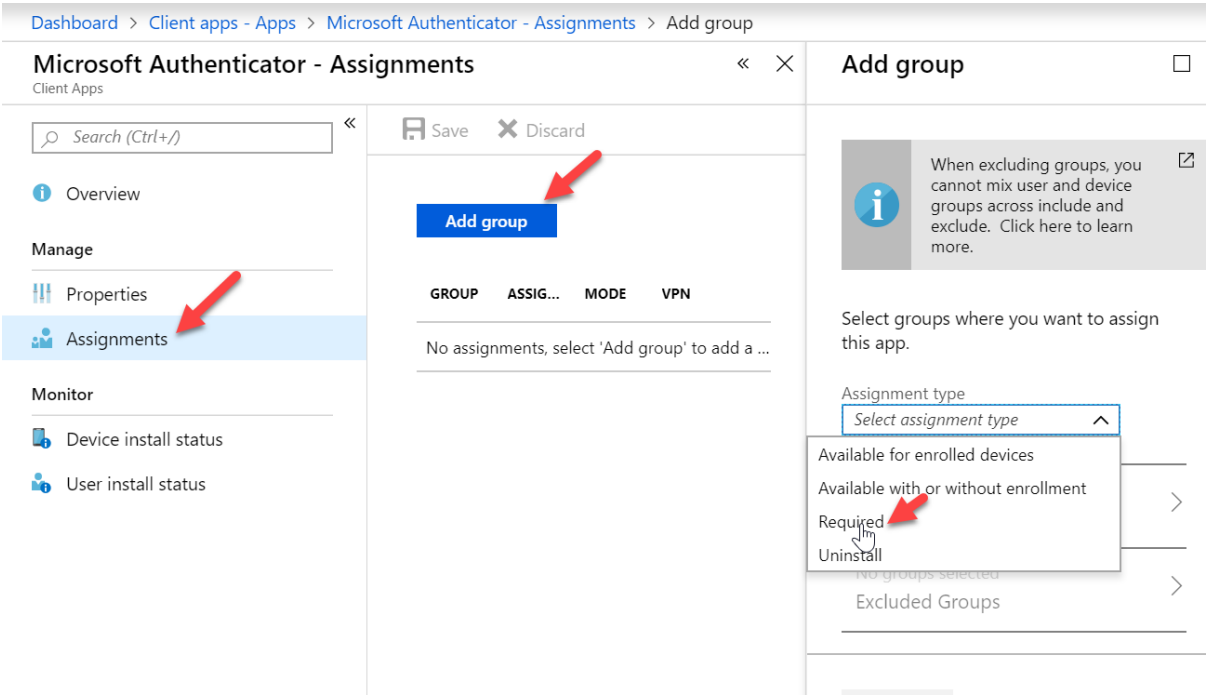
c. Select the app and click **Configure** under App Information. Say **Yes** for displaying app in Company Portal. Leave all other settings defaulted:



d. Click Add

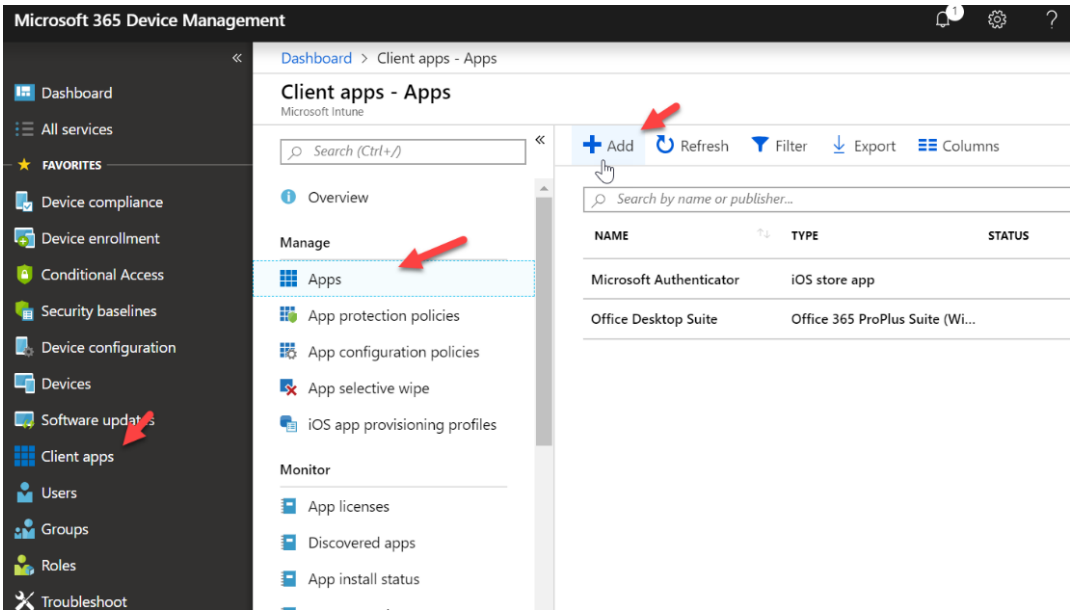


e. Click **Assignments>Add Group>Select Required** for Assignment Type. Save when complete



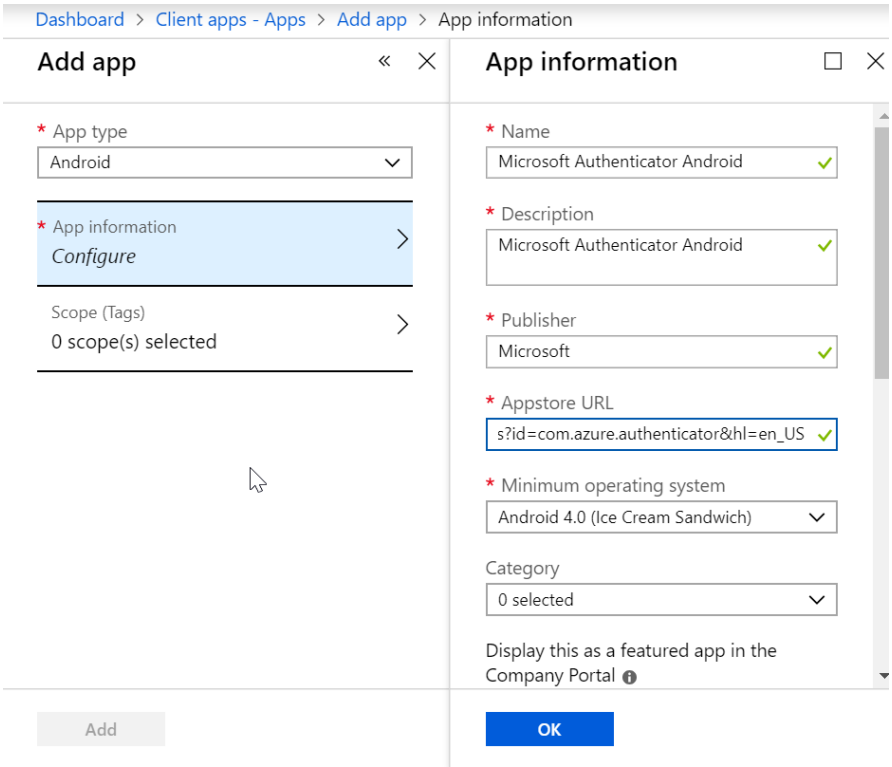
Android

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



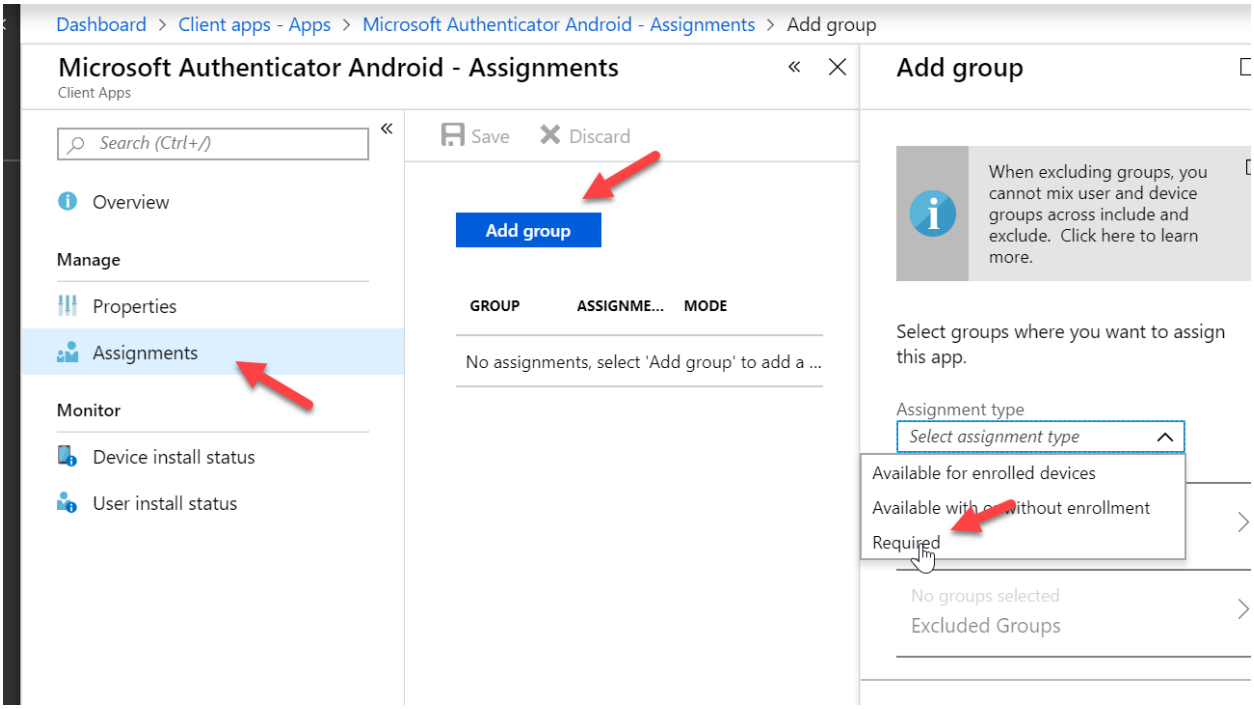
b. For App Type, select **Android** and fill out the fields as follows, including the following for AppStore URL:

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



c. Click **Add**

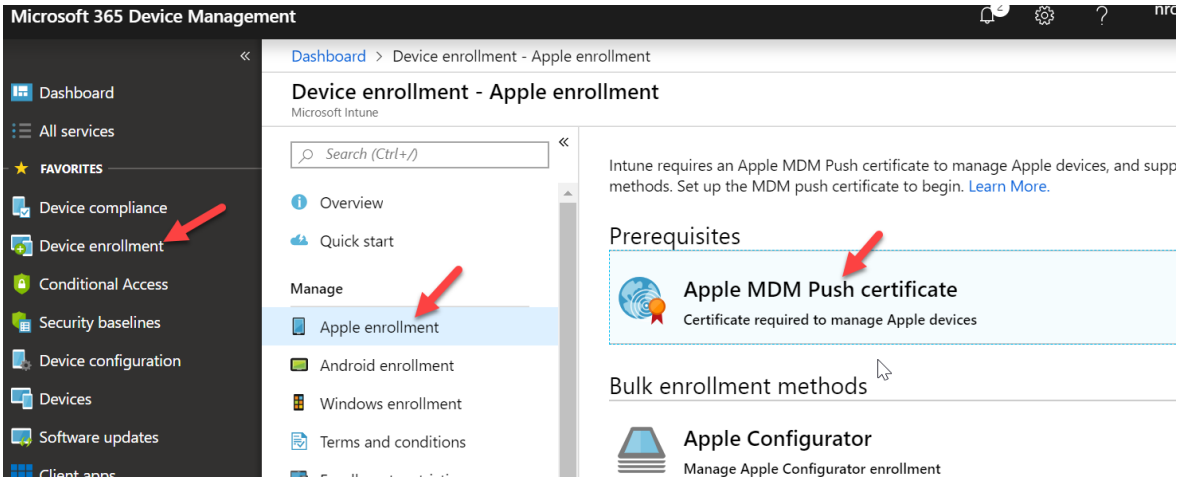
d. Click **Assignments>Add Group>Select Required** for Assignment Type. Save when complete



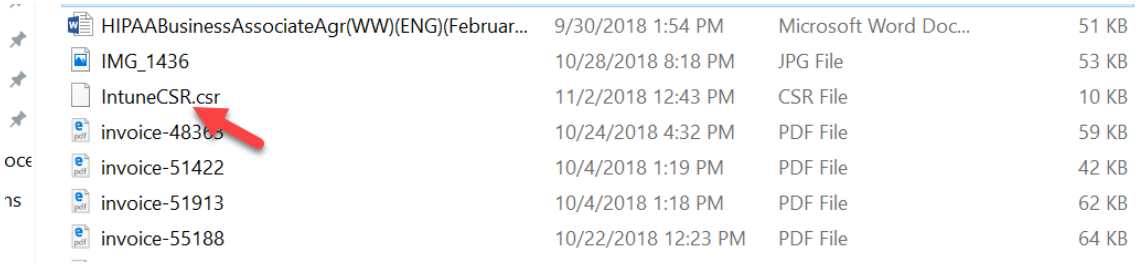
Set up Apple MDM Push Certificate

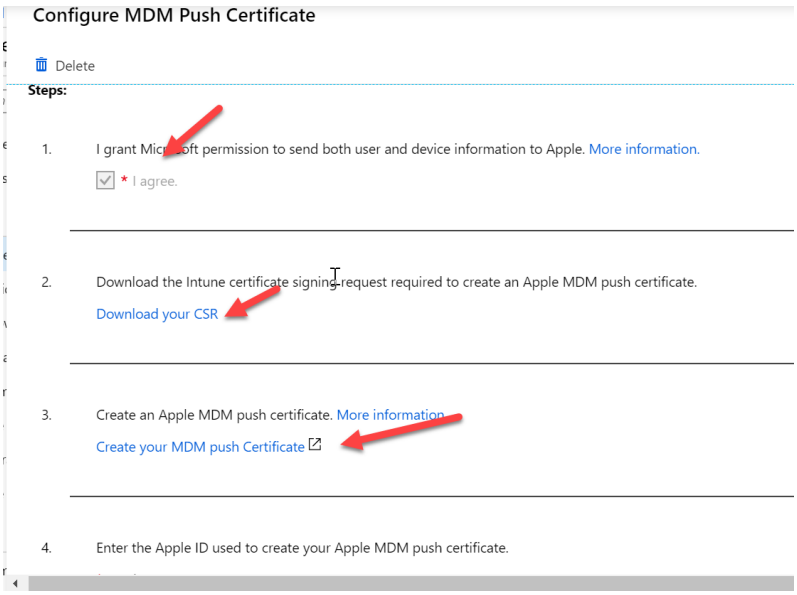
The Apple MDM Push Certificate allows us to start enrolling iOS devices. You can think of this cert as a shell account in which you can put all over your customers under. The certificate is associated with the Apple ID used to create it. As a best practice, use a company Apple ID for management tasks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

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

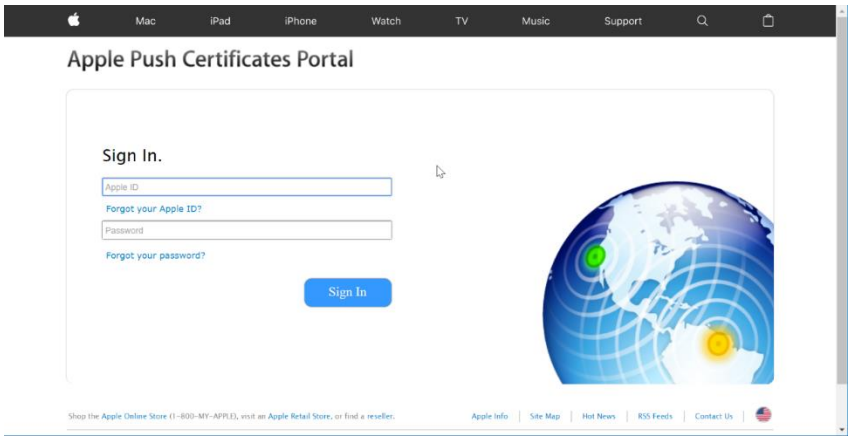


b. Agree to the terms and conditions, Download you CSR (save to another location or keep in downloads. The file is used to request a trust relationship certificate from the Apple Push Certificates Portal.), and click **Create your MDM Push Certificate** to open the Apple center

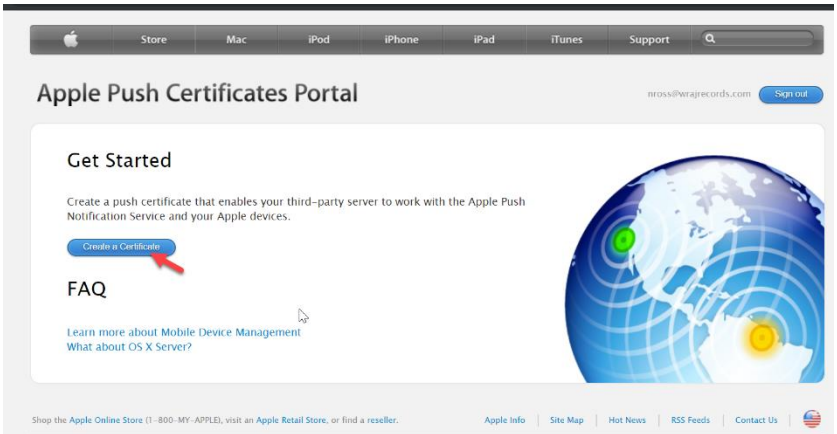




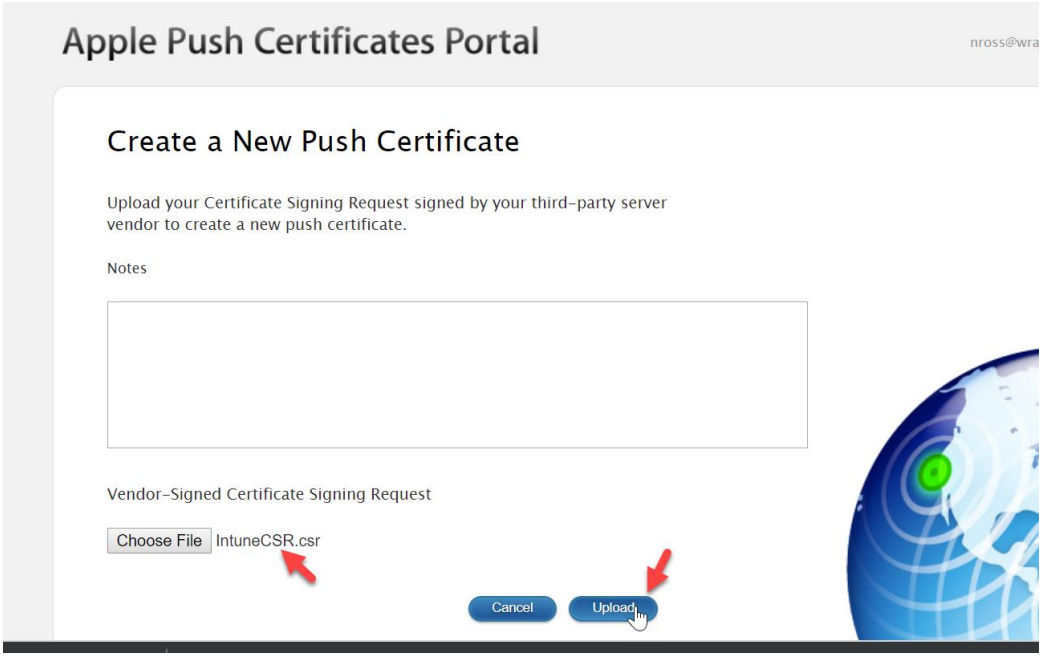
c. Sign in with your Business Apple ID or create a new Apple account for your business if you do not have one already. (takes 5 min and no financial commitment)

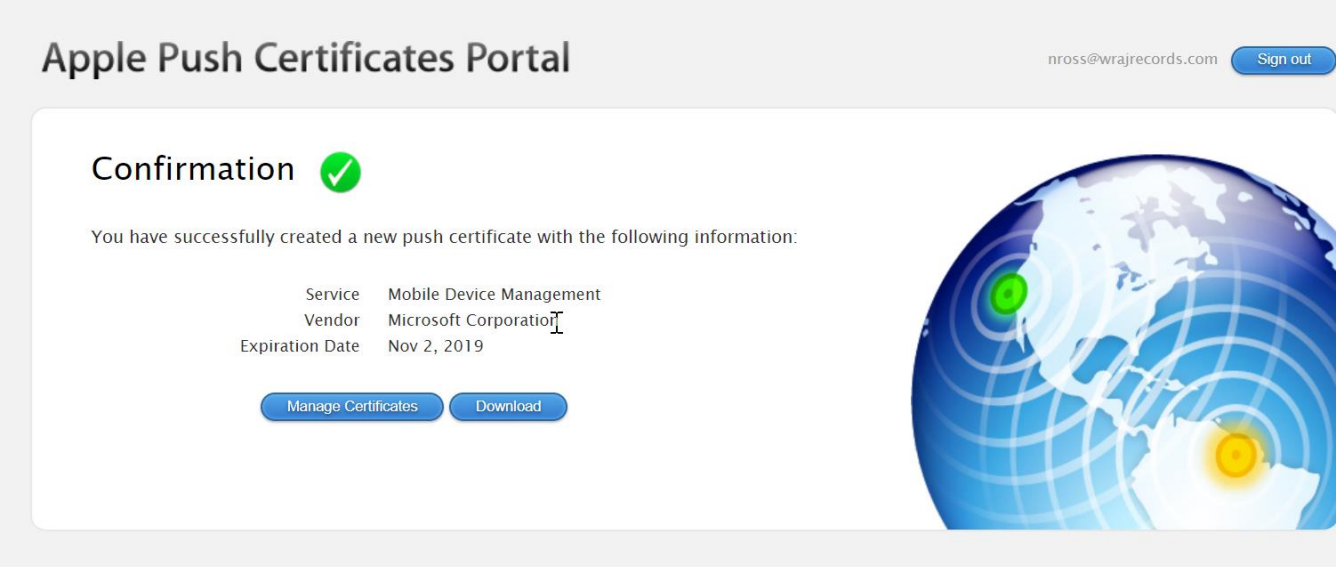


d. After you sign in click Create Certificate

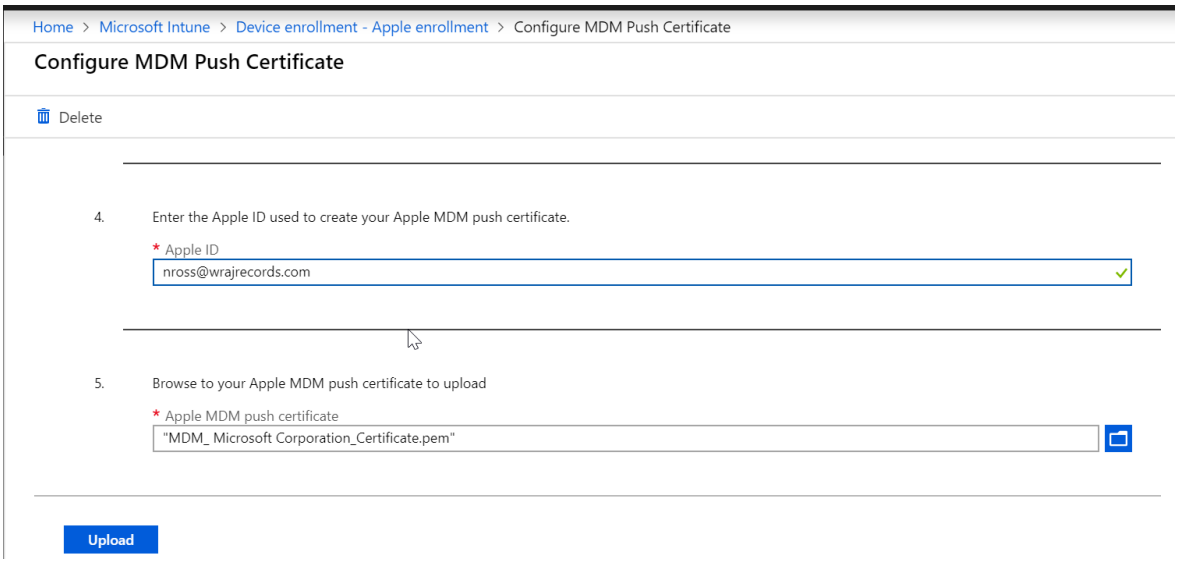


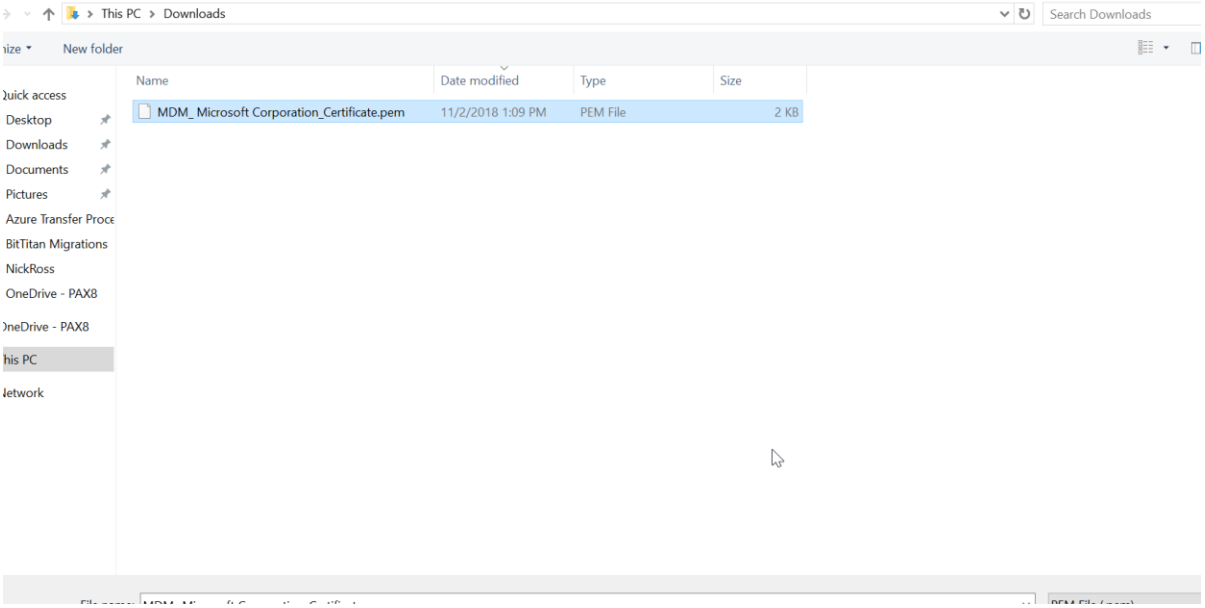
a. Upload your CSR file and then Download the MDM Push Certificate



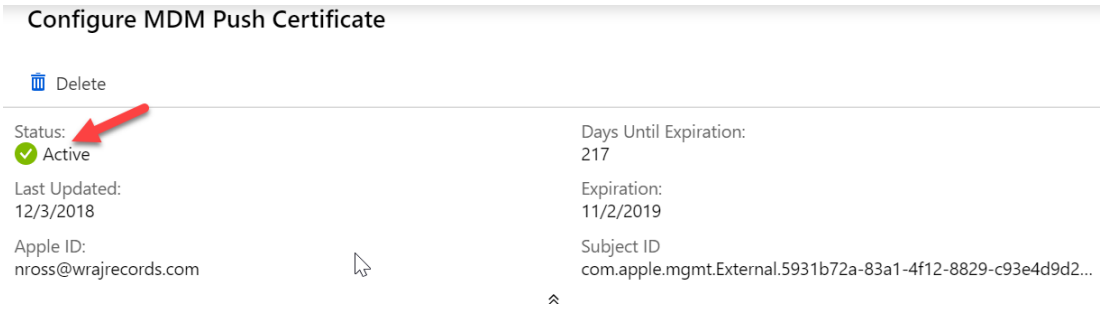


e. Back in Microsoft enter you Apple ID and upload the MDM Cert you just downloaded





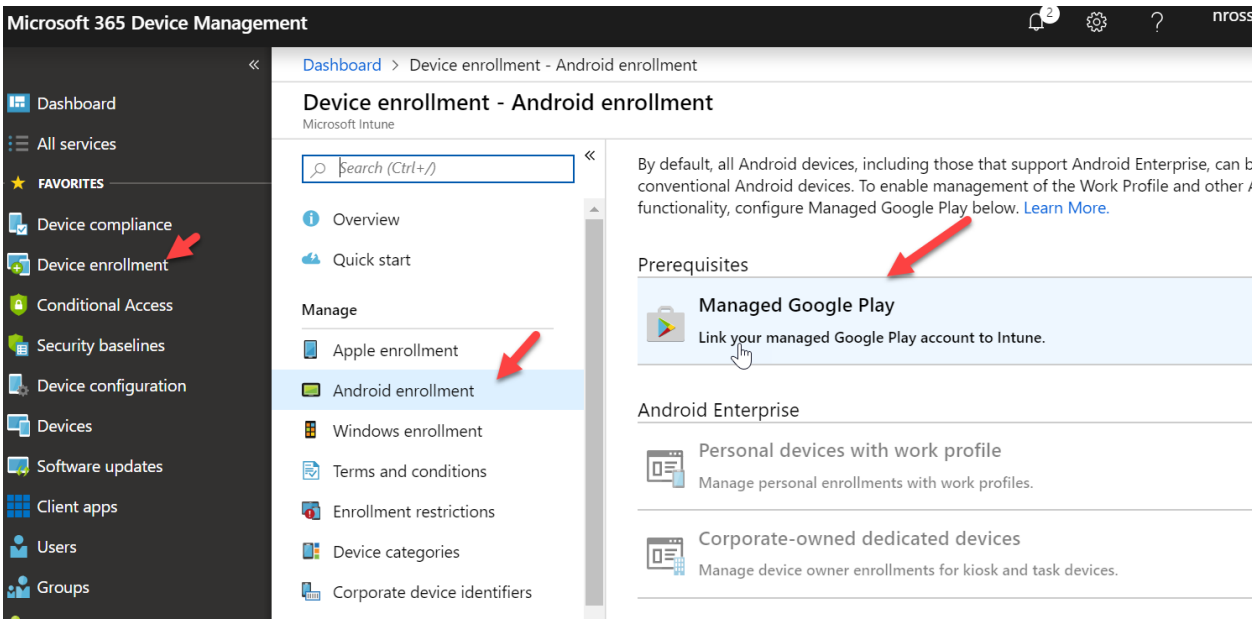
f. You will see the status as active



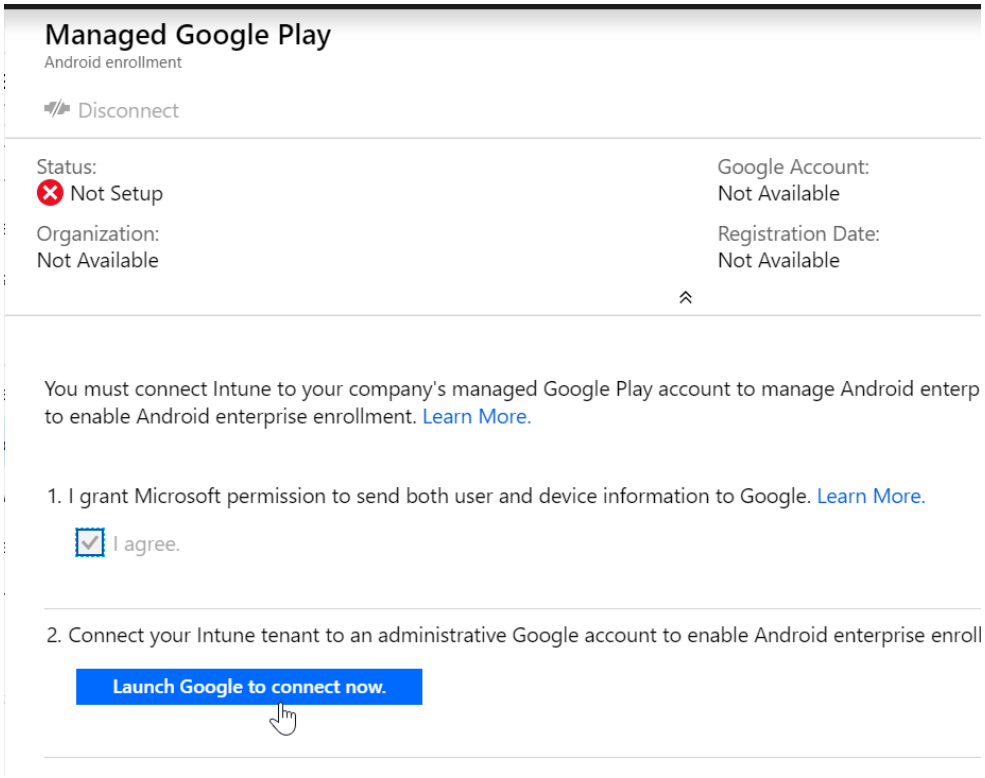
Setting Up Android Enrollment

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.

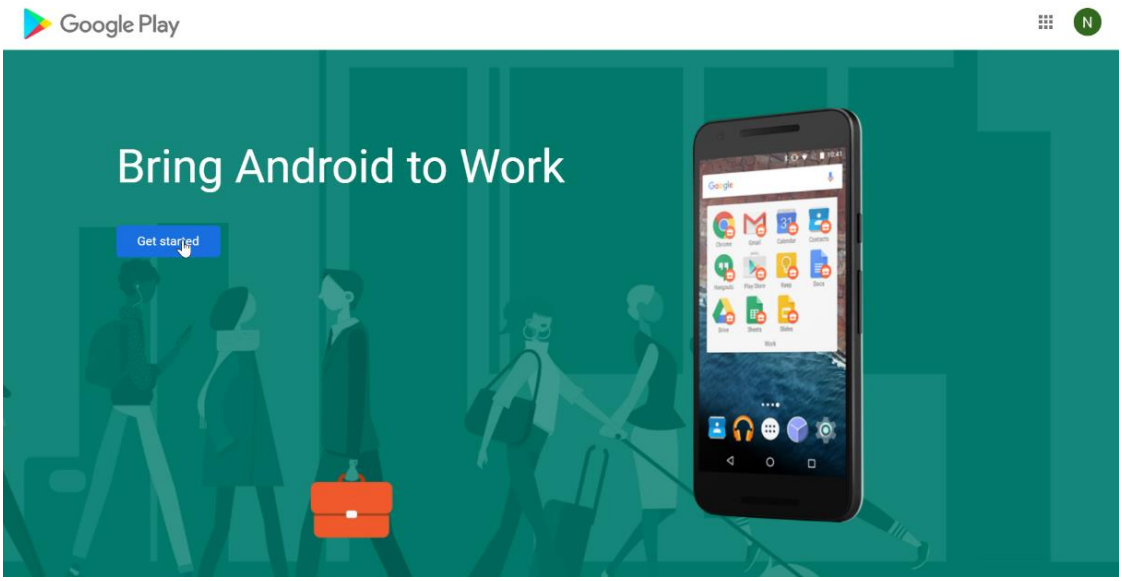
a. In the Device Management Admin Portal, go to **Device Enrollment>Android Enrollment>Managed Google Play**



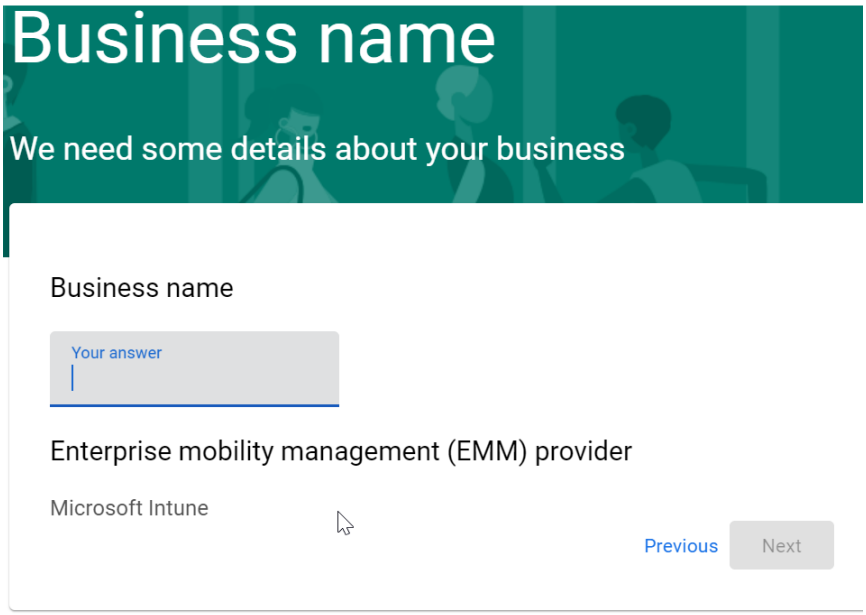
b. Agree to the terms and conditions and click **Launch Google to Connect now**



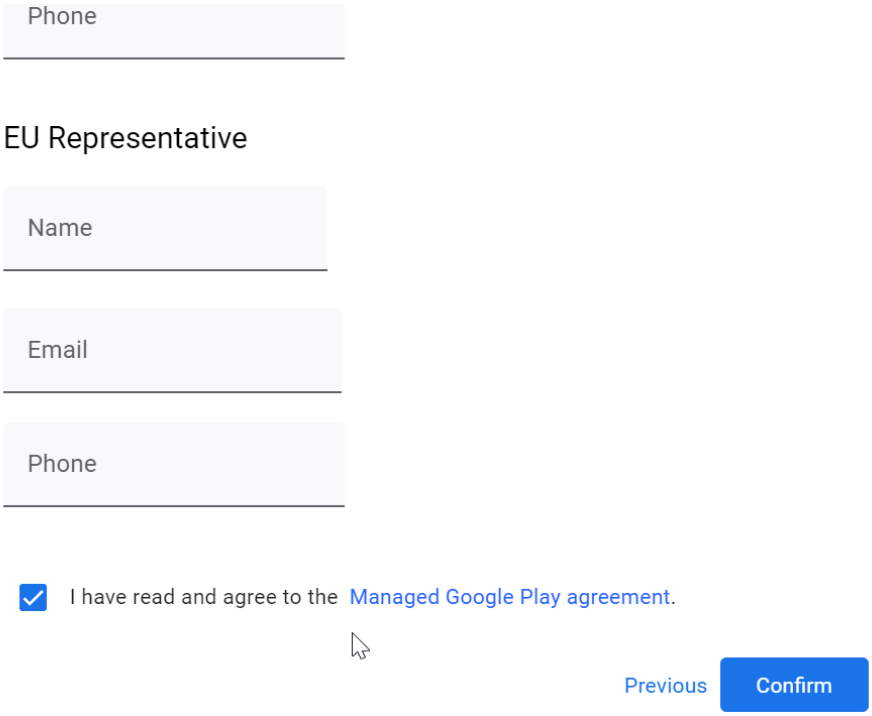
c. Sign in to your business Google Account. If you do not have one Create one now. Click Get Started:



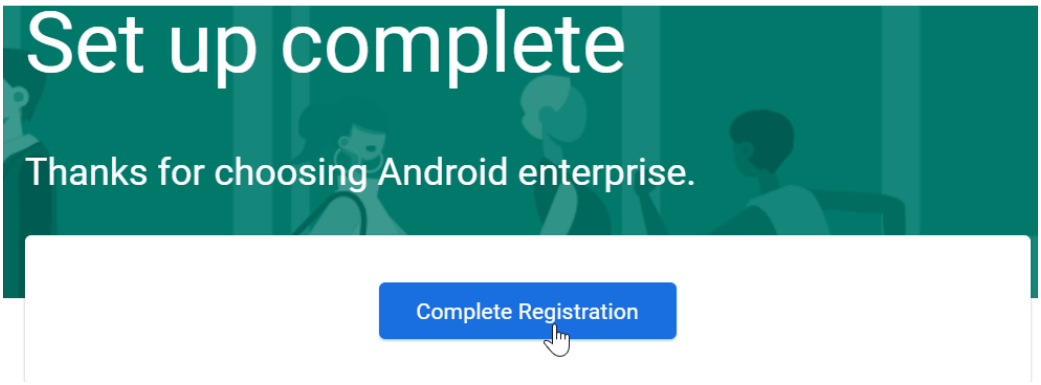
d. Enter your Business Name and click Next



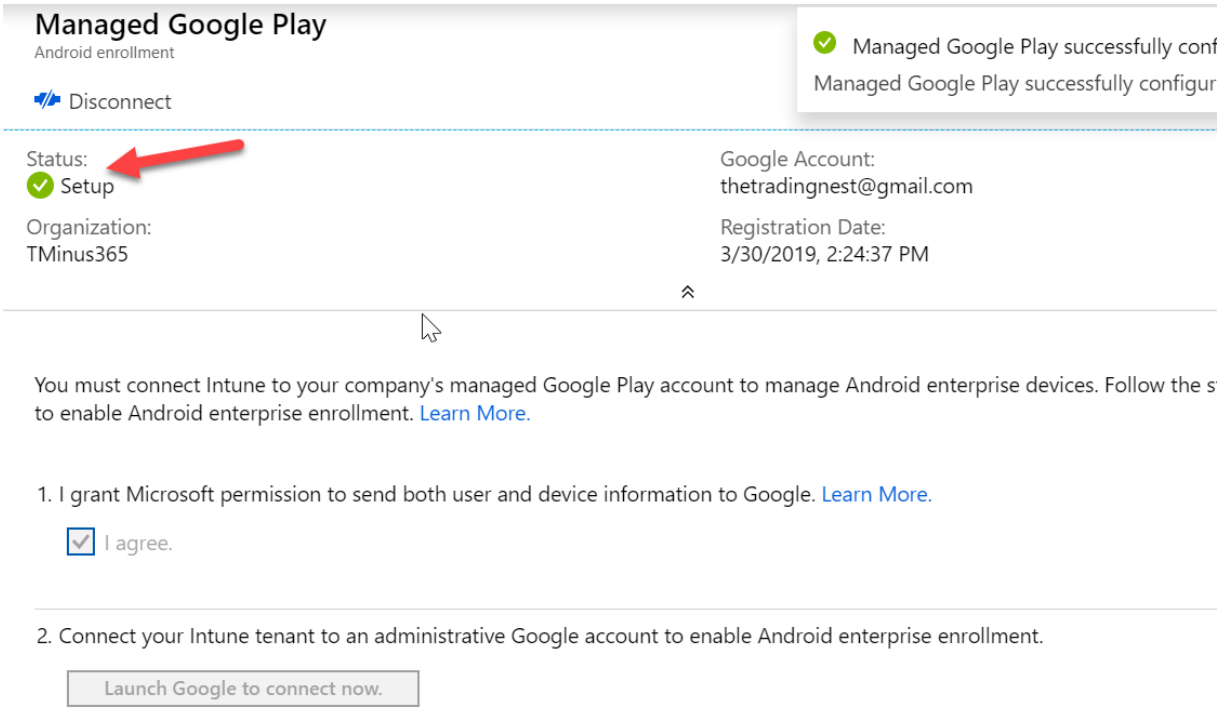
e. If you are in the EU, you can enter the contact of an EU representative. If not, simply agree to the terms and click confirm:



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.

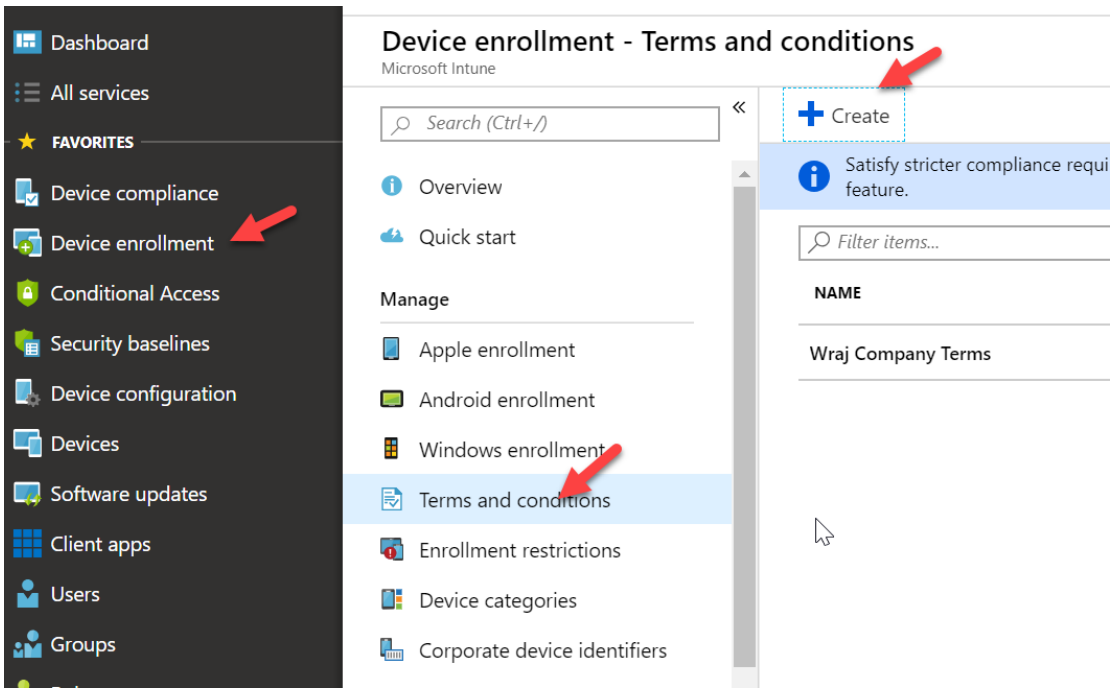


Setting Up Terms and Conditions

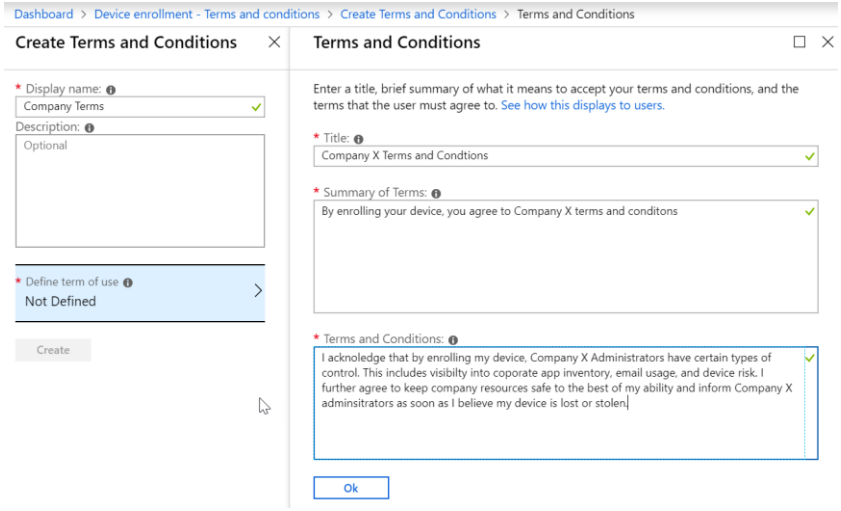
As an Intune admin, you can require that users accept your company's terms and conditions before using the Company Portal to:

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

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



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



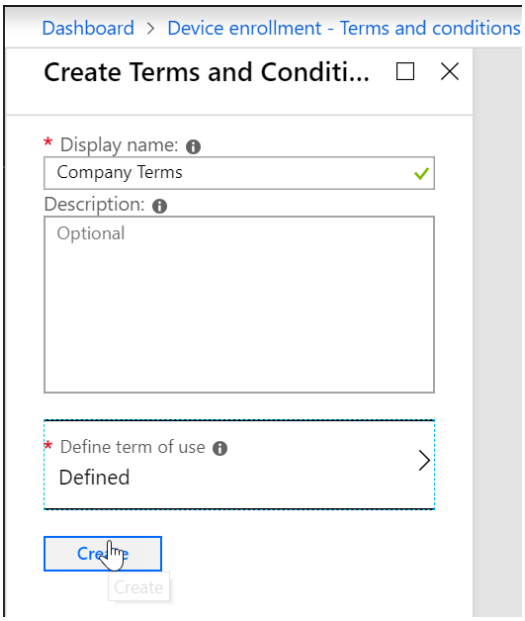
Ex. Summary of Terms

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

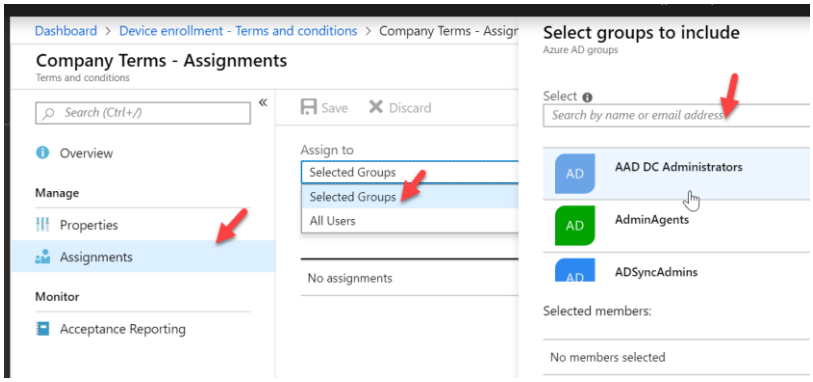
Ex. Terms and Conditions

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**



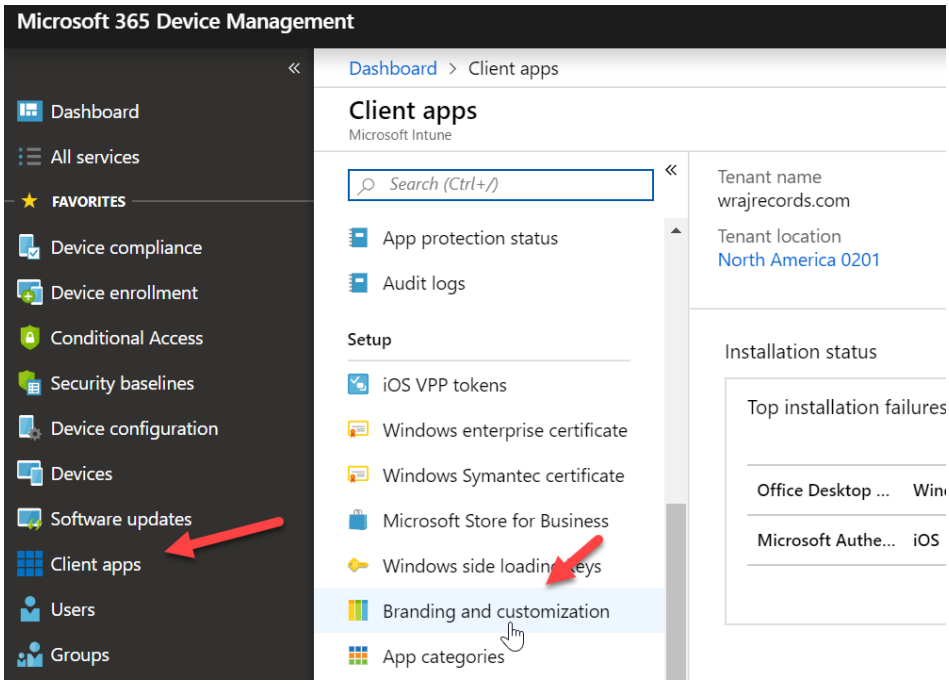
d. Click on the Policy after creation and click **Assignments** to assign the Terms to All Users or a select group:



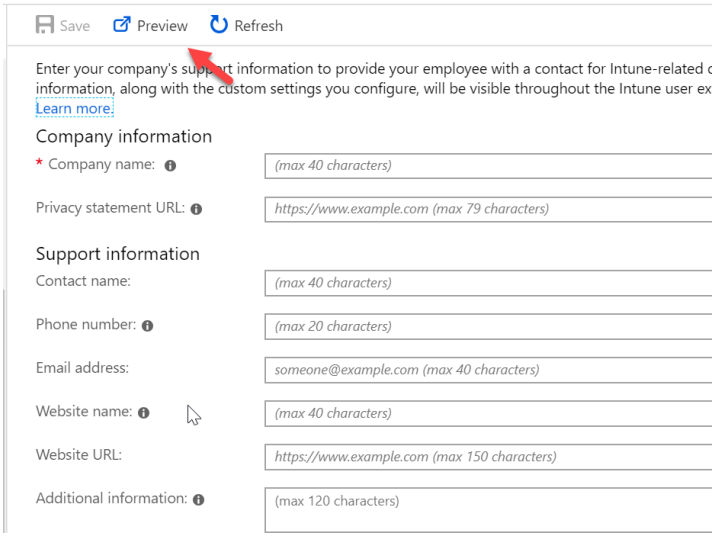
Add Company Branding

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 OOBE for new devices.

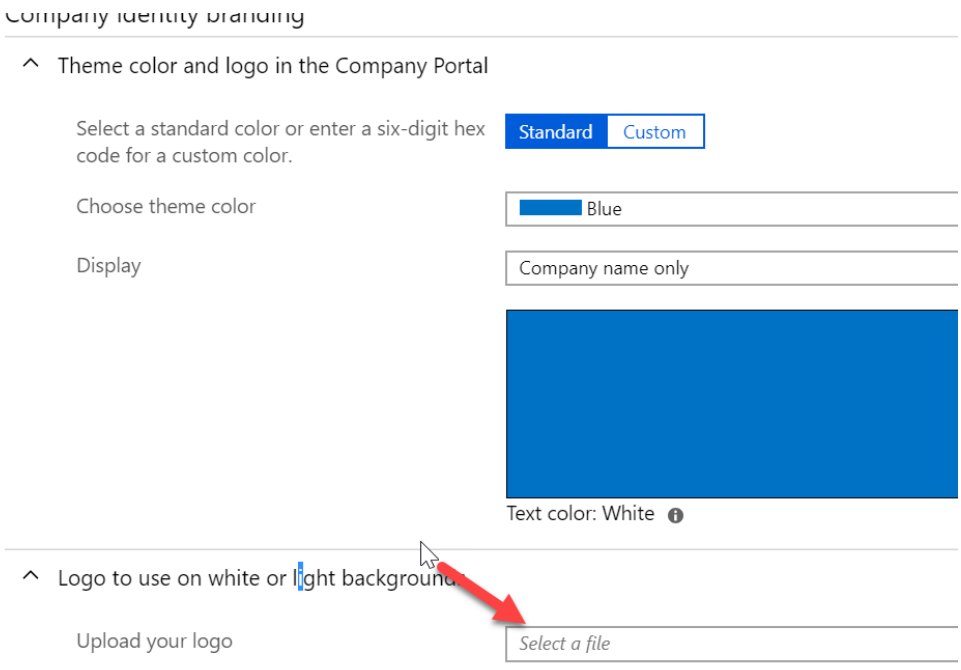
a. In the Device Management Admin portal, go to Client Apps>Branding and customization



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

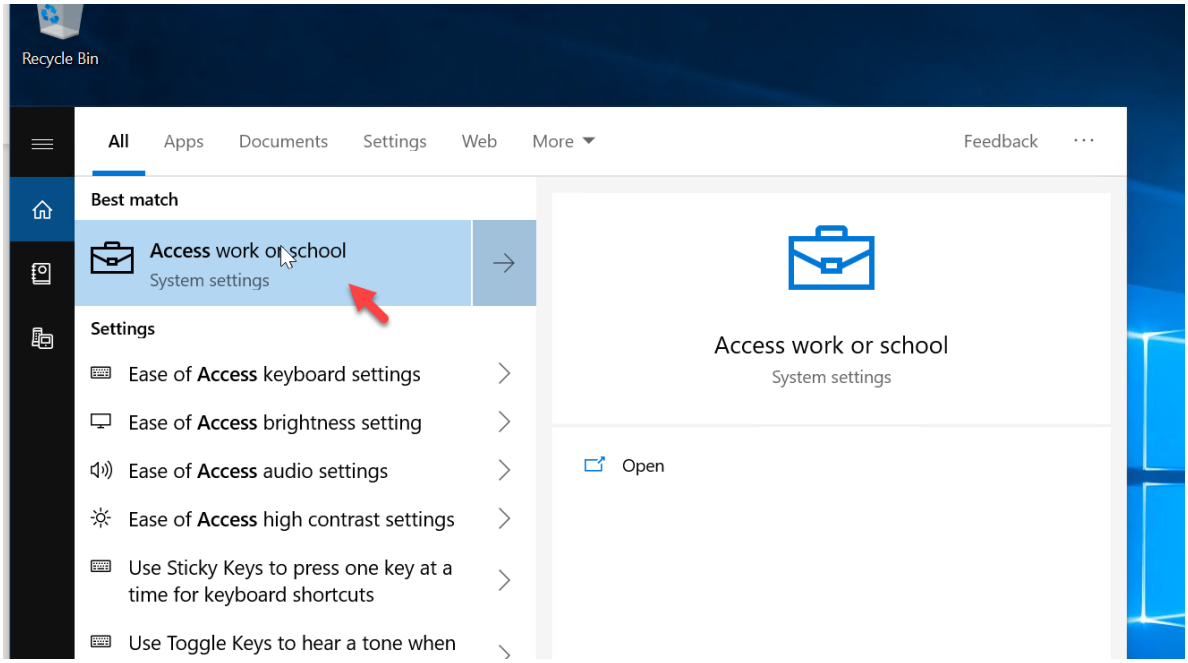


c. Choose your Theme and upload your logo. When done, click **Save**

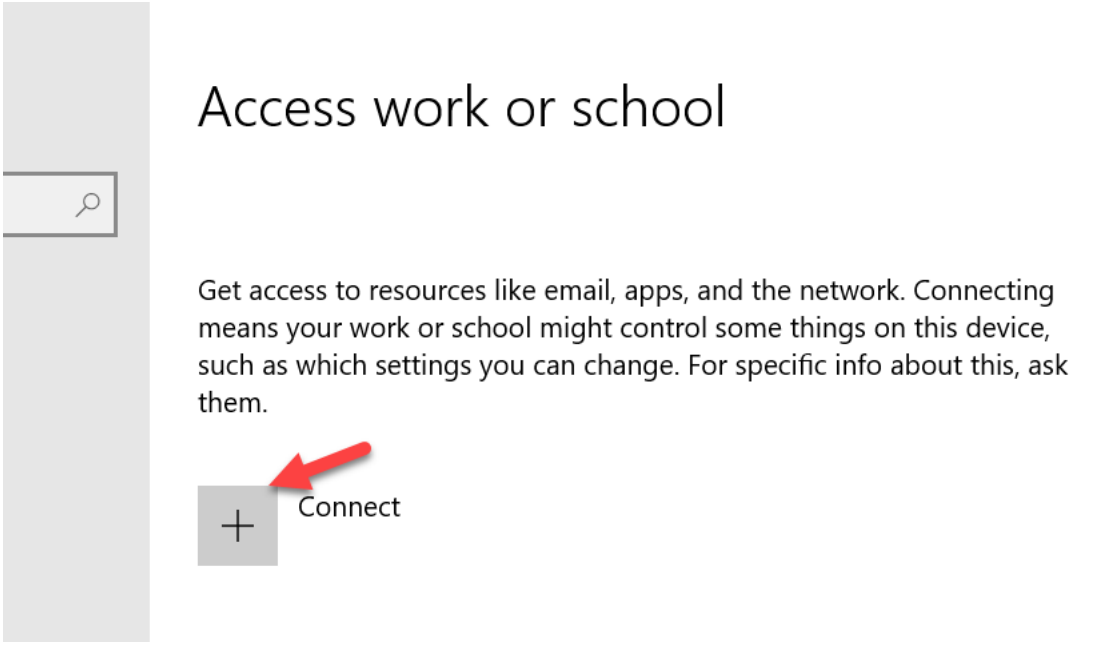


Enroll Devices: Windows

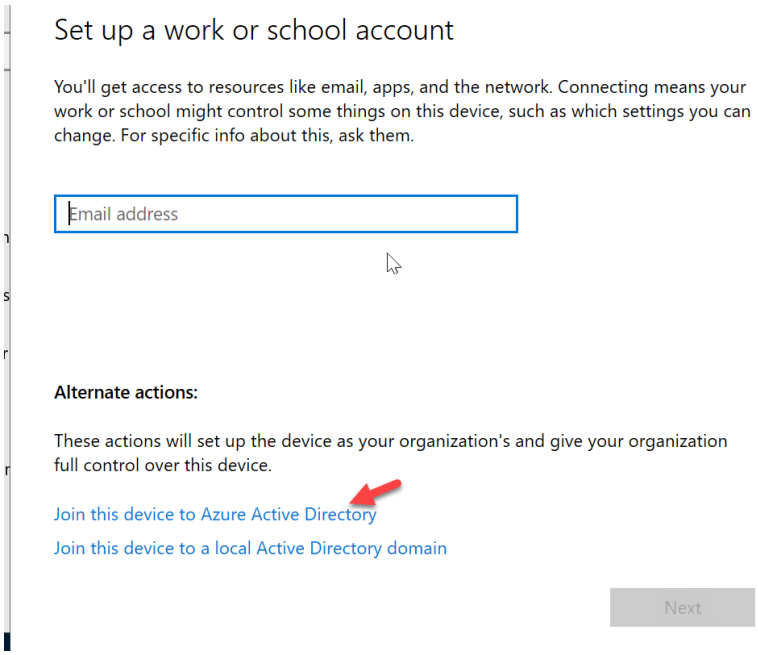
a. On the Windows 10 Device, click Start and type Access Work or School



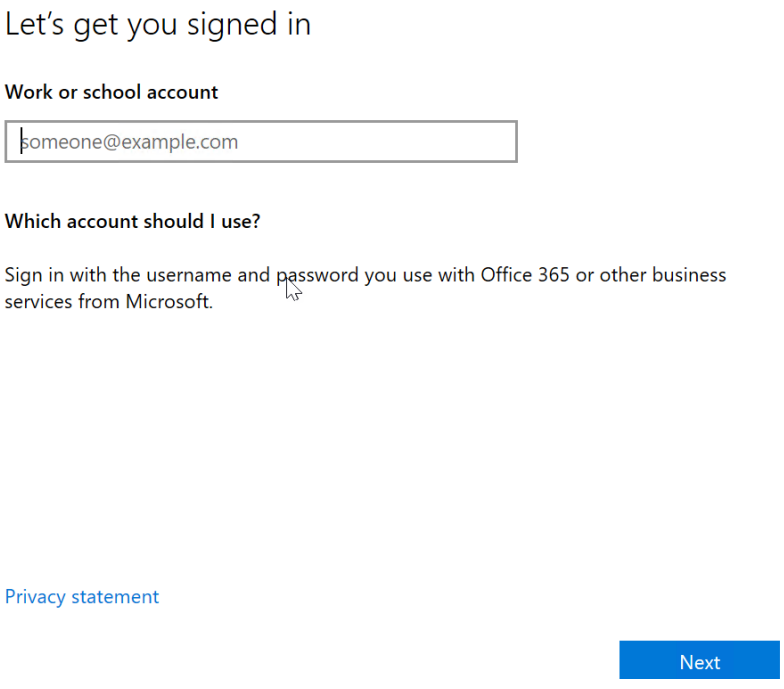
b. Click Connect



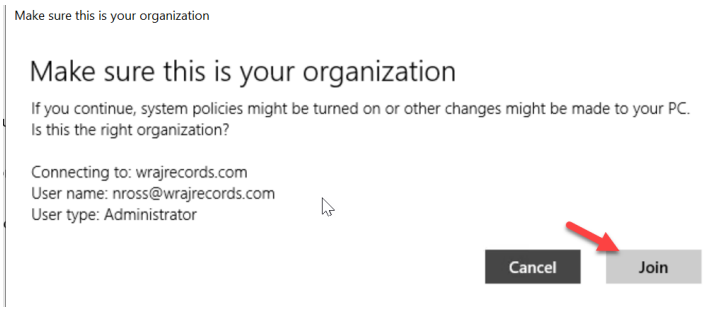
c. Click **Join this device to Azure Active Directory**



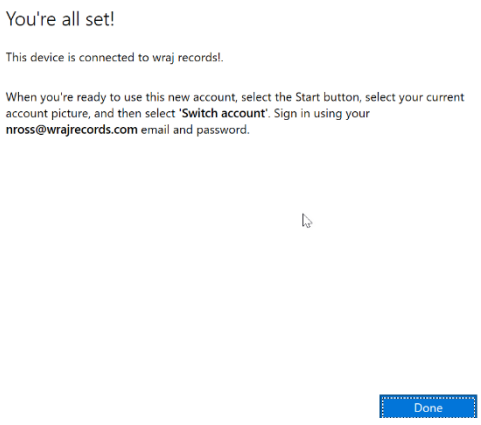
d. Sign-In with the Users Azure AD credentials



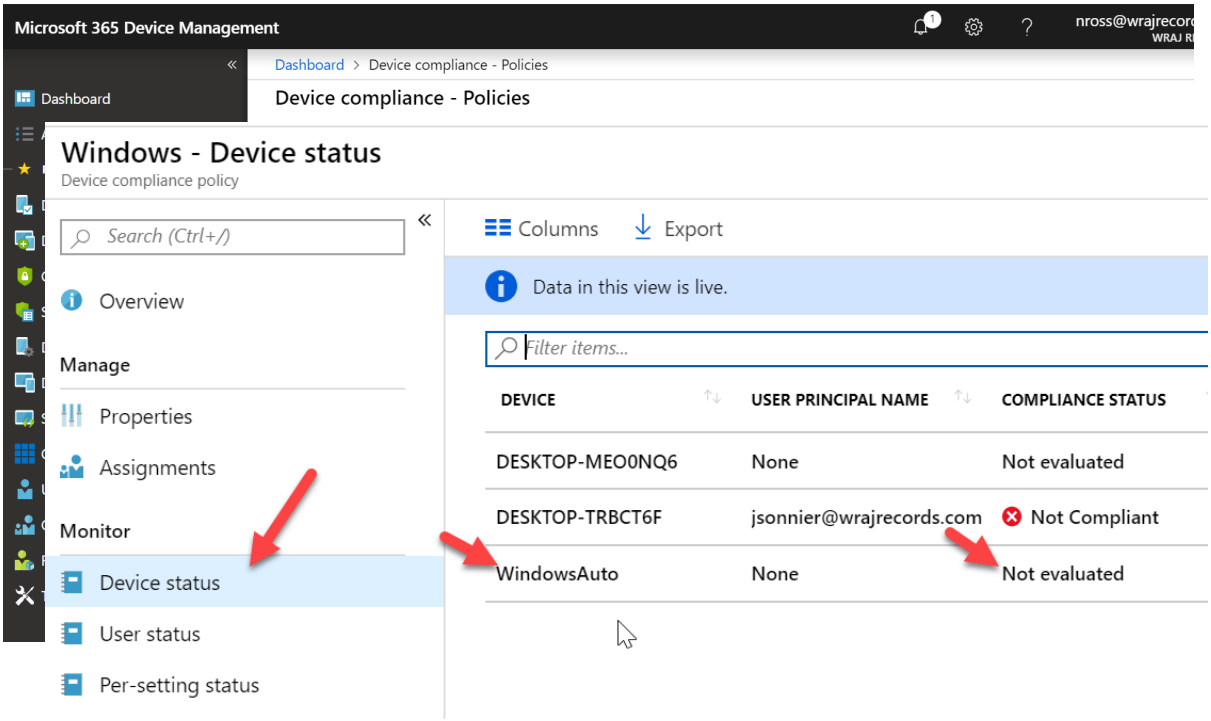
e. When prompted, click **Join**



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



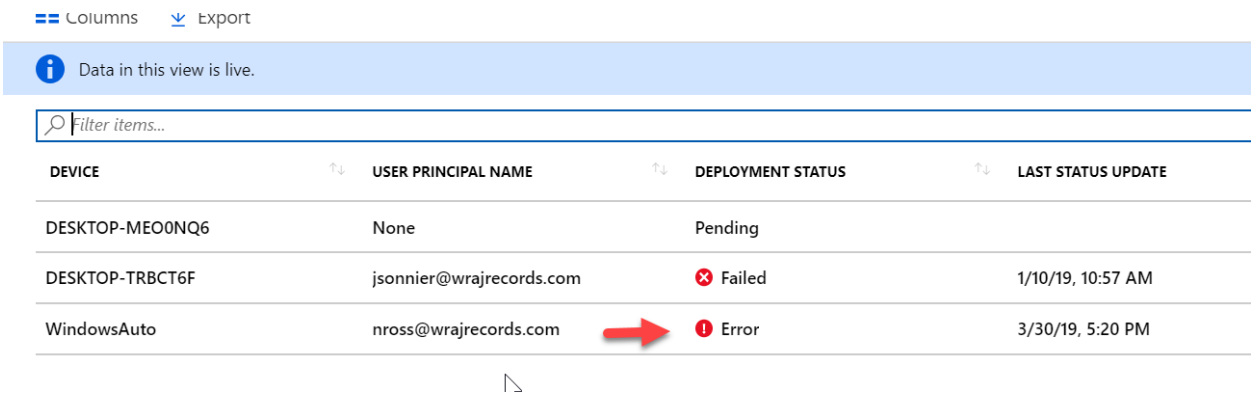
g. Back in the Intune Portal, you can go to **Device Compliance>Policies>Click on your Windows Policy** (we created earlier in this document)



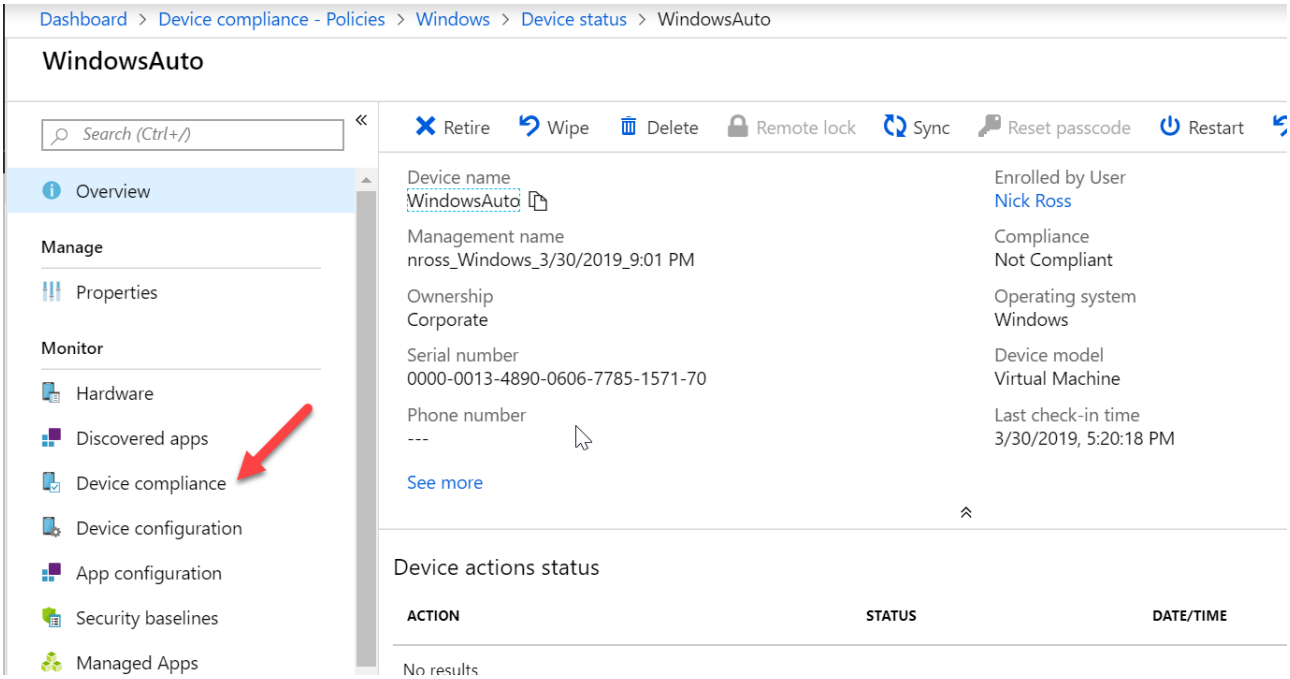
h. You can click on **Device status** to see compliance status. Note, it can take some time before the evaluation will complete. In this case, I see the device I just joined as "Not Evaluated". We just must wait for that to complete.

Monitoring

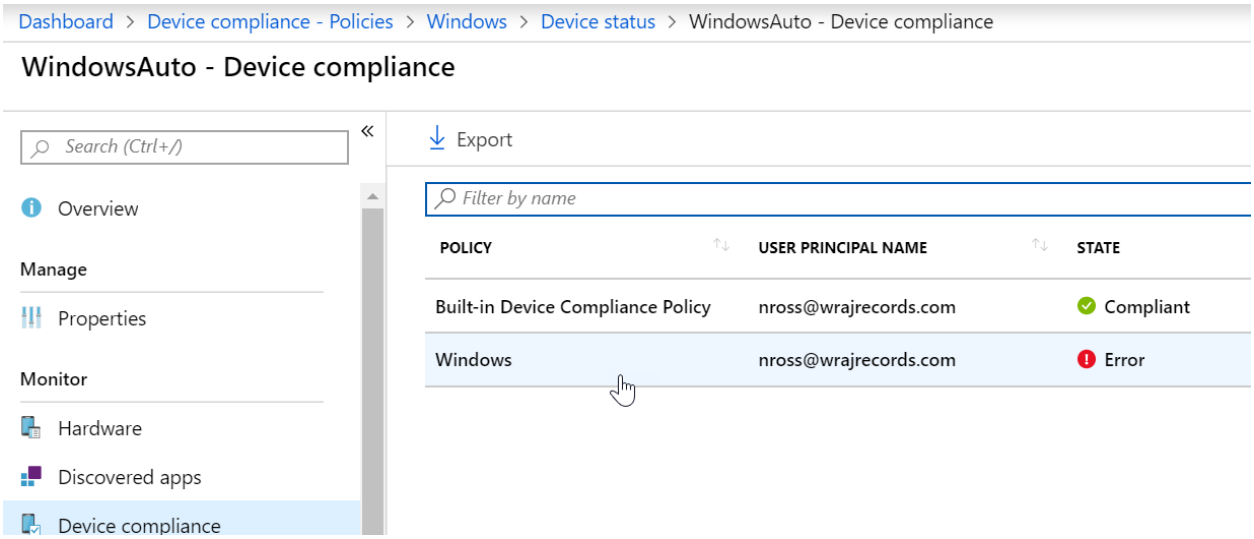
I can come back in later to see that it is in error:



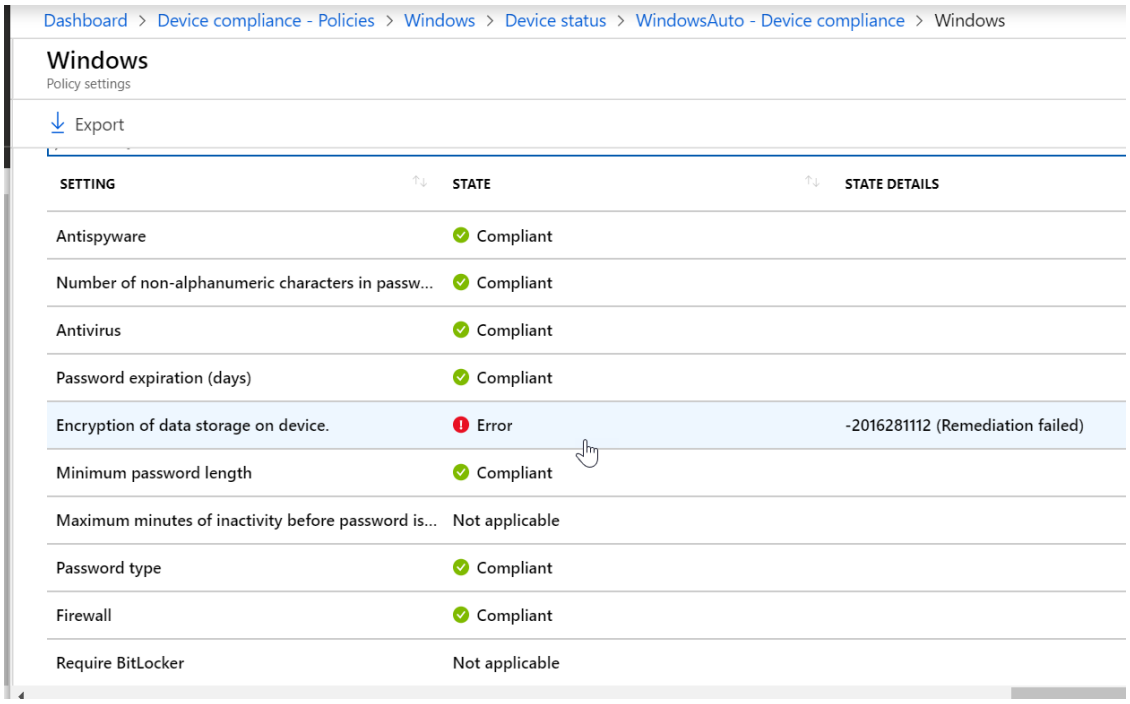
a. Click on this line item and the go to **Device Compliance** on the next page:



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

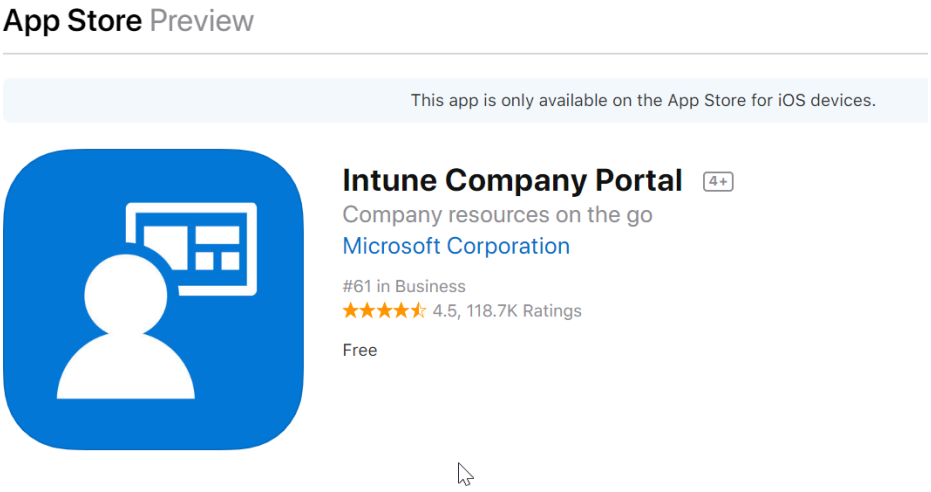


c. Here you can see why the device is out of compliance and take action steps to remediate. In this case it looks like we just need to finish setting up BitLocker to encrypt the drive:

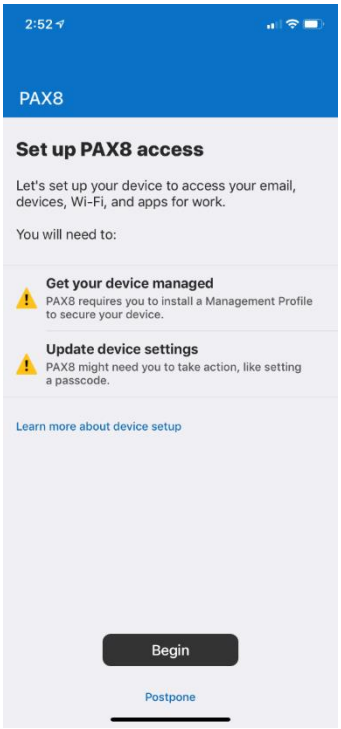


Enroll Devices: iOS and Android

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



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



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

   iOS

   Android

Pilot Testing and Remediation

During our Pilot we want to discover:

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

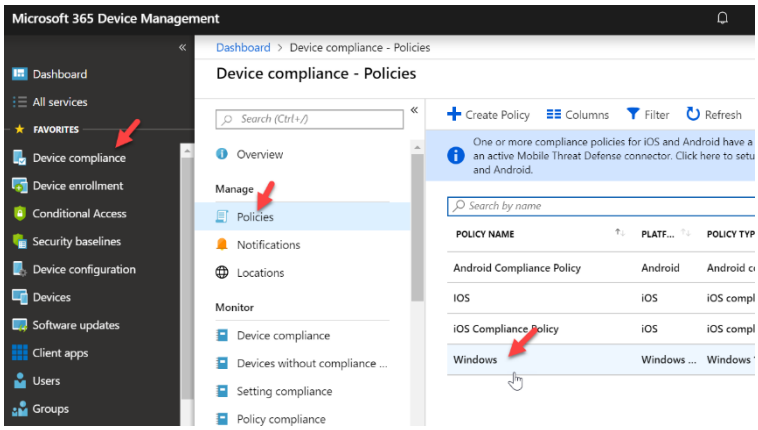
- End User Experience for Communications to Broad audience
- Common Troubleshooting Techniques for each platform

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

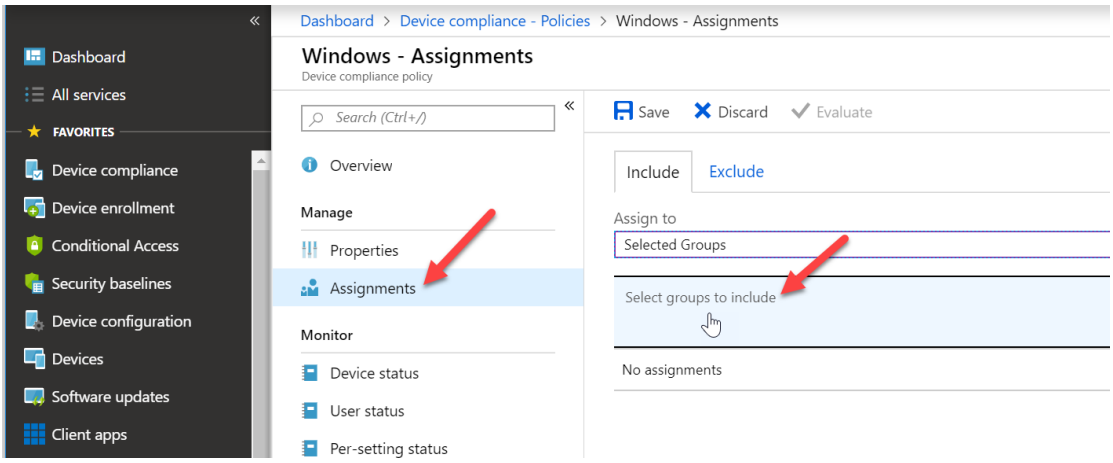
- Why is this service important?
- What pain points will it help them solve?
- What can end users expect?
- What are the steps to get my device enrolled

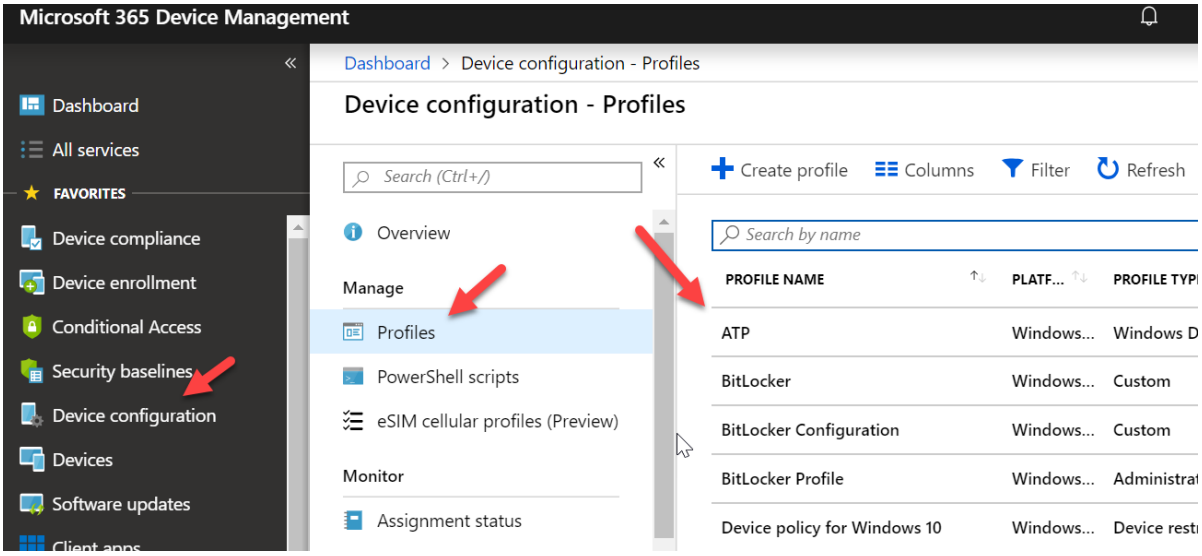
Lastly, after we have this pushed out and a target date for deployment, we can go back into the Device Management Admin Center and begin to add our groups to our policies and profiles:

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



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





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