Microsoft

Desktop-as-a-Service (DaaS)
Using Windows Virtual Desktop (WVD)

BYOD with M365 & Intune

Prepared for:
Service Provider Partners
Oct. 2019

Prepared by:
Microsoft – **O**ne **C**ommercial **P**artner (OCP)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Contents

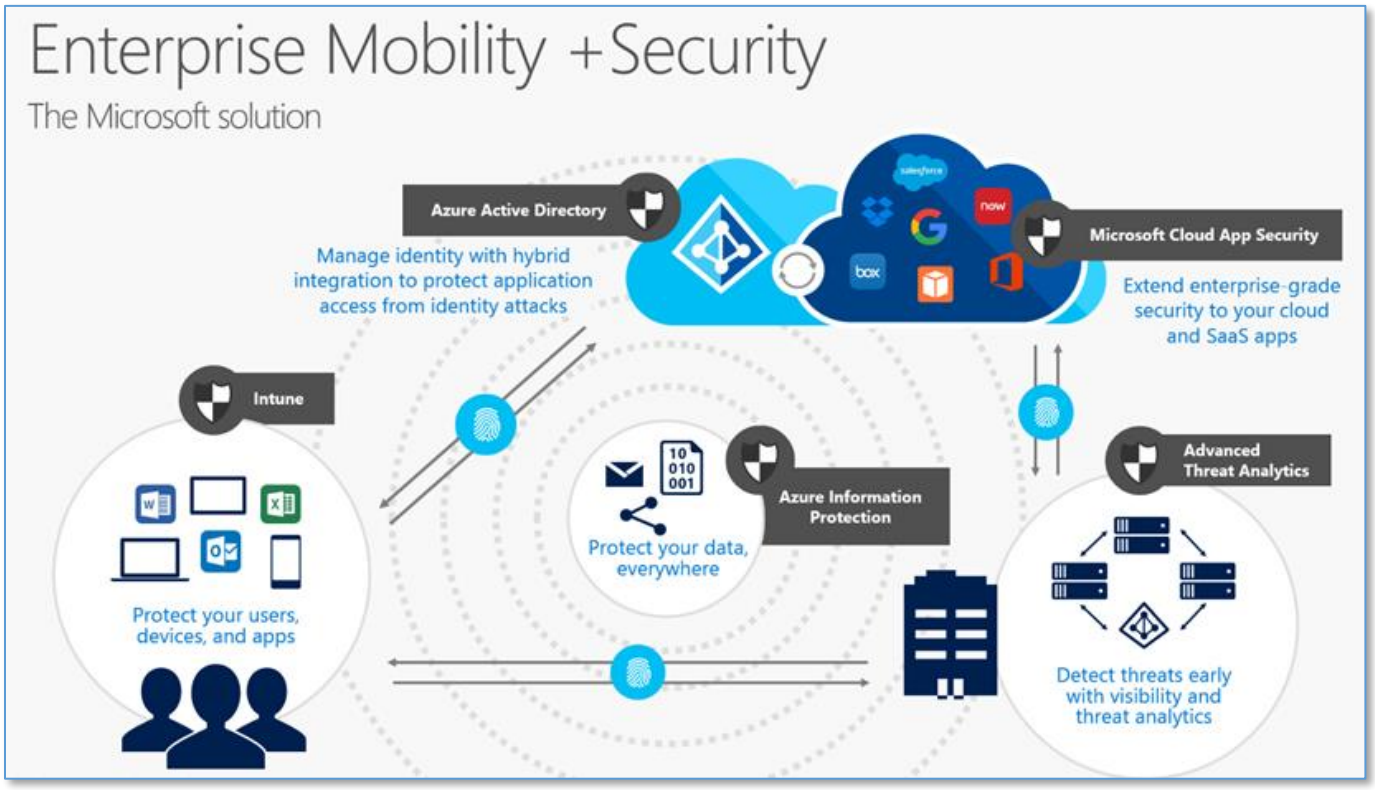
1. Overview 5
2. Prerequisites 5
   - Azure & Windows Active Directory Prerequisites 5
   - General Best Practices 6
   - Azure Networking 6
   - Azure Architectural Diagram 6
3. Setup Mobile Device Management (MDM) Services 7
   - Configure MDM Authority 7
   - Preparation for enrolling iOS devices 9
   - Preparation for enrolling Windows devices 14
4. Configure Company Portal 16
   - Device Enrollment Administrator 17
   - Device Group Categories 18
   - Creating Azure Active Directory Dynamic Device Security Groups 20
   - Create an AAD Dynamic Device Security Group 21
5. Device enrollment experience 22
   - Windows Devices 22
   - iOS Devices 24
6. Device Compliance Policies 24
   - Create a compliance policy 24
   - Assign a compliance policy 26
   - Configuration Policies 28
   - Create a configuration policy 28
   - Uninstall restricted applications policy iOS 32
   - Software Update Policies 35
   - Create a Windows software update policy 35
   - Create an iOS software update policy 40

7. Device Enrollment 43
Enable automatic enrollment for Windows 10 43
Enable automatic enrollment for iOS 44
Enrolling Windows devices manually 48
Microsoft Store App 50
Deploy Client Apps to Managed Intune Devices 53
8. Device Actions 57
Remotely erase data from a device 57
9. ATP and Intune Integration 58
Enable Microsoft Defender ATP in Intune 58
On-board devices by using a configuration profile 61
Create a device configuration profile 61
Assign a device profile 63
Create and assign a compliance policy 64
Create the compliance policy 64
Assign the device compliance to user/groups 66
Create a Conditional Access policy 67
Monitor device compliance 72
10. Support 72
11. Appendix 73
Device security and data protection security 73
Basic Security 73
Advanced Security 73

1. Overview

This document is a walk-through of implementing MDM, Intune, and ATP Azure Protection on Endpoints. Together, they let you manage smartphones, laptops, tablets, and desktops and multiple operating systems such as iOS, Android, Windows, macOS, and Chrome OS.

This document will cover deploying applications to devices, configuring your Company Portal, enrolling end user devices, creating policies, and more.



The image above shows the integrated cloud services designed to protect data and control access. In this document we will work with the majority of these tools to protect, analyze and track threats, and enforce security and update compliance for accessing the sensitive data of your organization.

Learn more about the device security and data protection services available for BYOD.

2. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- An Azure Active Directory
- A Windows Server Active Directory in sync with Azure Active Directory. This can be enabled through:
    - Azure AD Connect
    - Azure AD Domain Services
- An Azure subscription, containing a virtual network that either contains or is connected to the Windows Server Active Directory

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

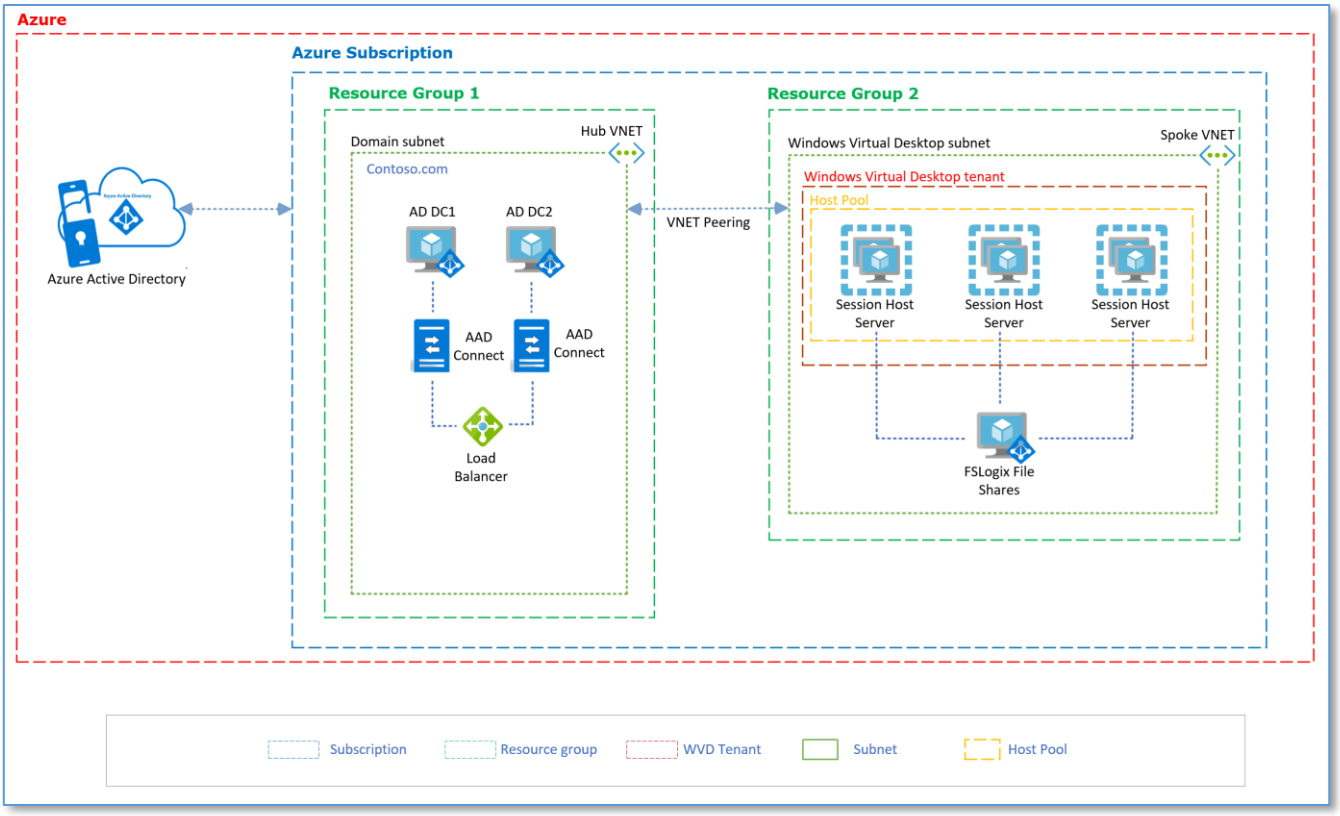
- Please follow the guidance here to maintain a consistent naming convention across your resources, unless you are already using a naming system.
- Azure security best practices and patterns
- Azure Active Directory Hybrid Identity best practices
- Azure identity management and access control security best practices
- Azure Networking & security Best Practices
- Azure Storage security overview
- Best practices for Azure VM security

Azure Networking

The recommendation is to design your Azure Networking using a Hub-Spoke topology. Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.



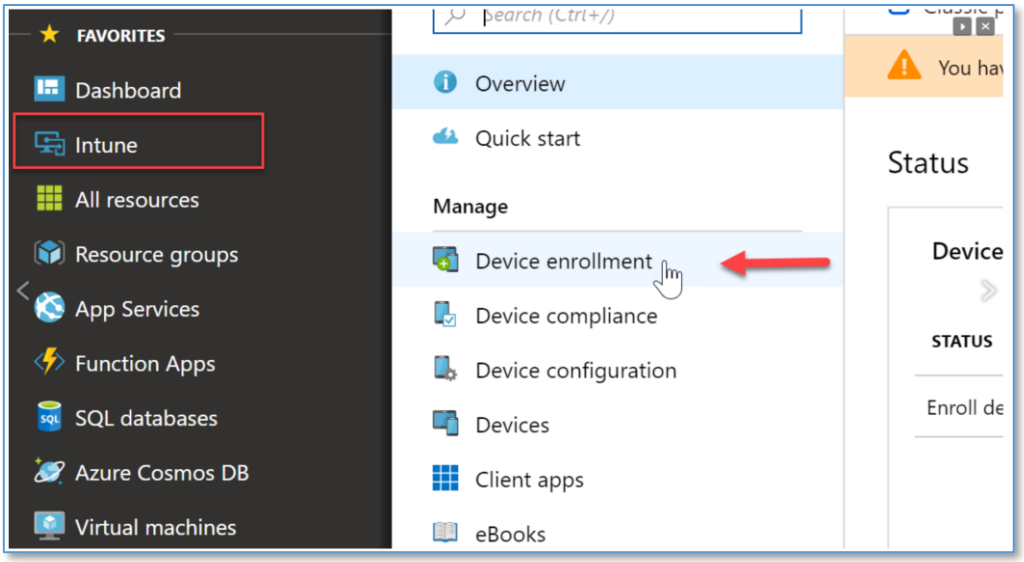
3. Setup Mobile Device Management (MDM) Services

In this section we'll implement Azure Mobile Device Management (MDM) Services. This includes setting up the enrollment processes for the various device types.

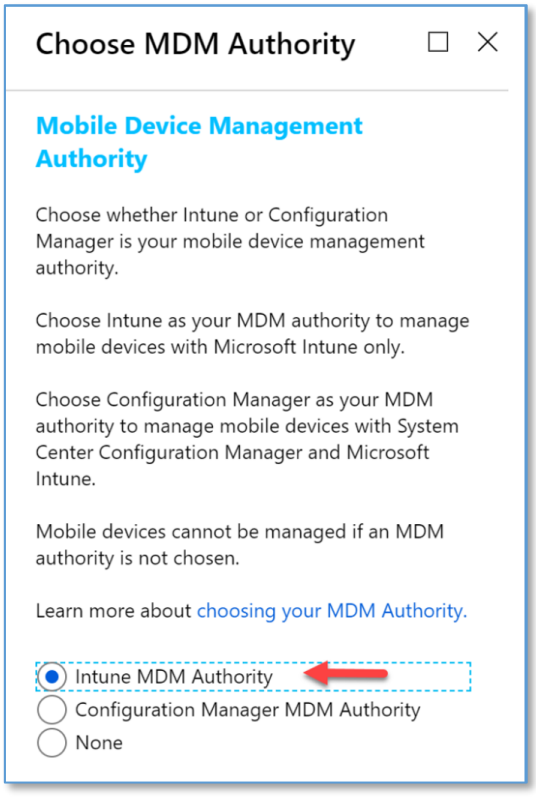
Configure MDM Authority

First, we must configure Intune as our MDM authority. We are setting up MDM as stand-alone, so we'll use Intune as the only authority, and not Configuration Manager.

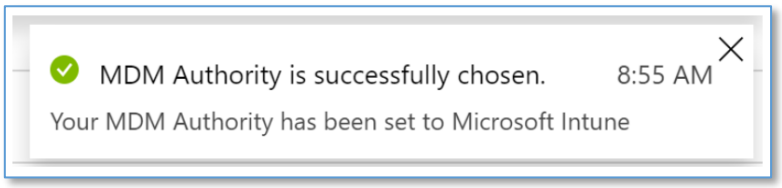
1. Logon to portal.azure.com, and search for "Intune".
2. Open the service console, then expand the Intune node and select "Device Enrollment".



3. Select "**Intune MDM Authority**" and then click "**Choose**":



1. We will get a notification that the changes were saved successfully

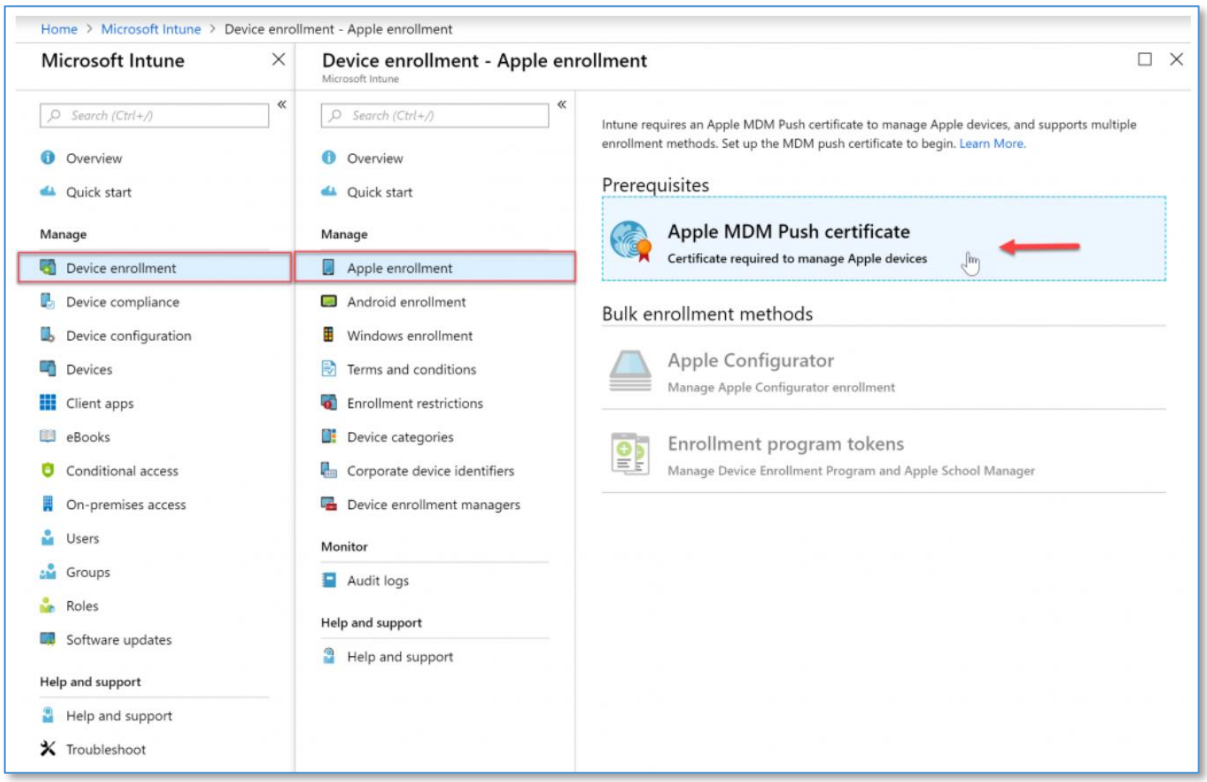


After the MDM Authority is configured, we go next to Configuring APN Certificate. These steps are necessary for managing iOS devices.

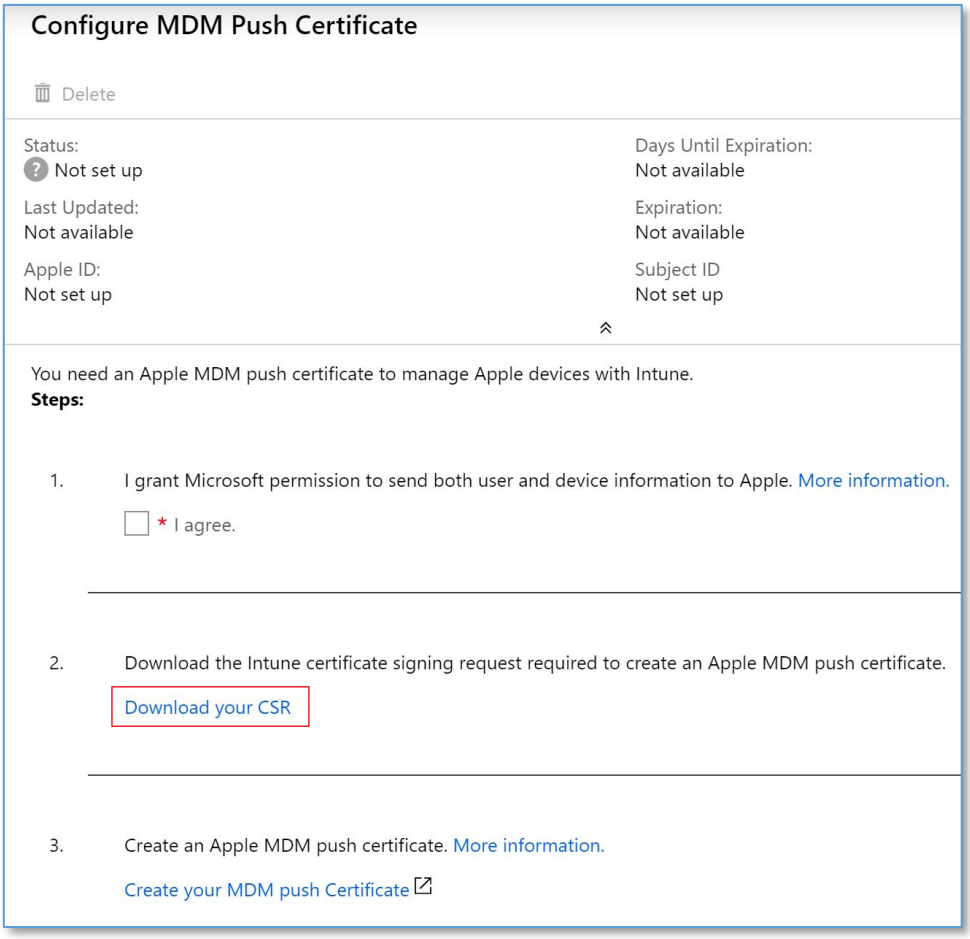
Preparation for enrolling iOS devices

To manage iOS devices, we must create an Apple Push certificate:

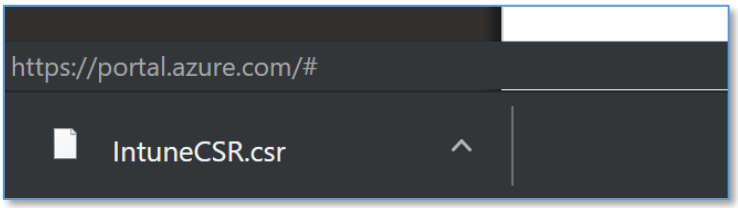
1. In the Intune blade, go to **Device Enrollment** > **Apple Enrollment**, select "Apple MDM Push Certificate"



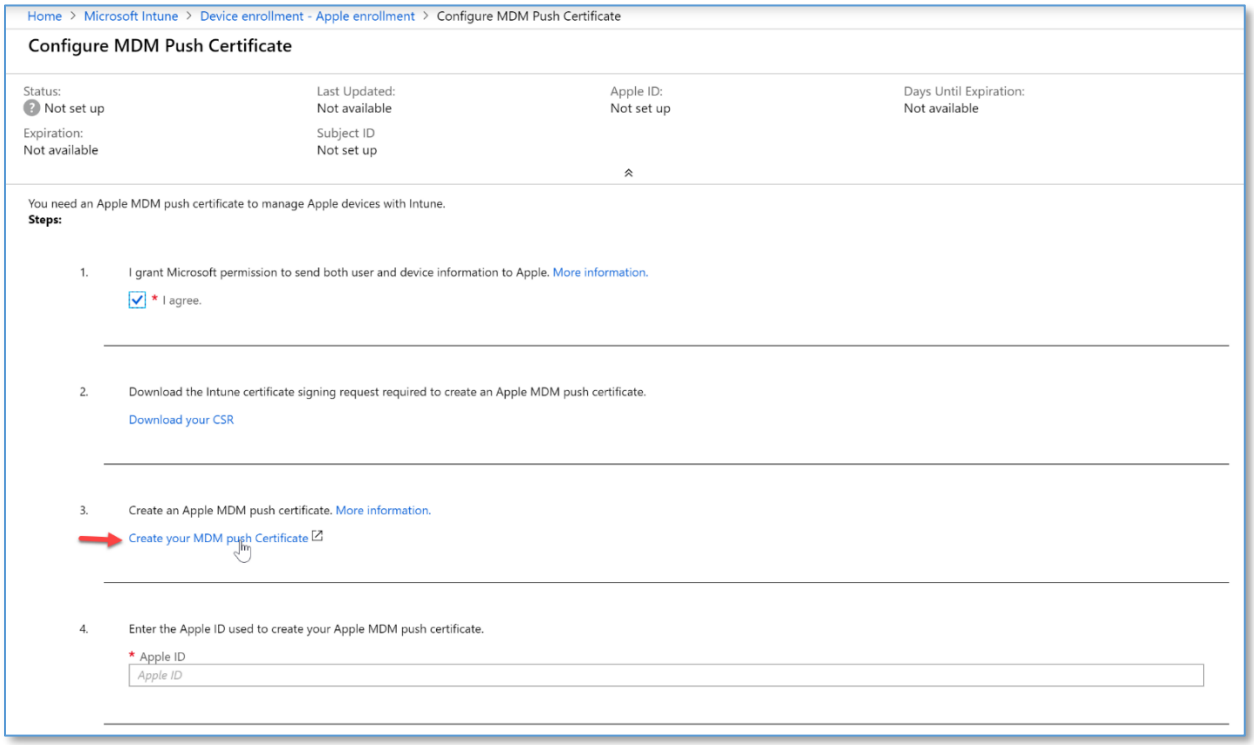
2. Agree to the terms and then download the CSR:



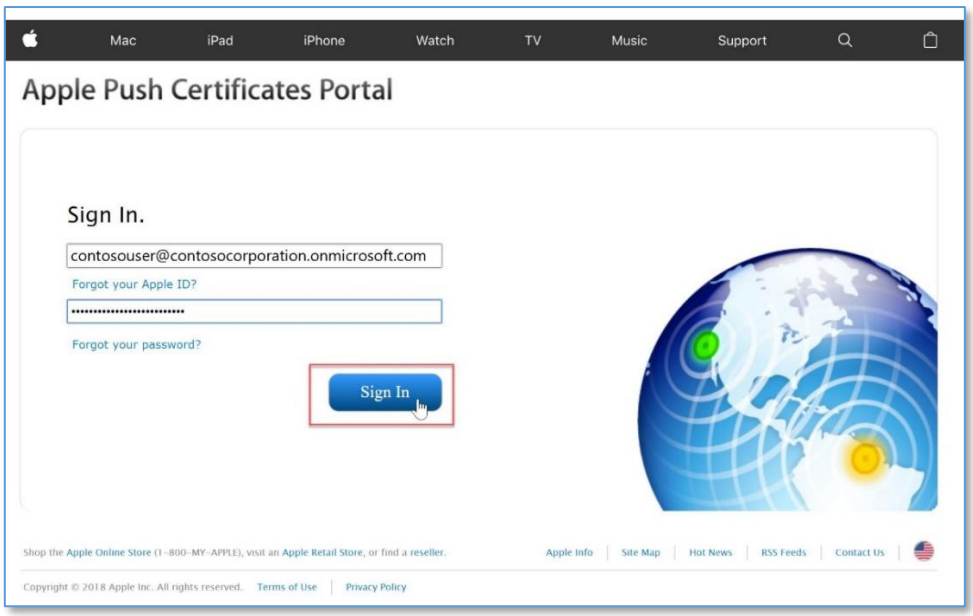
3. The file, "IntuneCSR.csr" will be downloaded.



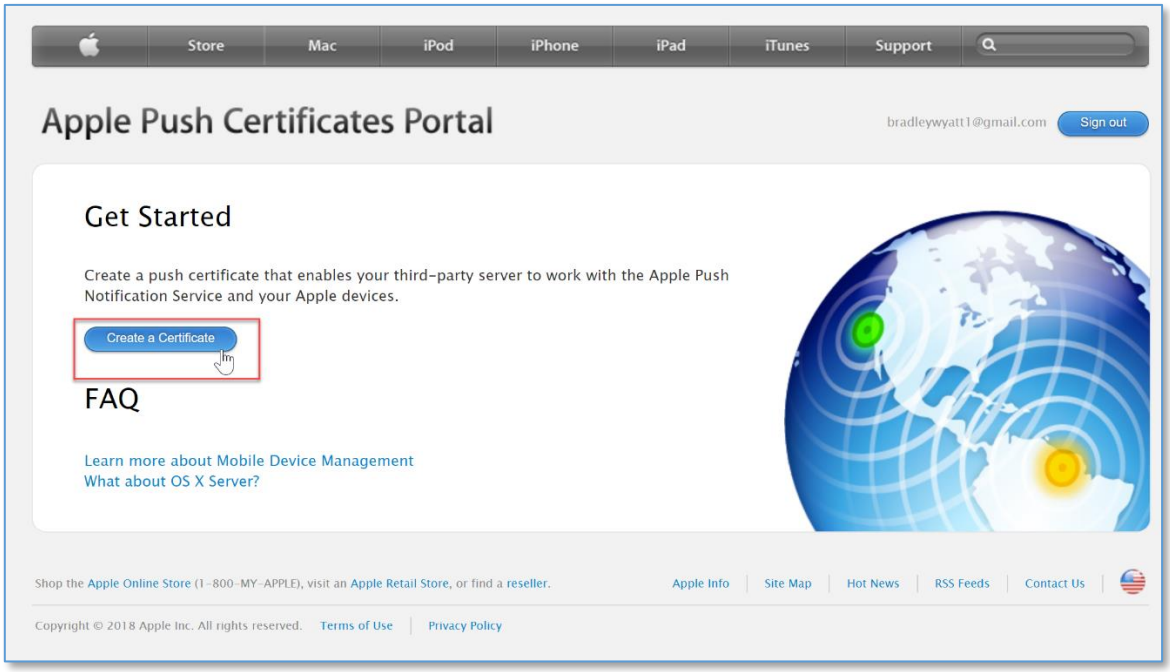
4. Click **Create your MDM push certificate**. You will need to have an Apple ID so if you do not have one you will need to create one.



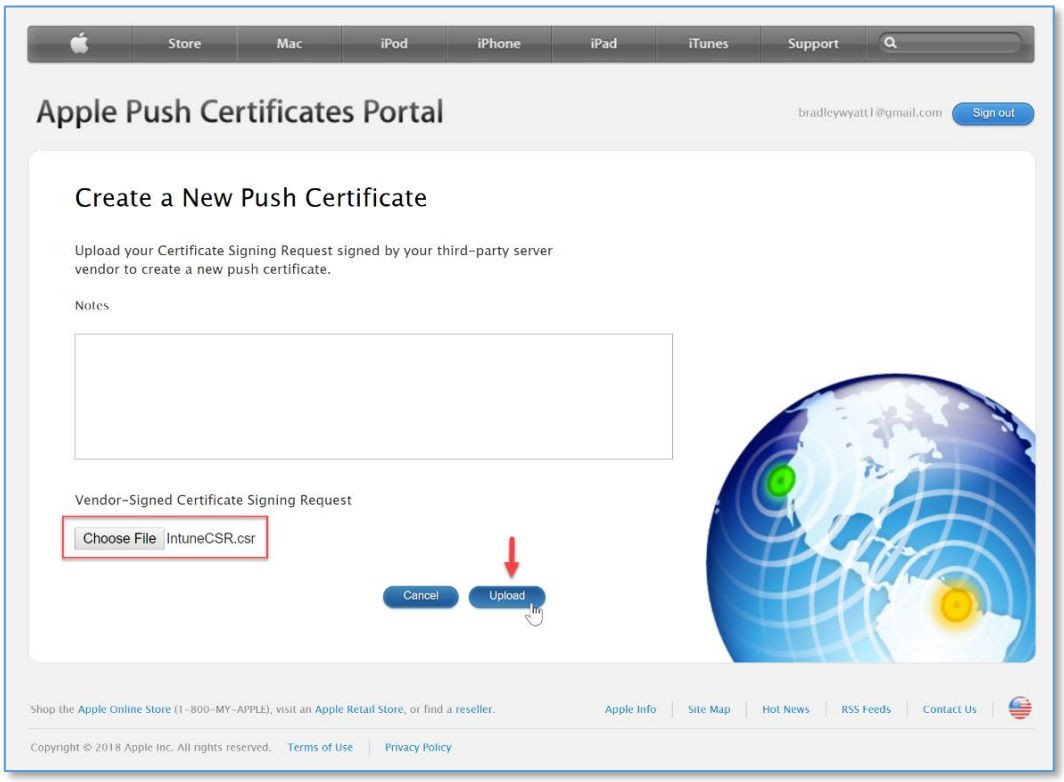
5. Sign in with your Apple ID into the Apple Push Certificates Portal:



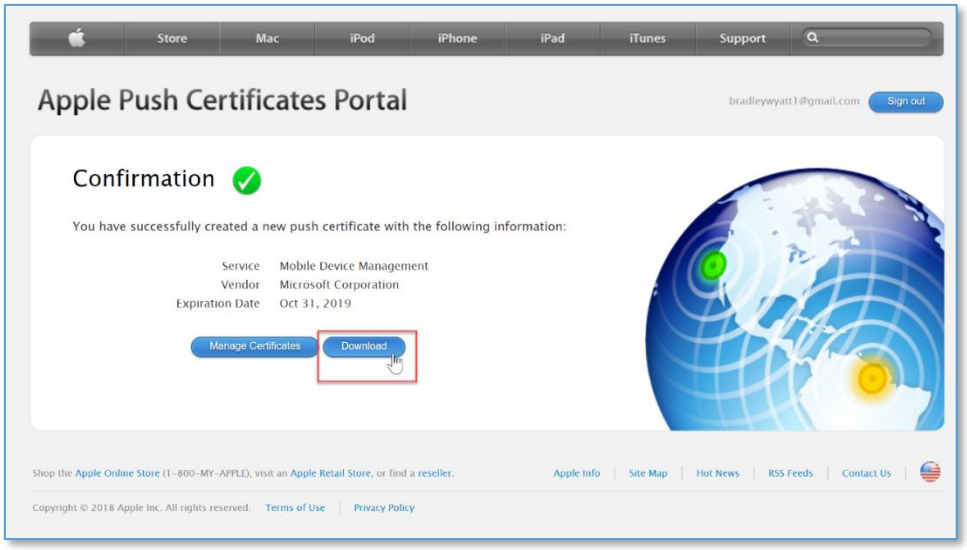
6. Now click “Create a Certificate” after you have successfully signed into the portal:



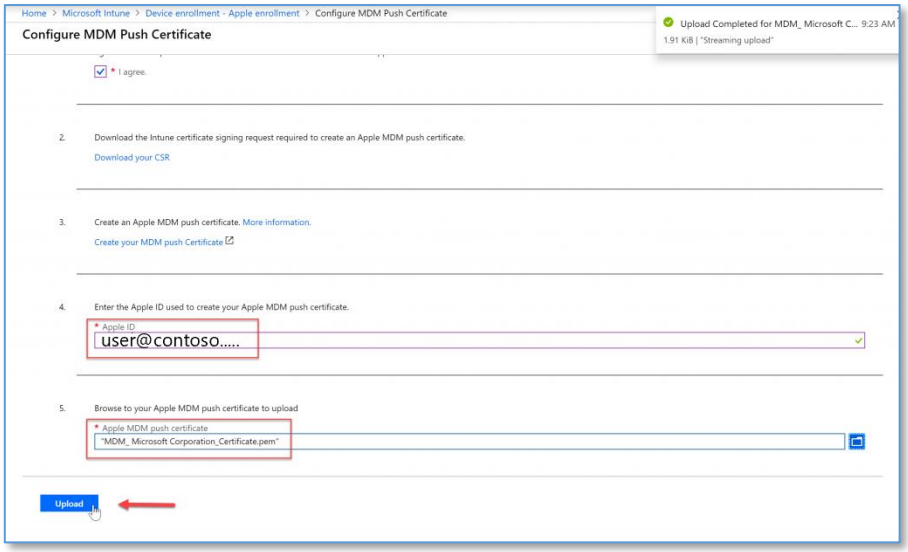
7. Navigate to the CSR file that we downloaded from the Intune portal, & select “Upload”



8. Once you have a green confirmation, download your certificate:



9. Go back to the Intune portal, and in **step 4**, enter your **Apple ID**. In **step 5** browse to the downloaded **certificate** and then press "**Upload**":

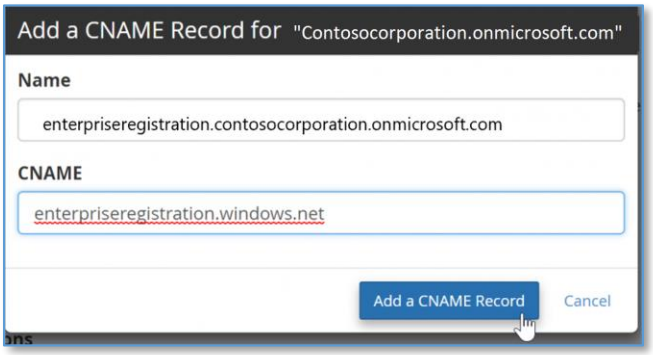


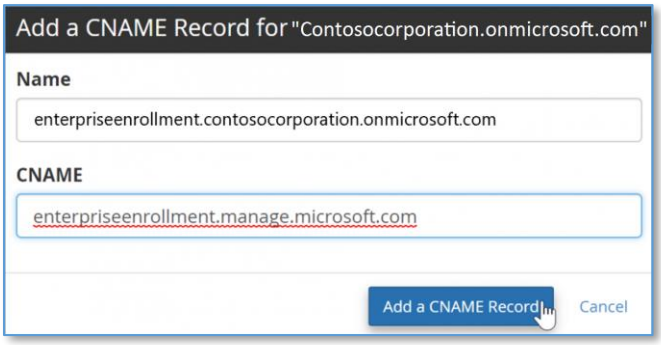
iOS device enrollment is now setup.

Preparation for enrolling Windows devices

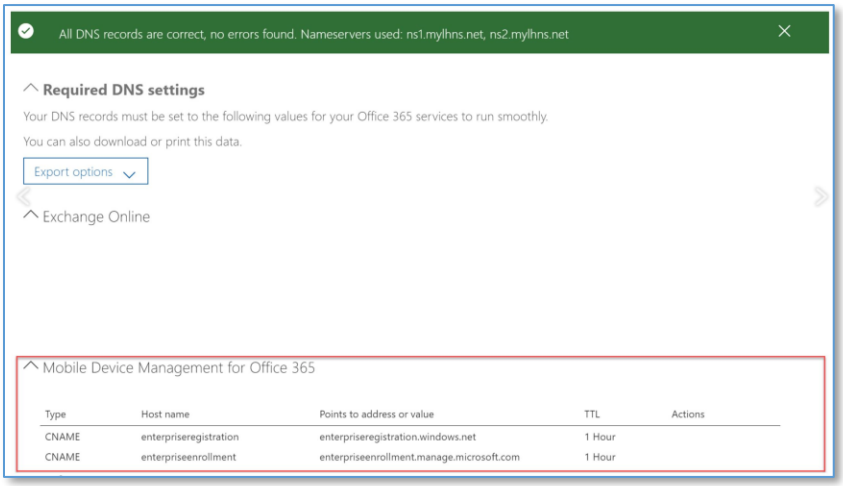
For Windows devices, there are two DNS CNAME records that need to be created within your domains DNS zone. These will redirect the devices to the Intune servers for automatic device management. In our example, we're adding them to Contosocorporation.onmicrosoft.com:

1. Add **enterpriseregistration**.[domain name] and **enterpriseenrollment**.[domain name]

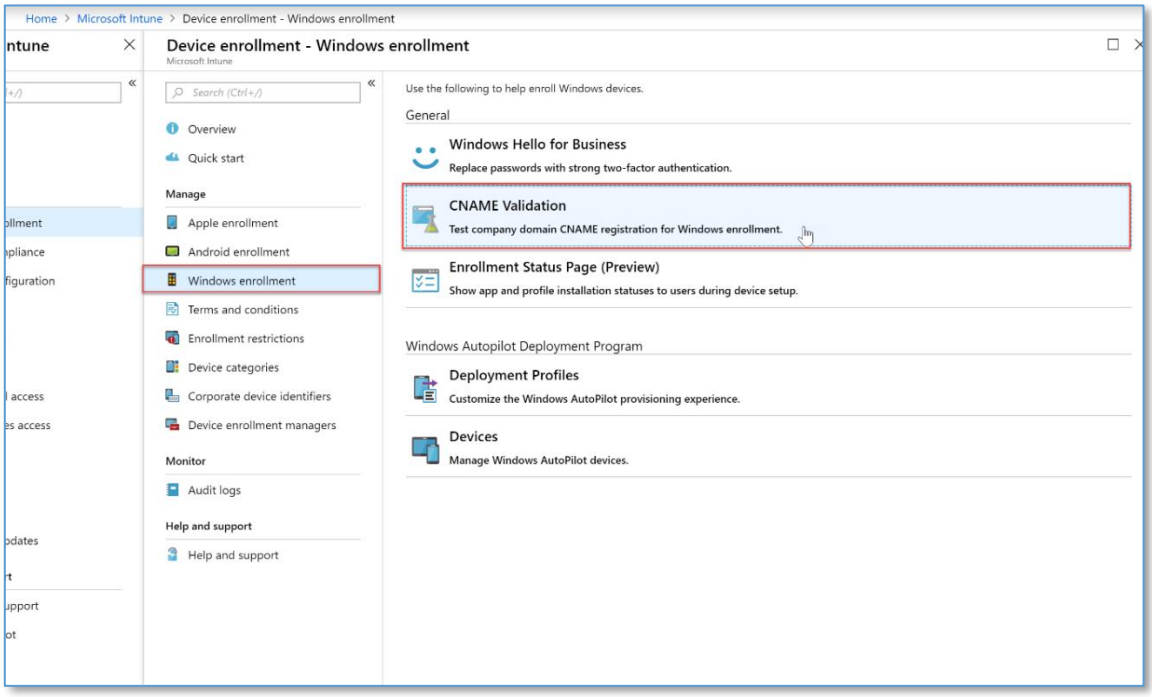




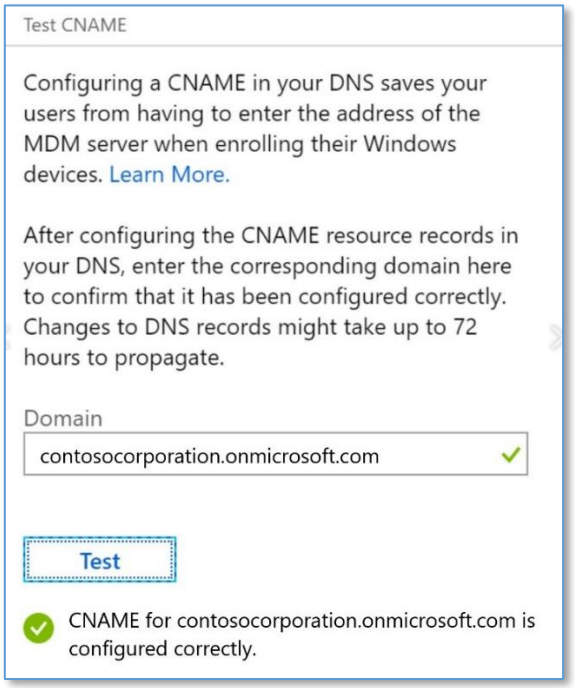
2. Check DNS for MDM, to see that the records are now in place and valid:



3. In the Intune Azure portal, open **Device Enrollment**
4. Click **Windows enrollment** > **CNAME Validation**



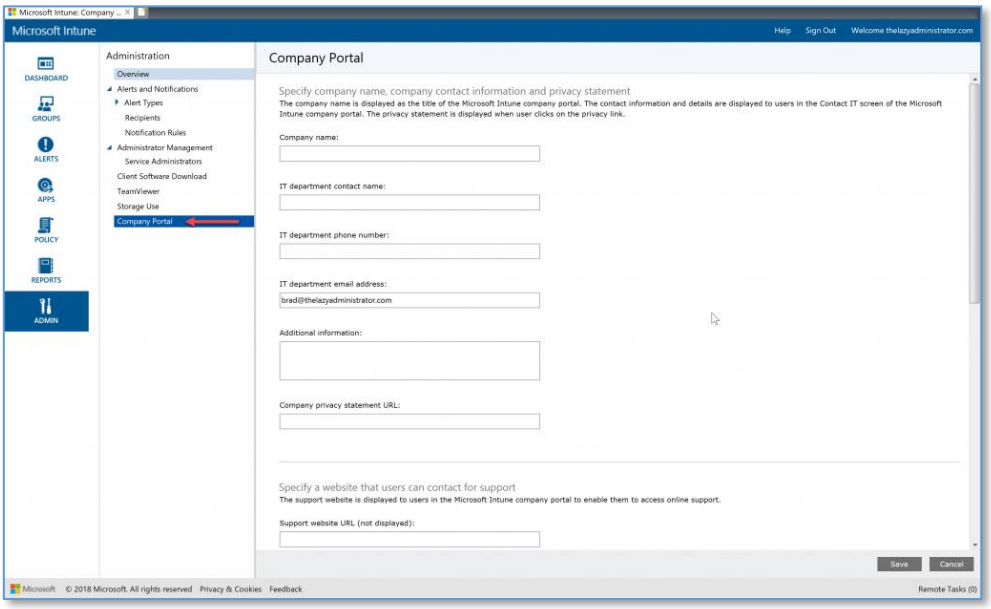
5. Test that the domain is verified successfully:



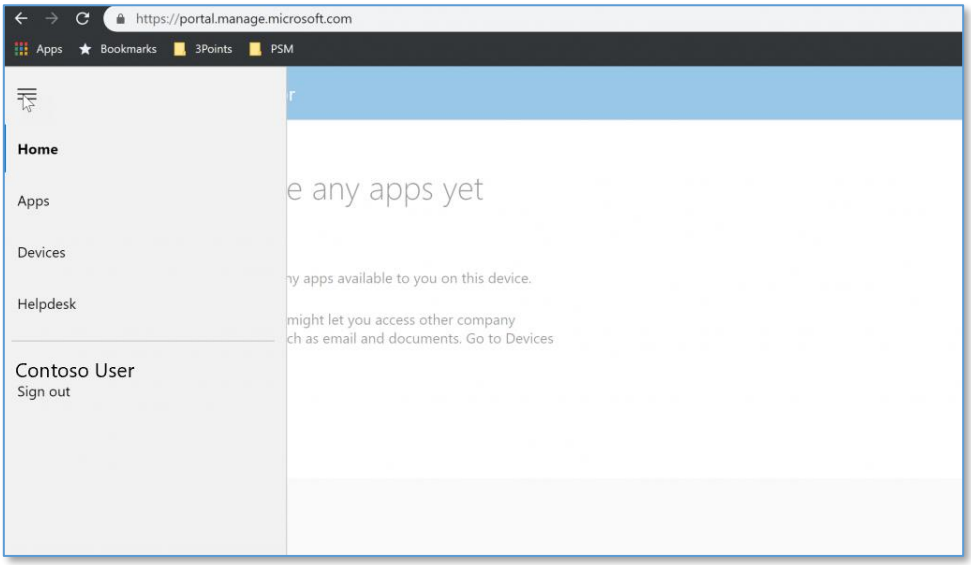
4. Configure Company Portal

The Company Portal is a web page and a mobile device application that supports BYOD users. It gives them a centralized location to install published applications, self-management, and retrieve information.

The Company Portal is configured on the Intune Portal at https://portal.manage.microsoft.com/



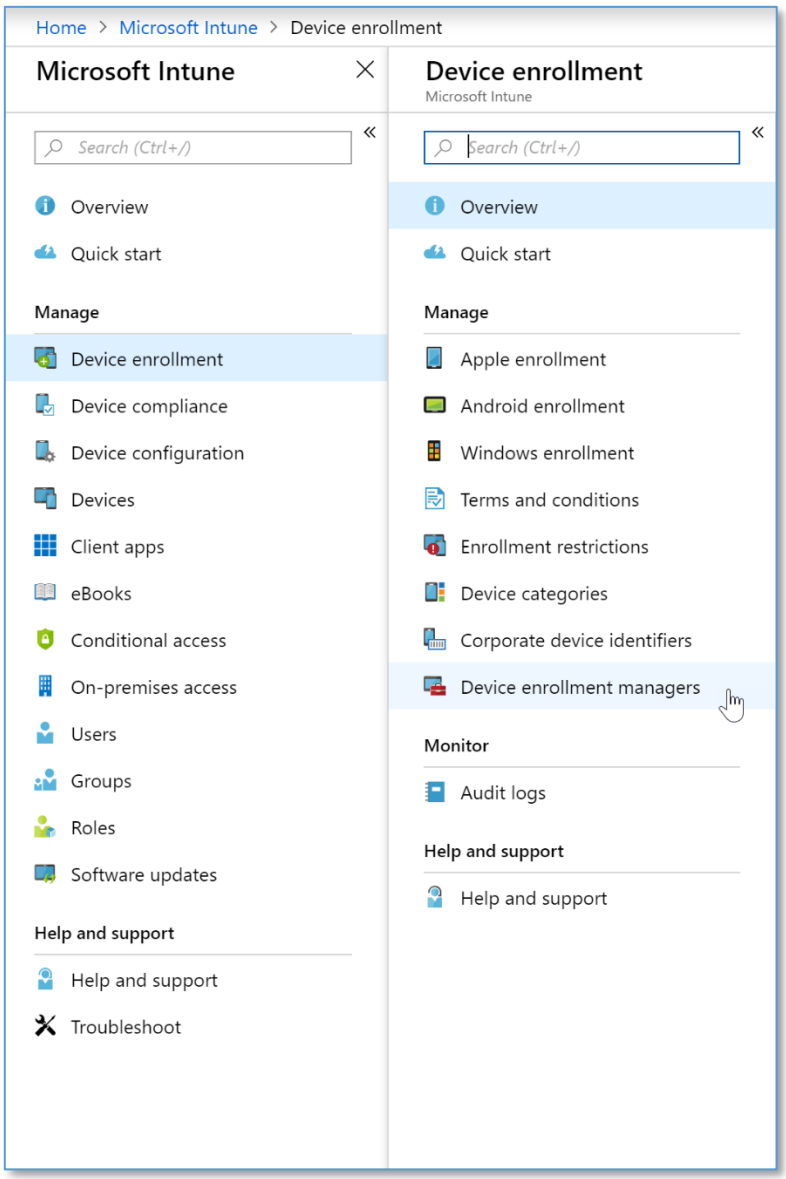
Once the administrator saves the Company Portal changes, you can launch the portal website (https://portal.manage.microsoft.com/) and get the apps and devices registered to the user.



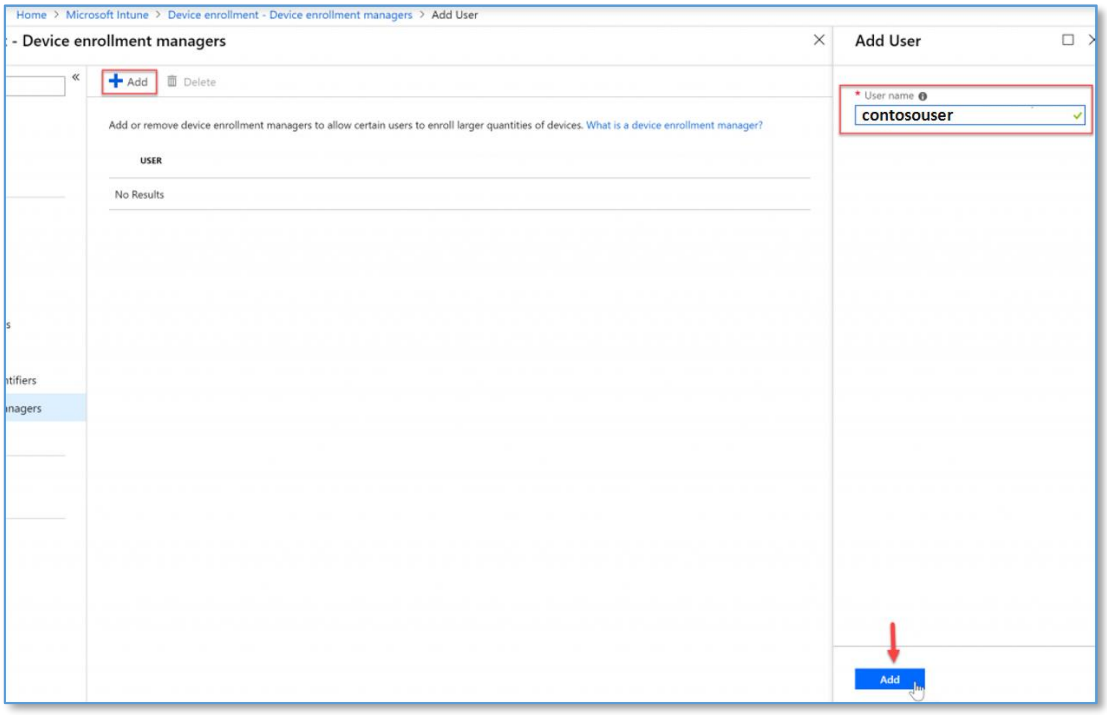
Device Enrollment Administrator

Device Enrollment Administrators are users that are able to enroll more than the default of 5 devices to Intune (which is meant for a standard user and not an Administrator account.)

1. Navigate to the Azure Portal and expand the Intune blade
2. Expand “Device Enrollment” and select “Device Enrollment Managers”



3. Click Add and then enter your users UserPrincipalName and then select the "Add" button on the bottom. In this case we're adding "contosouser":



Device Group Categories

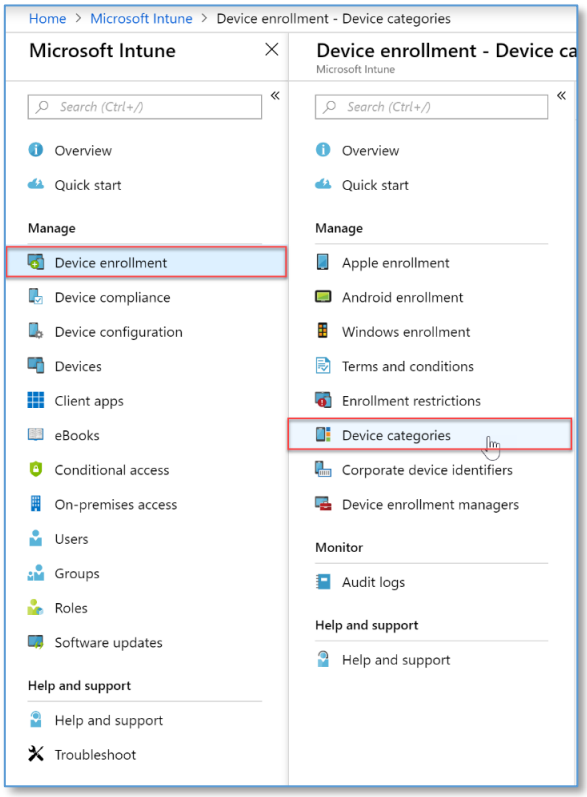
Use Microsoft Intune **device categories** to automatically add devices to groups based on properties that you define. This makes it easier for you to manage those devices as a group.

In this walk-through, we'll create two device categories.

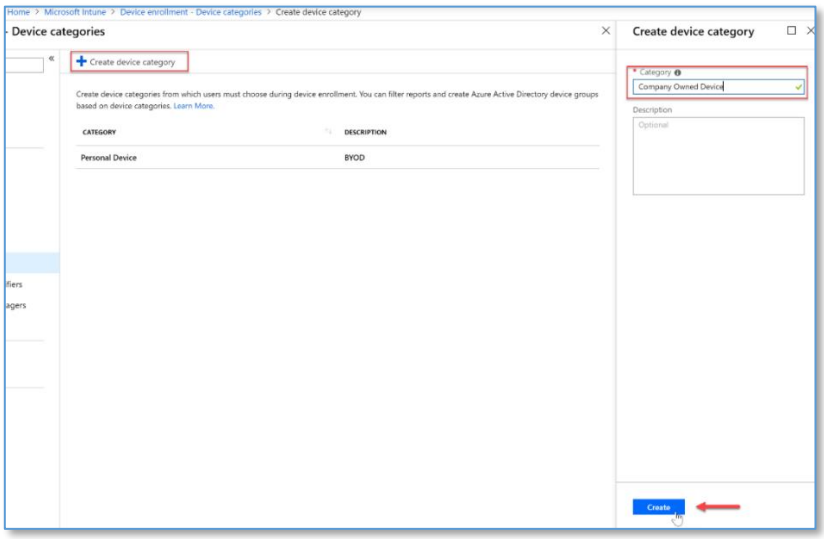
- **Company Owned Devices**. These devices are purchased by the company, and given to the end users through the IT department.

- **BYOD** devices, or personal devices. These will be devices that end users own but may use them for work.

1. In the Azure Portal, expand the **Intune** blade.
2. Select "**Device Enrollment**" and then click "**Device Categories**"



3. To add a new category, click **Create Device Category,** supply a valid name, and press "**Create**". We're adding the category called Company Owned Devices:



Repeat this step for each category you wish to add.

Creating Azure Active Directory Dynamic Device Security Groups

In this section, you will create dynamic groups in the Azure portal, based on the device category and device category name.

Use the information in this section to create a device group with an advanced rule, by using the **deviceCategory** attribute. For example: **device.deviceCategory -eq** "*Personal Device*".

When users of **iOS** and **Android** devices enroll their device, they must choose a category from the list of categories you configured. After they choose a category and finish enrollment, their device is added to the Intune device group, or the Active Directory security group that corresponds with the category they chose.

Windows users should also use the Company Portal website to select a category.

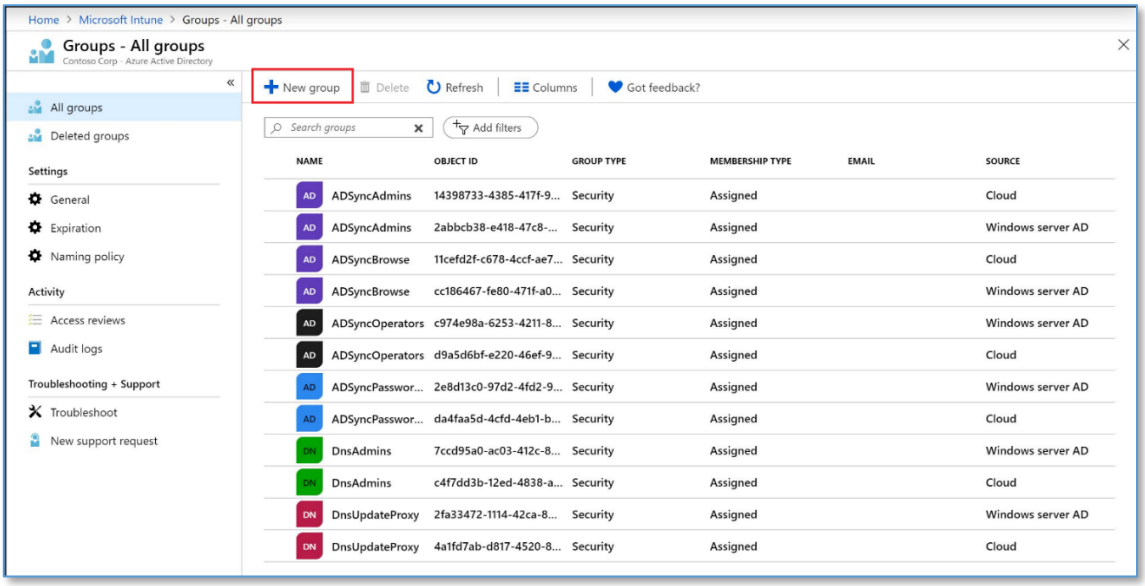
Regardless of platform, your users can always go to *portal.manage.microsoft.com* after enrolling the device. Have the user access the Company Portal website, and go to **My** Devices. They can choose an enrolled device listed on the page, and then select a category.

After choosing a category, the device is automatically added to the corresponding group.

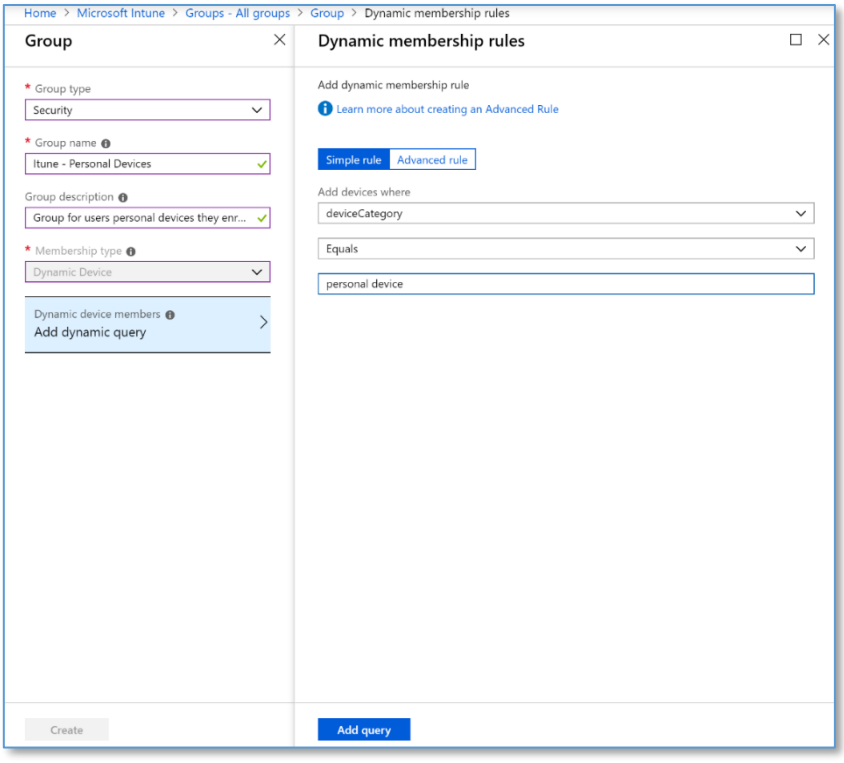
- If a device is already enrolled before you configure categories, the user sees a notification about the device on the Company Portal website. This lets the user know to select a category the next time they access the Company Portal app on iOS or Android.

Create an AAD Dynamic Device Security Group

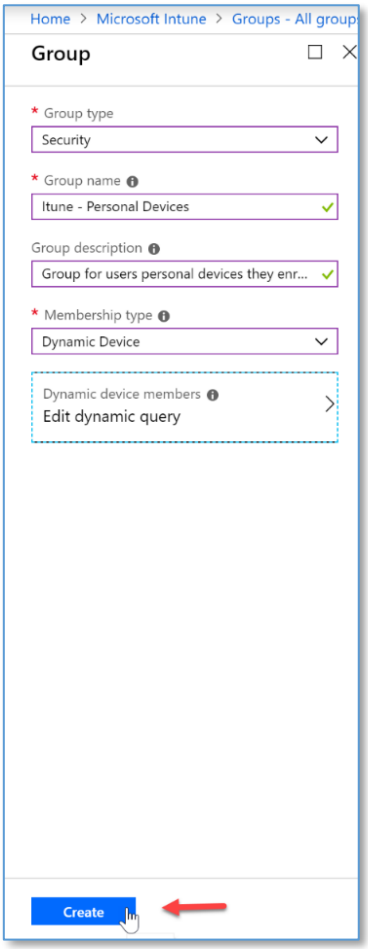
1. In the Intune blade, select **Groups**, and the select "**All Groups**" and click "**New Group**":



2. Give your group the required properties like type, name and description. We will want to add a dynamic membership rule. Our example below will contain all devices that a user selects as their Personal Device.



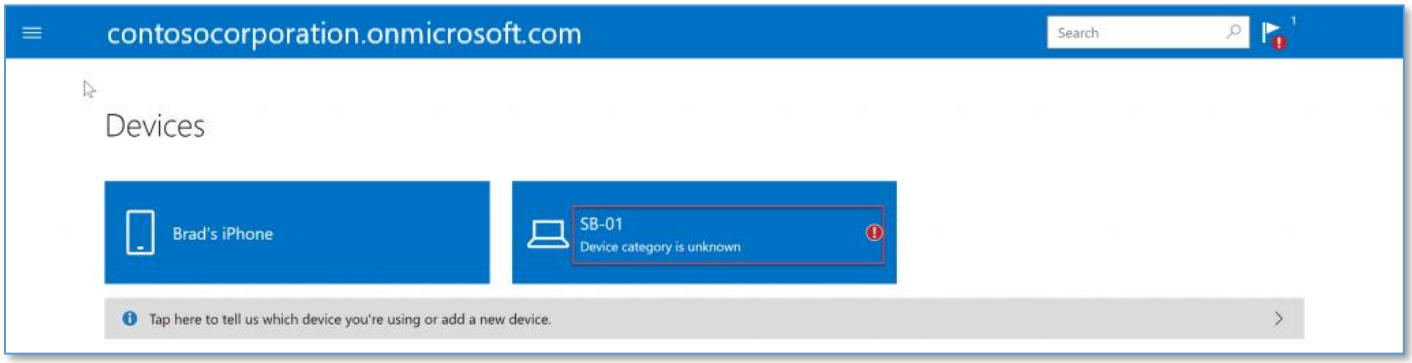
3. Once you have your new Group with the correct properties and query, click "**Create**"



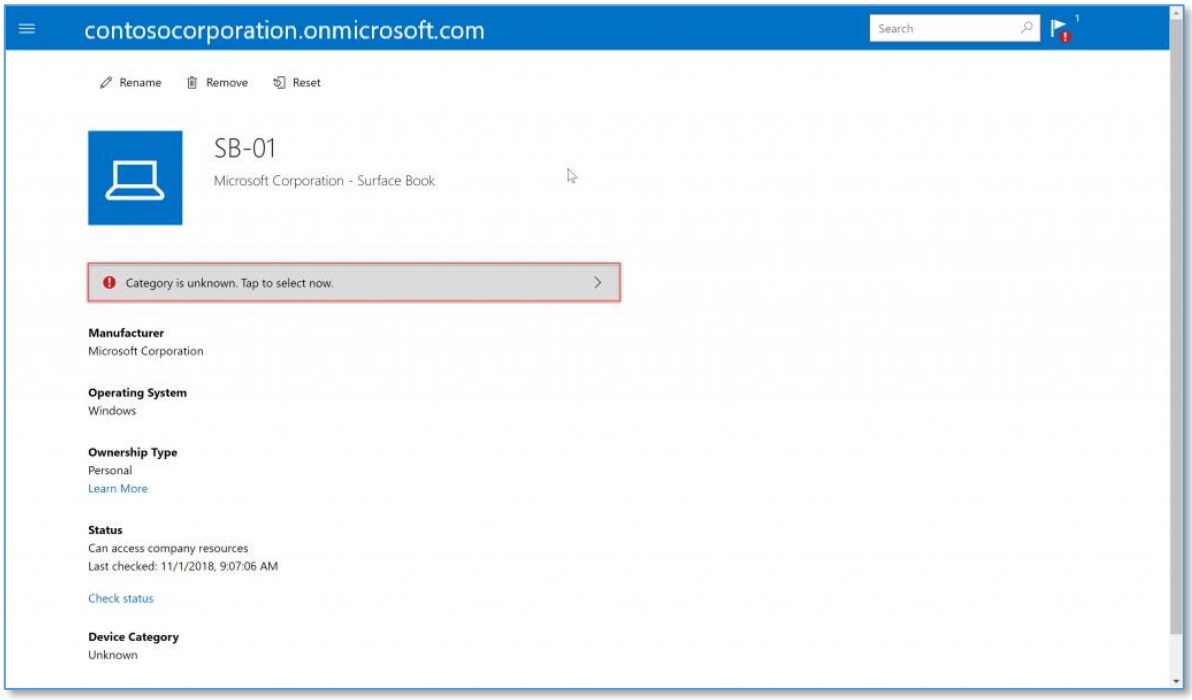
5. Device enrollment experience

Windows Devices

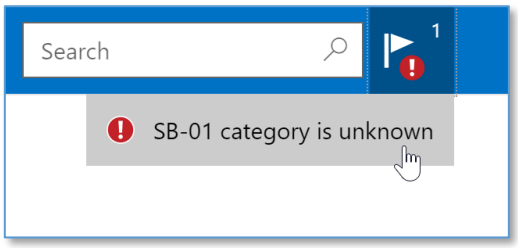
When users enroll their Windows devices, they must select a category in the online Intune portal:



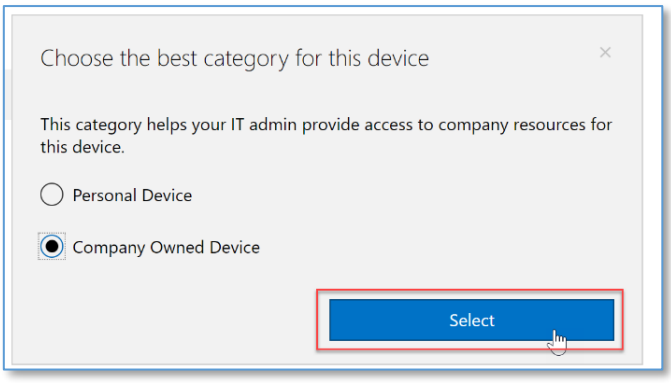
Clicking on the device will show them the outstanding alert and allow them to select a category:



In the top right of the portal they will also see a notification:

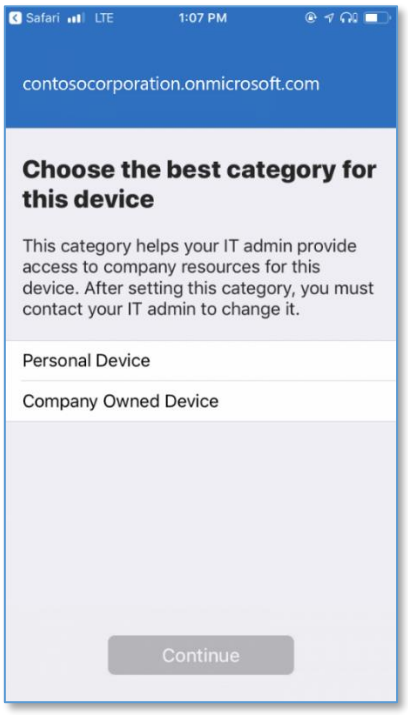


Here we see the two categories I set up for the users to select. Since this machine is a Company Owned Device, I will select that category. Behind the scenes, this device is added to that dynamic group and allows for a better management experience.



iOS Devices

When users enroll their iOS devices using the Company Portal application, they will select which category the device should be placed in:

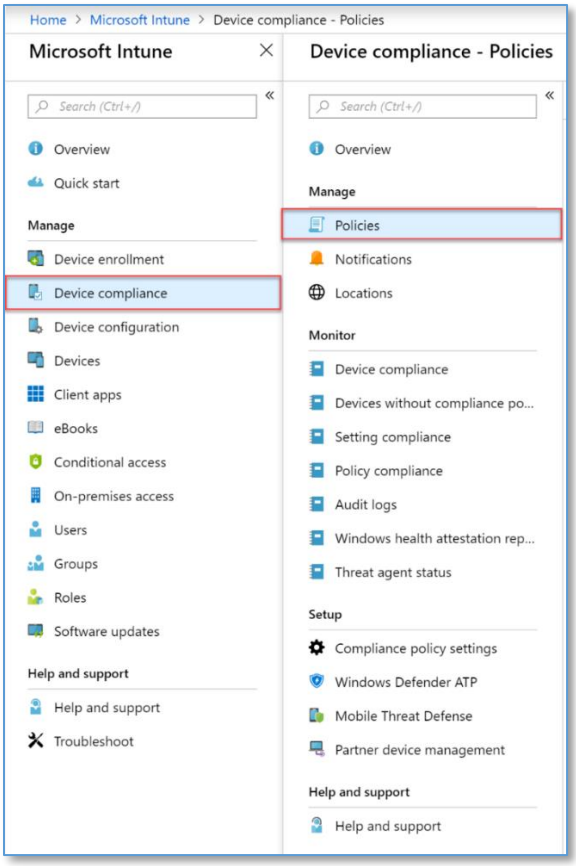


6. Device Compliance Policies

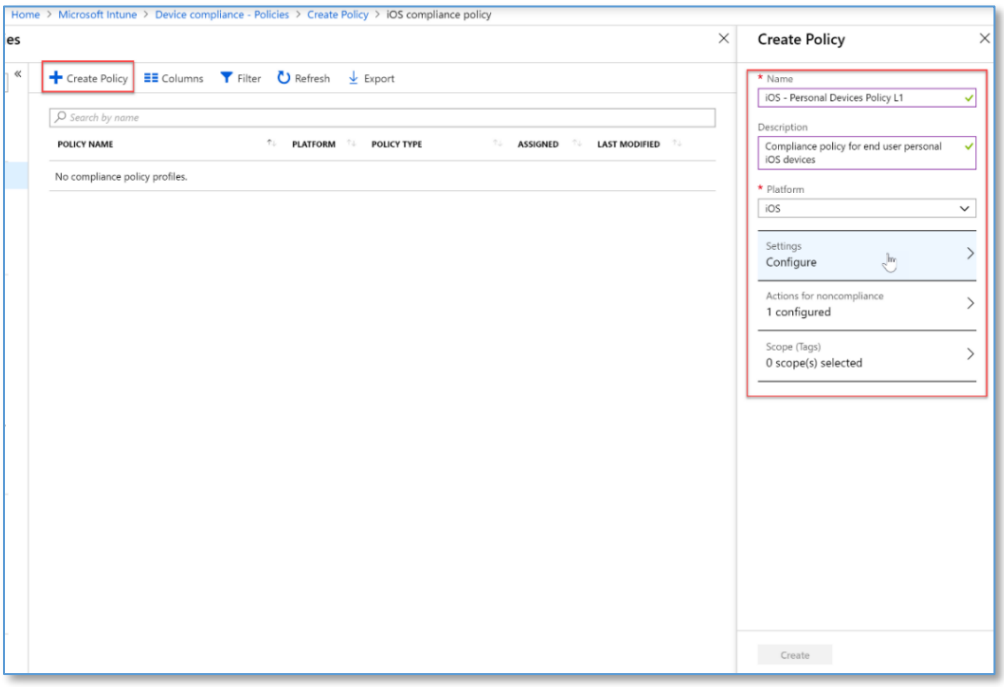
Create a compliance policy

Compliance policies in Intune define the rules and settings that a device must comply with in order to be considered compliant by conditional access policies. In this walk-through, we'll create, and enforce, a policy that requires a user to enable password protection:

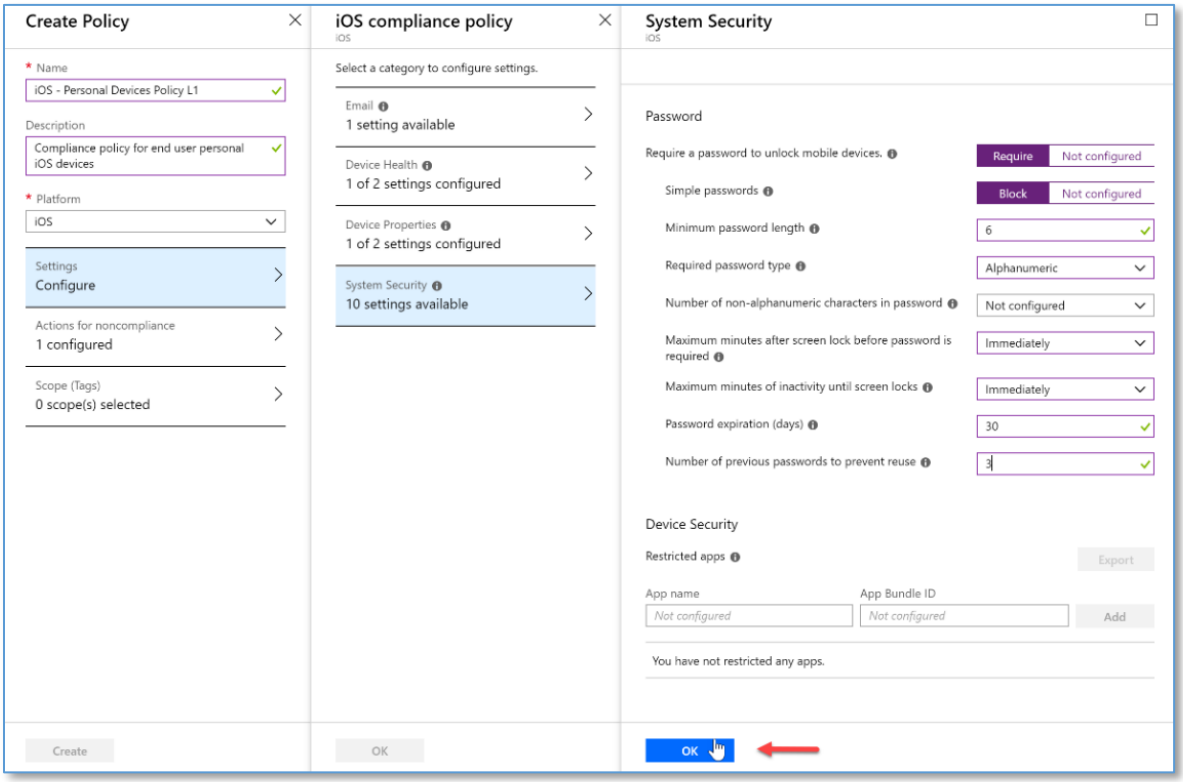
1. Navigate to the Azure portal and select the Intune blade
2. Select "**Device Compliance**" and then "**Policies**"



3. Click "**Create Policy**" and then I am going to create a policy that I will apply to my end users personal devices. This will be a policy for the group we created earlier.

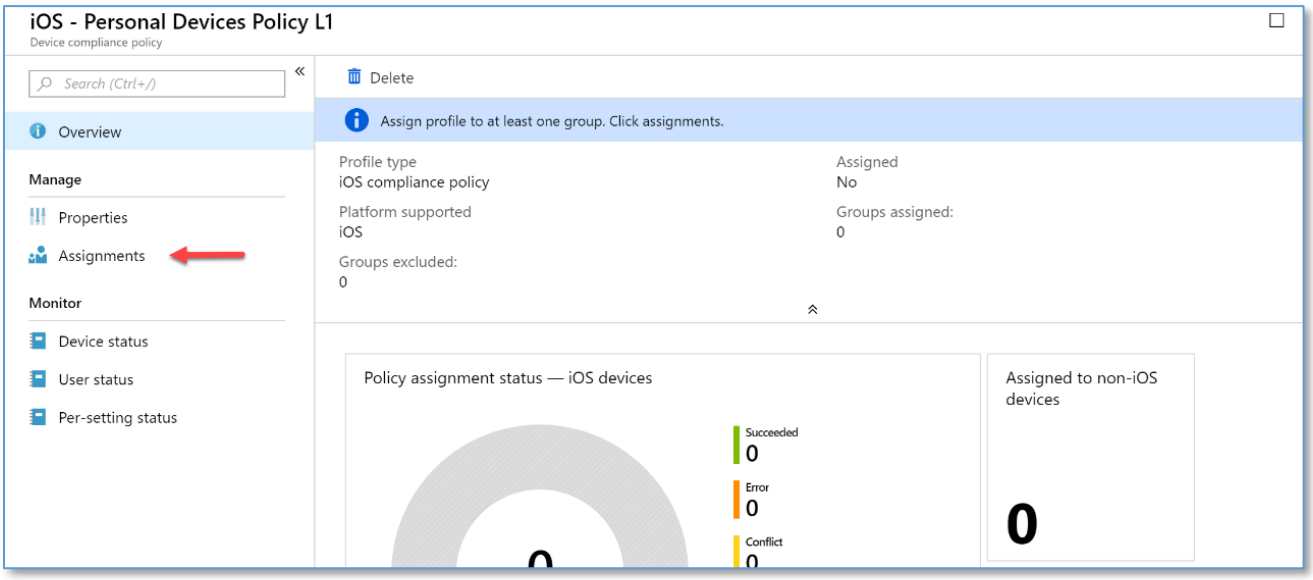


4. Once you have configured all of the Compliance settings, save the policy.

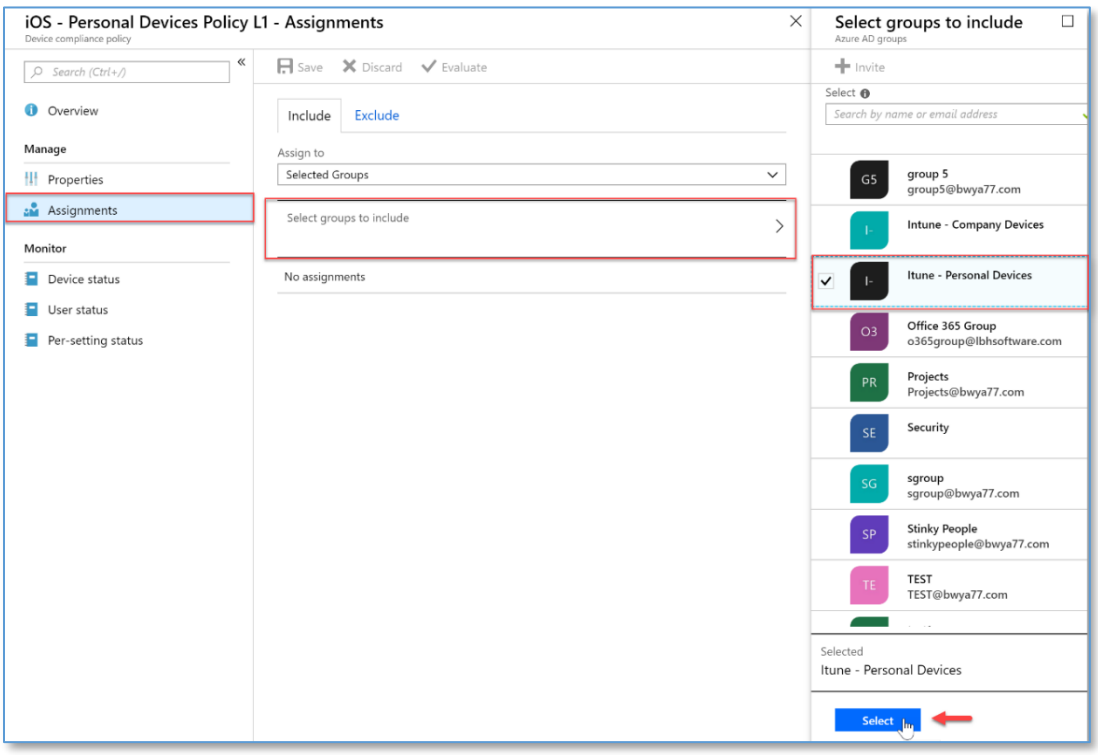


Assign a compliance policy

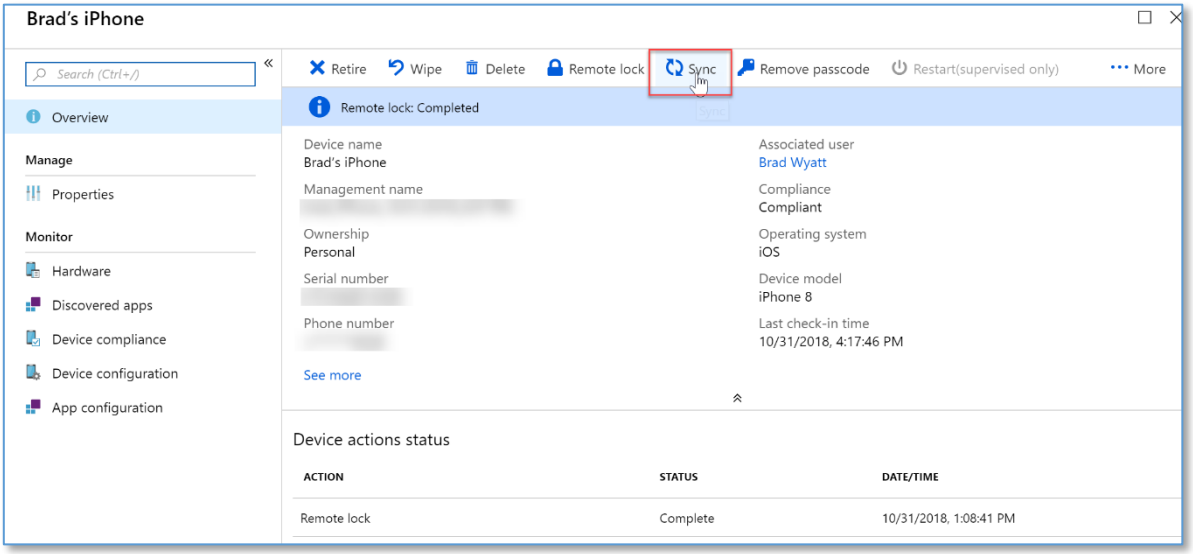
5. To assign this policy to devices or users. Click the **Assignments** item under Manage:



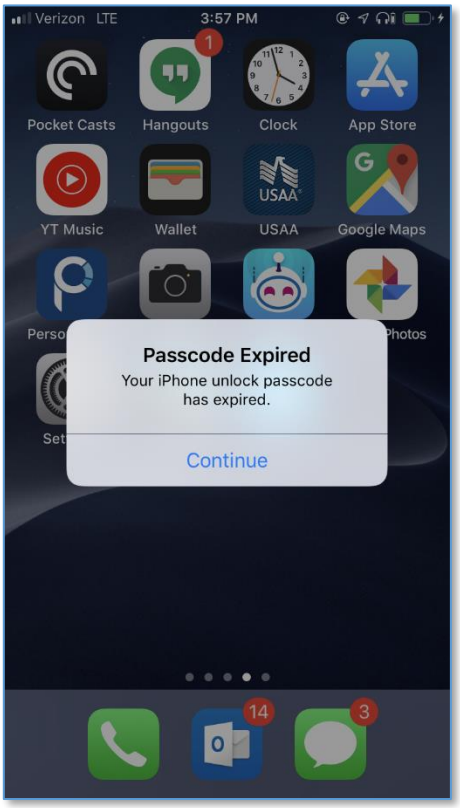
6. Once I click "**Select groups to include**" I can select my Intune – **Personal Devices** dynamic group and then **save**:



- As an added example, I want to make sure the policy goes into effect immediately on some device. I simply go to **All Devices,** find that device, and click **Sync**:



- If you set a passcode and the users current passcode does not match, they will be greeted with a password expiration notification. From there they can set their own passcode:

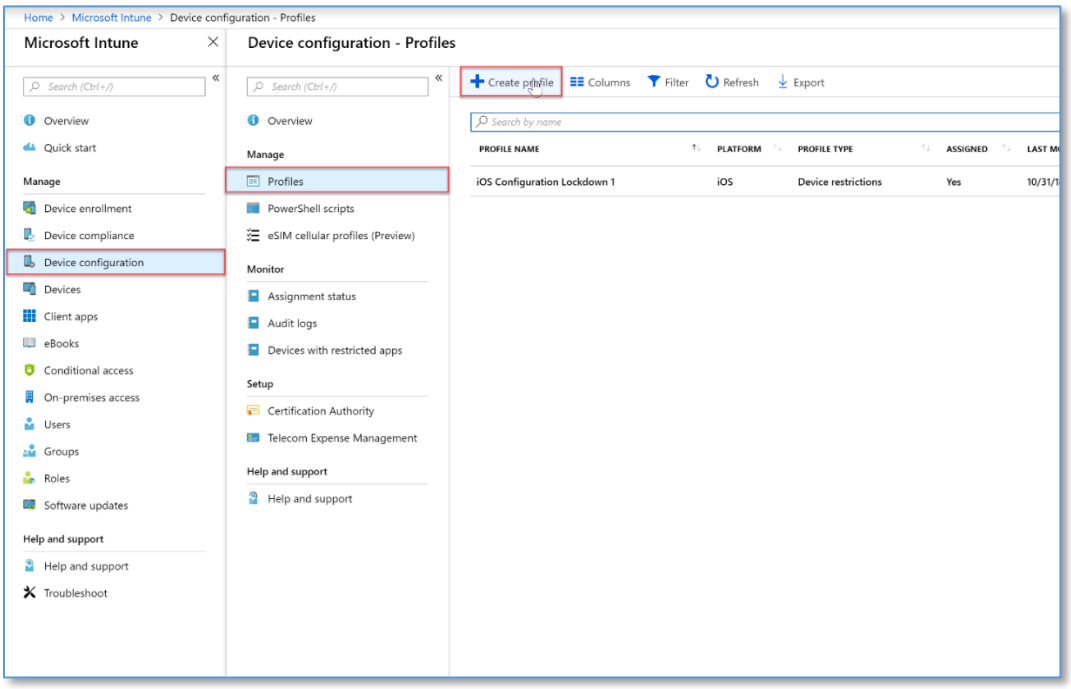


Configuration Policies

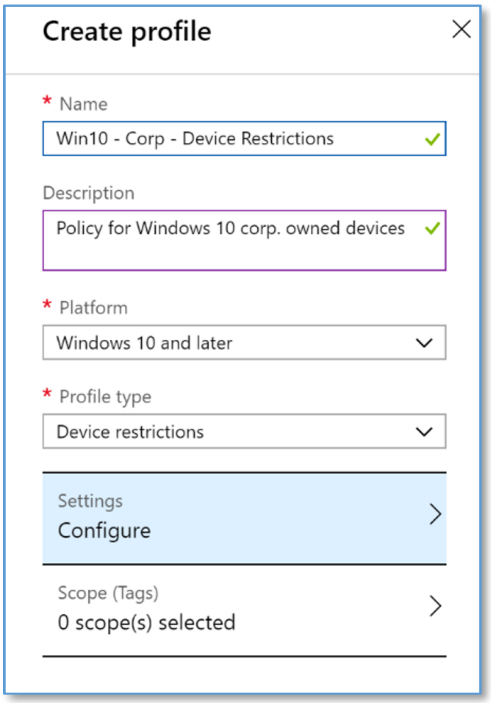
Commonly used to manage security settings and features on your devices, including access to company resources. In this walk-through, we'll create a policy for a Windows 10 device, that requires a complex password, sets a screen-lock time limit, and enables Windows Hello!:

Create a configuration policy

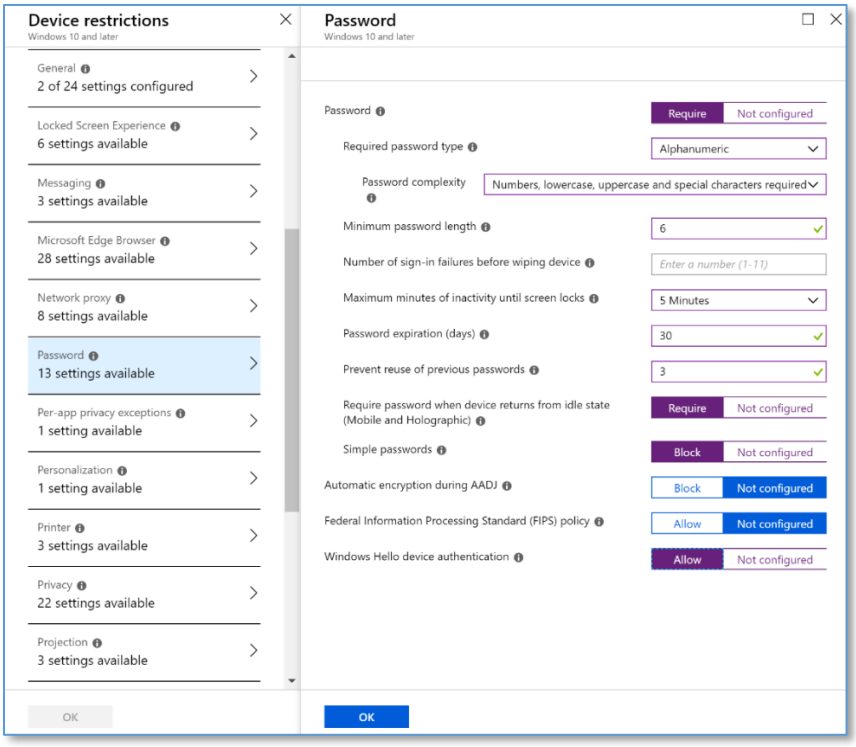
1. Expand the Intune blade and then select "**Device Configuration**", "**Profiles**" and then click "**Create Profile**" to create a new device configuration profile:

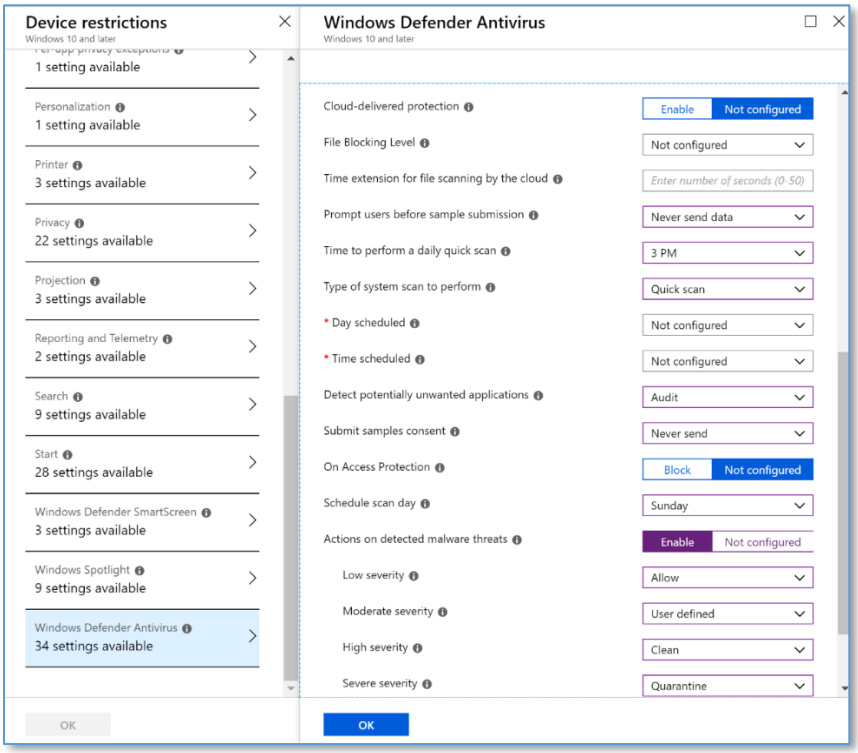


2. Enter the appropriate information regarding your profile/policy. In our example I will be making a policy that is applied to corporate owned Windows 10 devices:

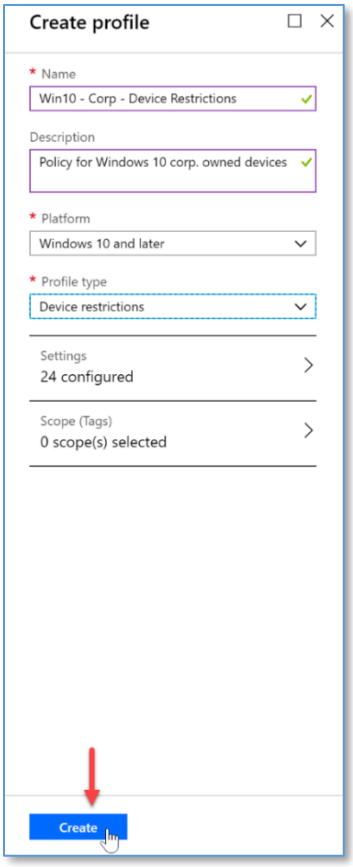


3. Select the the required settings for this policy:

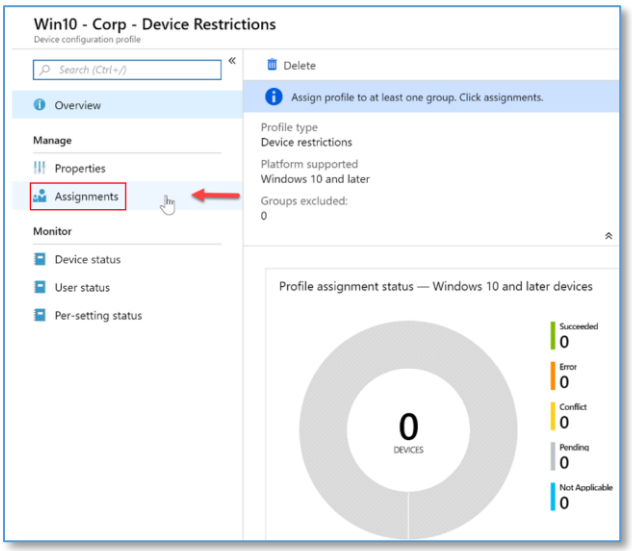




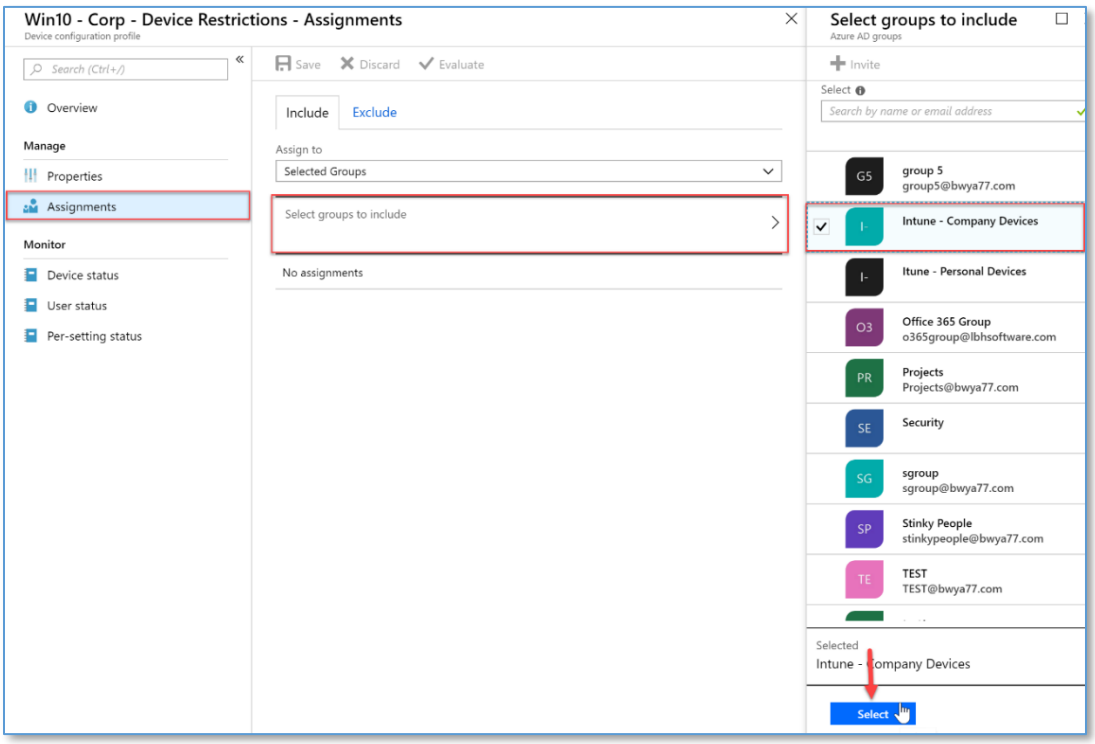
4. Once you have configured all of the settings, press "**Create**" under the create profile blade:



5. Next, click "**Assignments**" so we can assign this policy:



6. From there I will select my Intune – **Company Devices** group to apply this policy to:

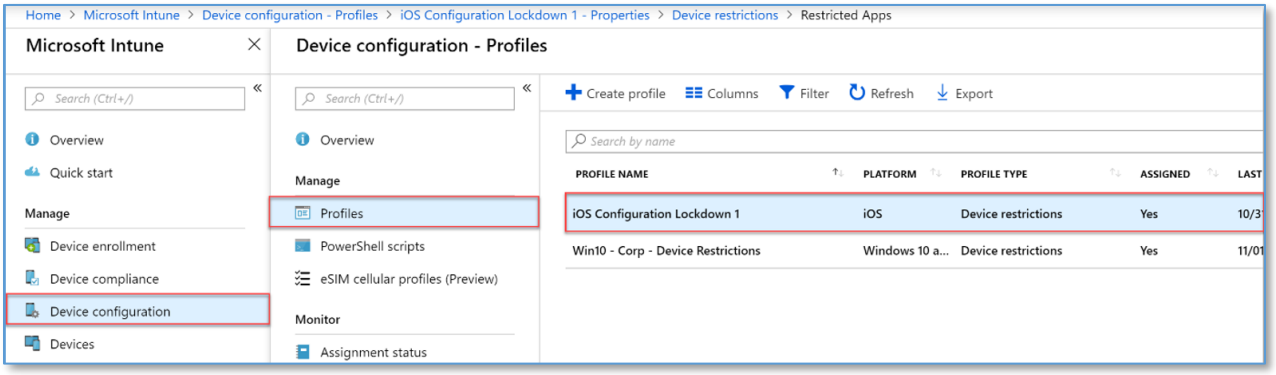


Uninstall restricted applications policy iOS

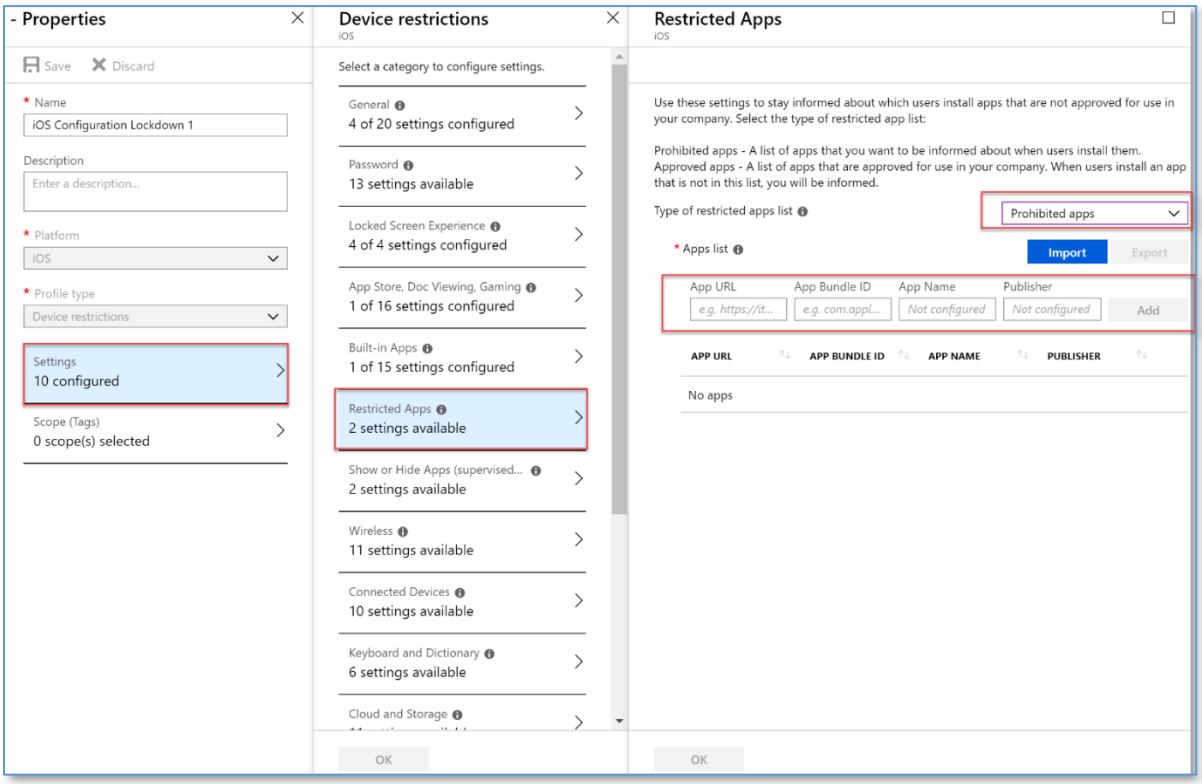
In this example I will be configuring a restricted application and applying it to my iOS devices. Restricted applications are applications that users are not allowed to install and run. Users are not prevented from installing a prohibited app, but if they do so, this is reported to you.

1. In the Intune blade select **Device configuration** > **Profiles,** then select the profile you want to edit, or create a new one. In our example, we will modify the profile applied to iOS

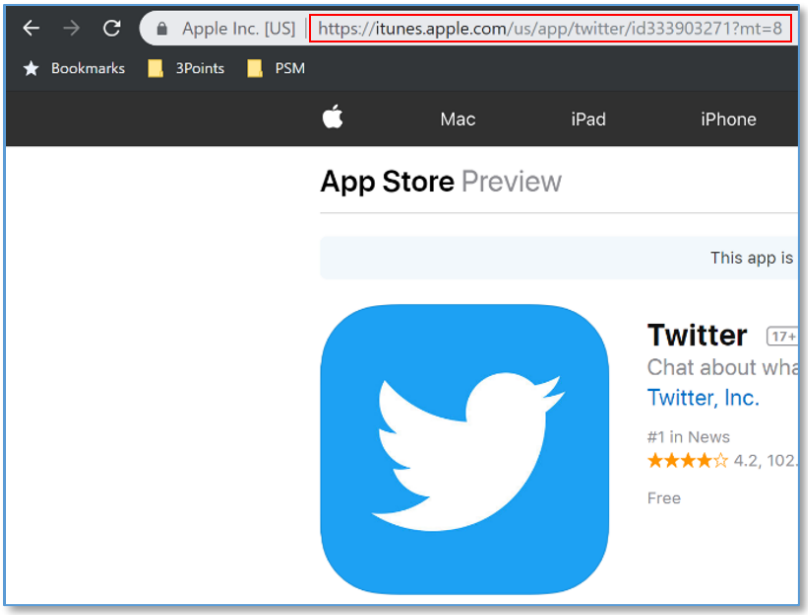
devices:



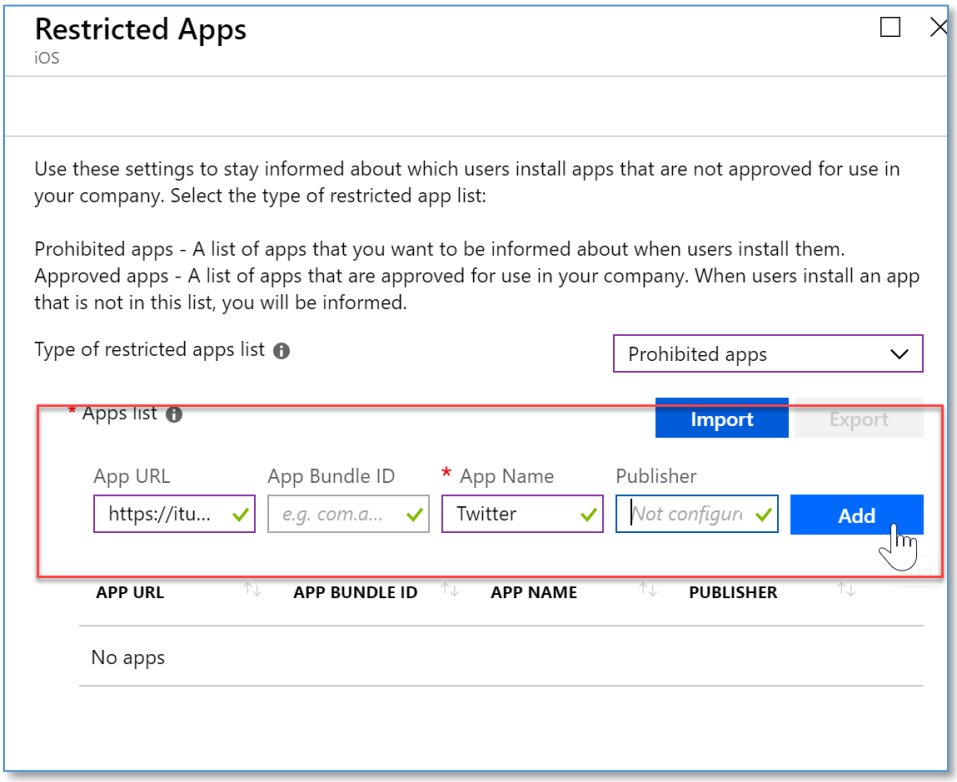
2. In the profile select **Settings** > **Restricted Apps**, and then under type of restricted apps list select **Prohibited Apps**.



3. Open a tab in a browser, look up the application you want to block, and Copy the itunes store URL:



4. Back in the Azure Portal, paste the link into **App URL** and then click "**Add**":



5. When you have finished your apps list, click **OK** at the bottom and then save your policy.

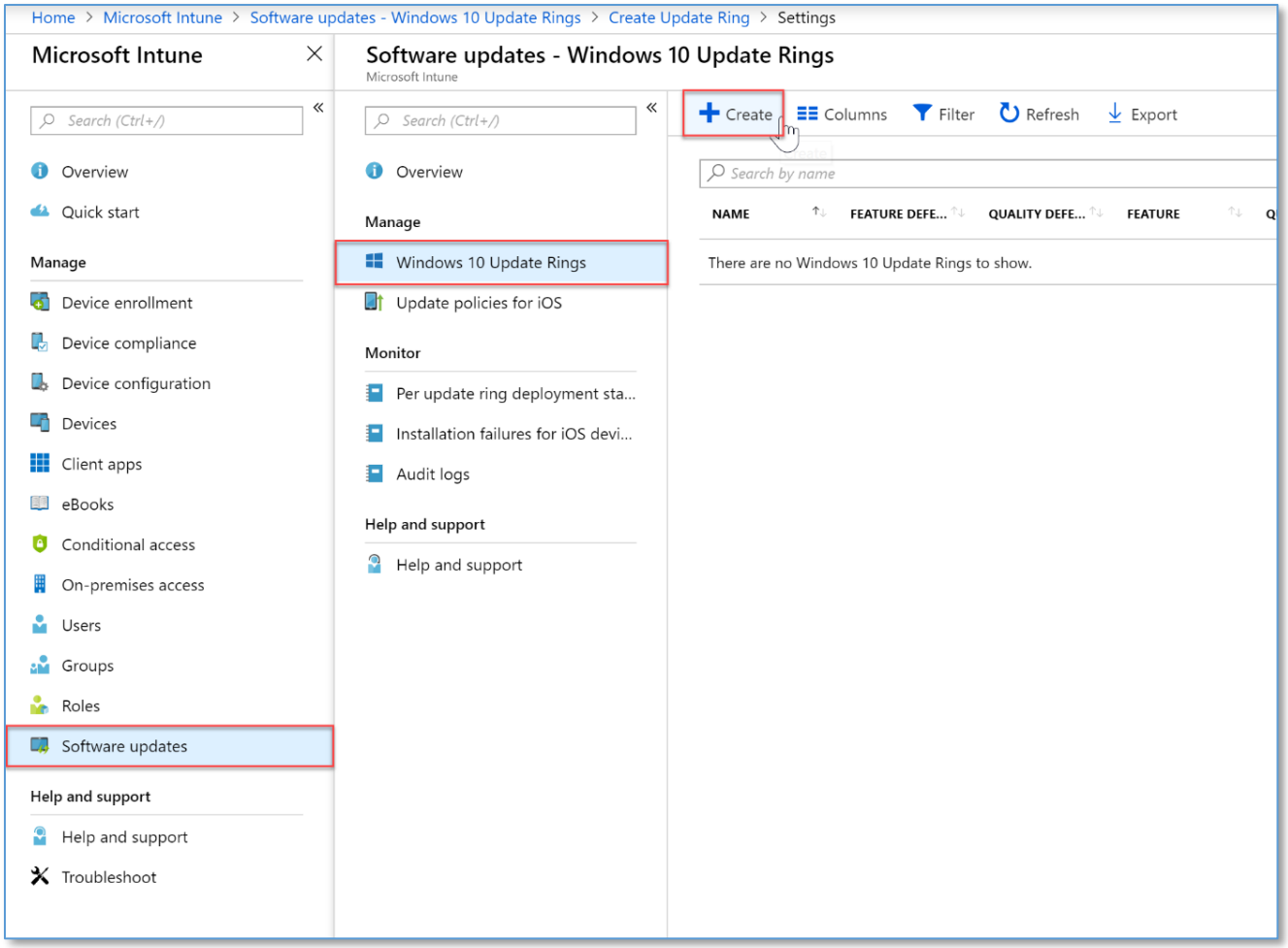
- The company portal will display a message that I must uninstall the Twitter application since it is now a disallowed application:

Software Update Policies

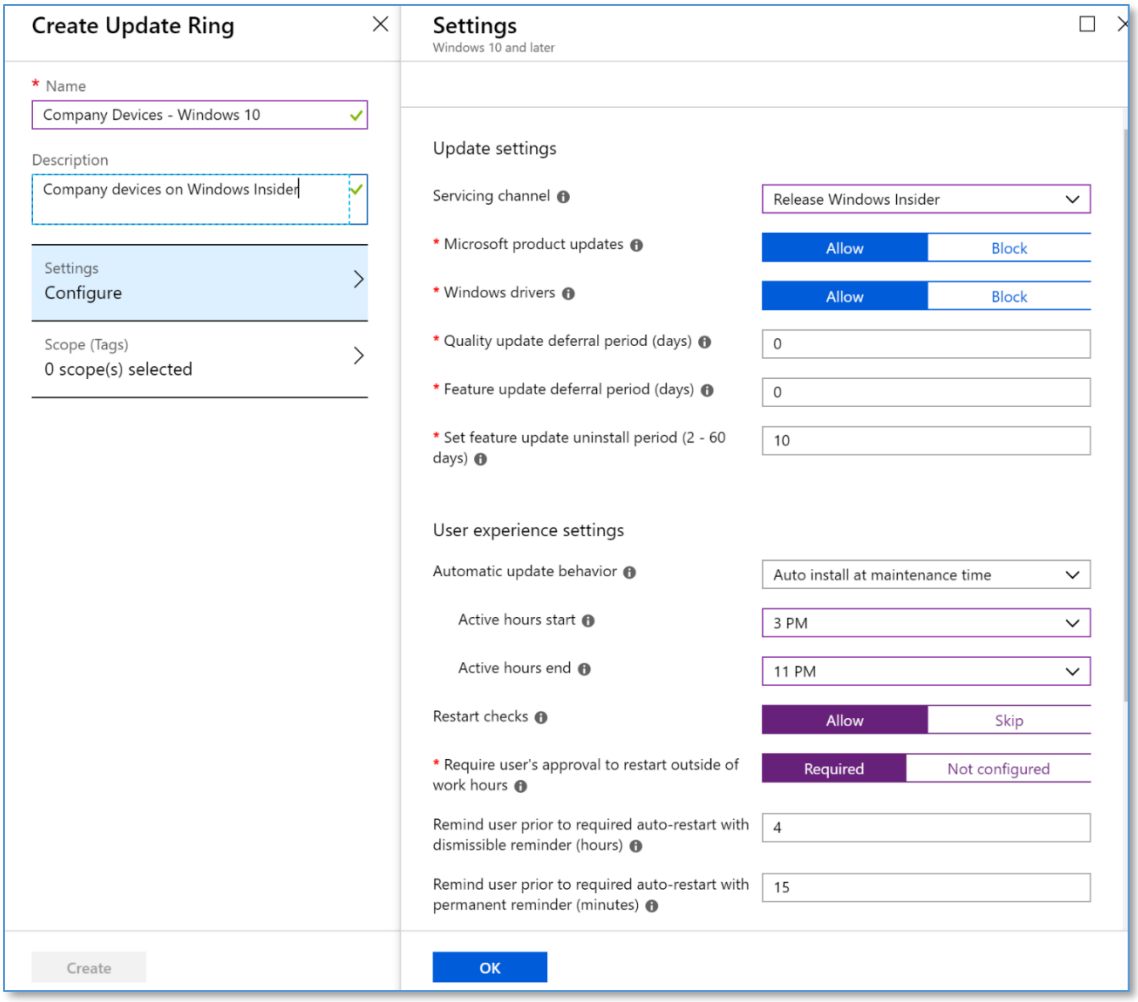
With Software Update Policies you can control when users can update to the newest iOS, you can restrict it so they cannot download it during business hours, or how long they must wait after it has been released until they can install it. With Windows Devices you can control devices servicing channel (Insider, Semi-Annual, etc), auto updates, maintenance windows, and more.

Create a Windows software update policy

1. From the Intune blade, click **Software Updates** > **Windows 10 Update Rings**, and **Create**

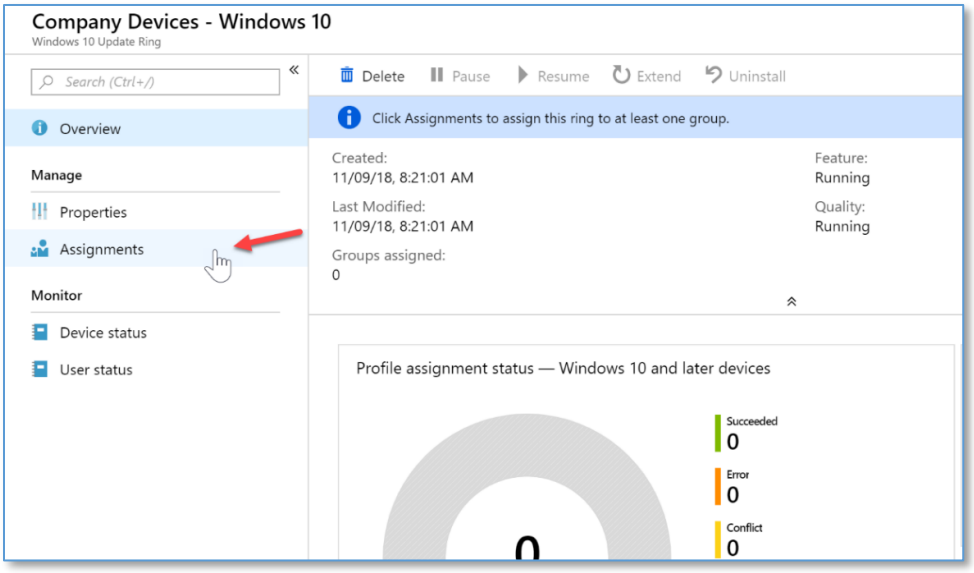


2. Give your policy a name and description. In our example, I'm putting my devices on the Windows Insider update ring. They will also get Microsoft product updates, and drivers. You can configure a deferral period which may be recommended for a production environment. In the User Experience Settings administrators can configure maintenance hours, in my environment I am auto installing the updates anywhere from 3PM to 11PM:

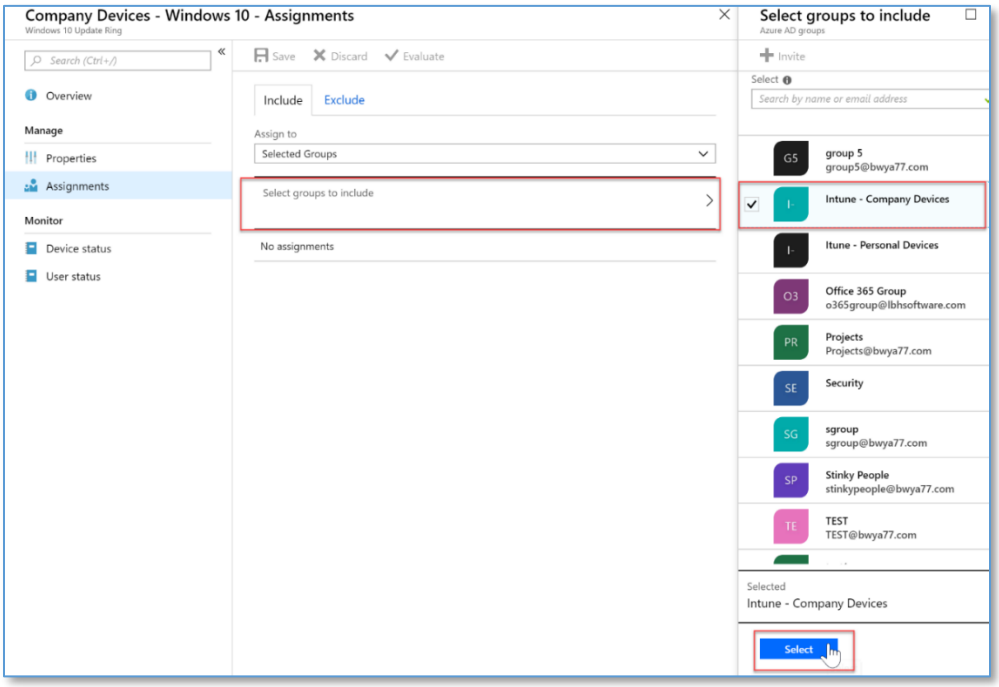


3. Once you have the policy settings configured to your needs you can add scope tags and then press "**Create**" to create the policy.

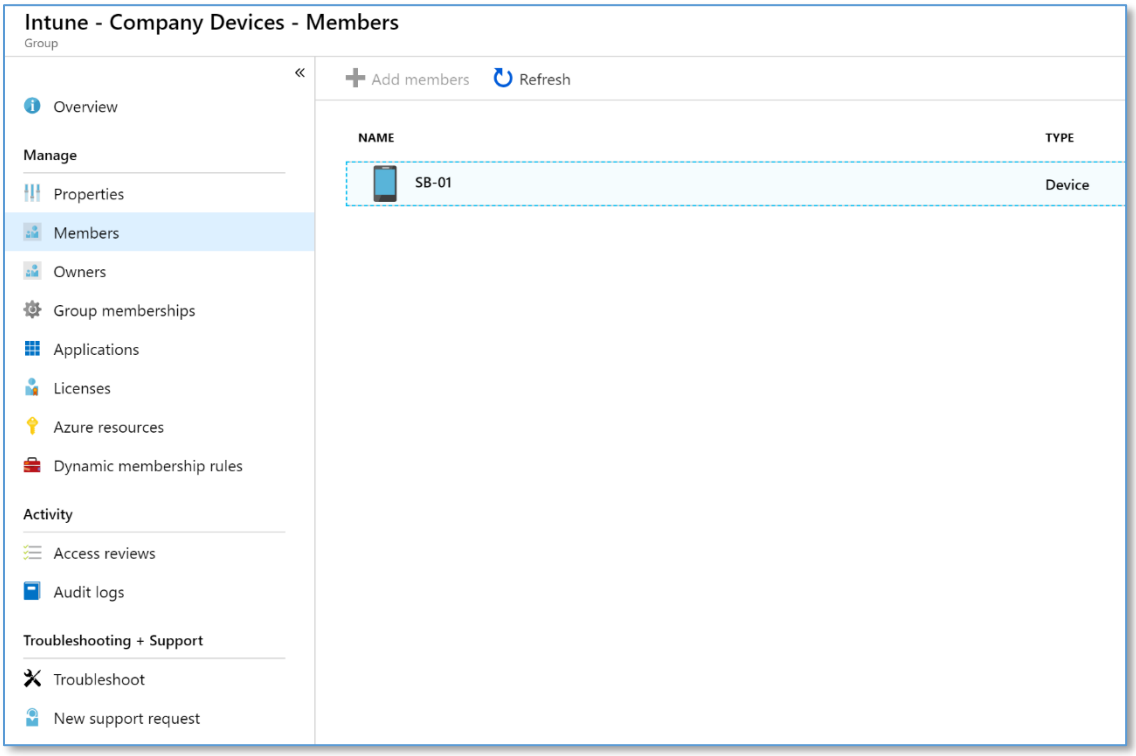
4. Once the policy has been created, click "**Assignments**" to assign the policy to devices or groups.



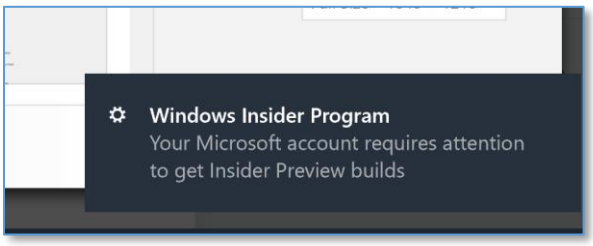
5. You can apply to all devices using the "Assign to" drop down, or in my case I will apply it to one of my dynamic groups I created earlier by clicking the "Select groups to include" and then selecting my "Intune – Company Devices" group:



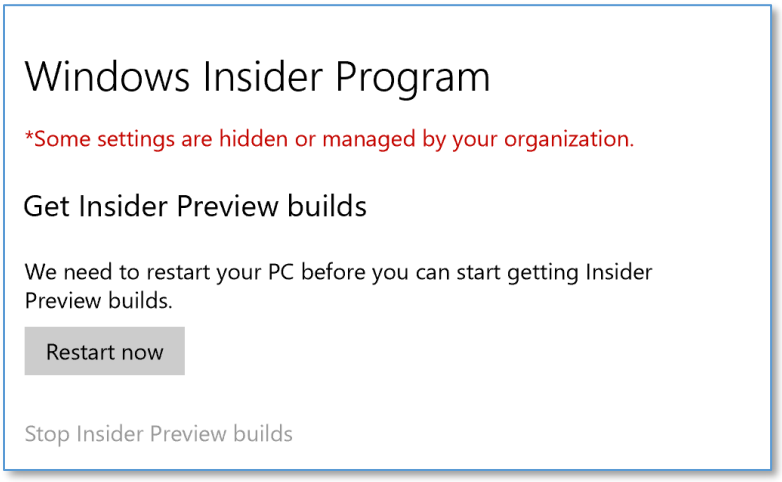
6. In my Group settings I can see that my windows machine SB-01 is a member of that group so I can be sure that the policy will be applied to that machine:



7. A few minutes later, that machine gets a toast notification regarding my build change:

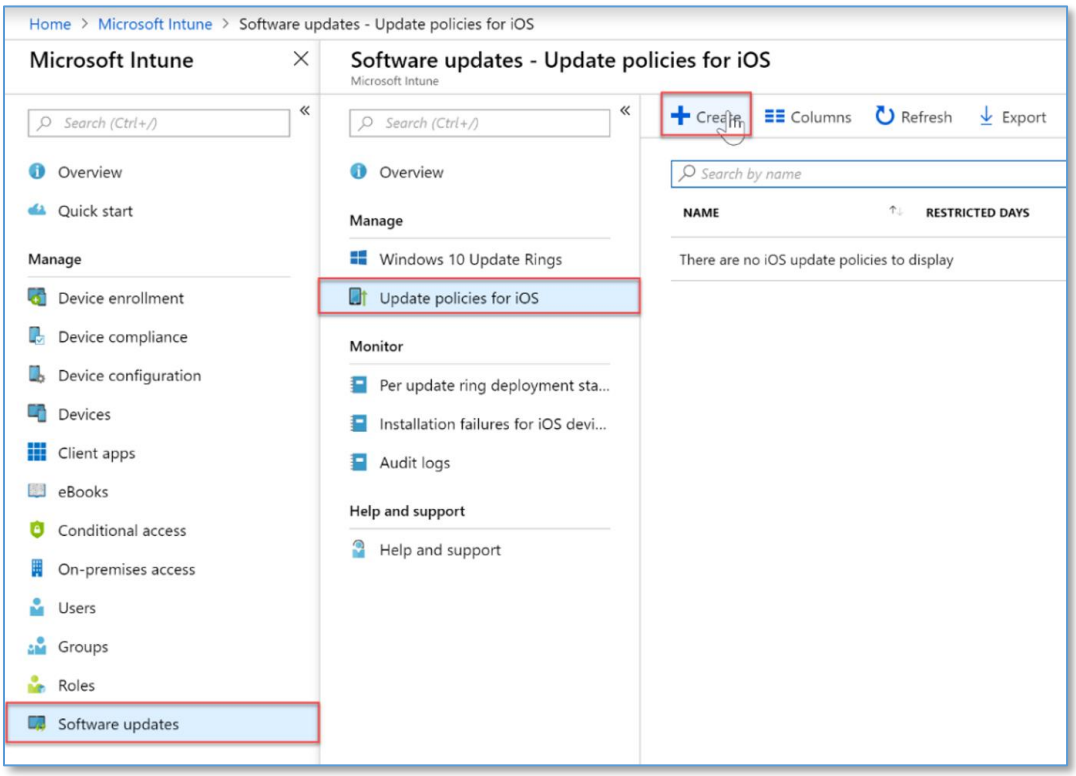


8. In the Settings application on the device I can see that my computer is pending a reboot. After the reboot I will be on the correct build:

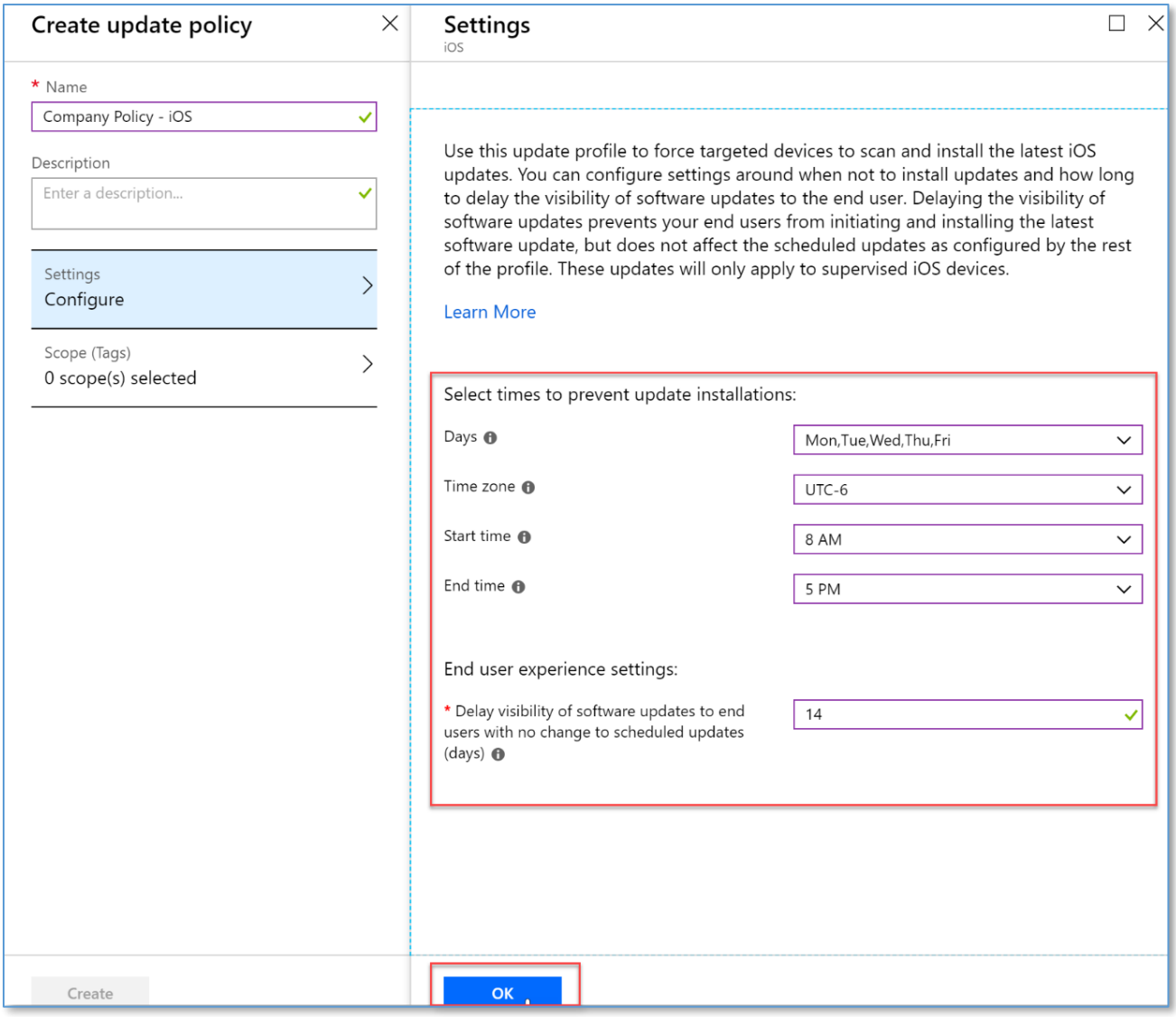


Create an iOS software update policy

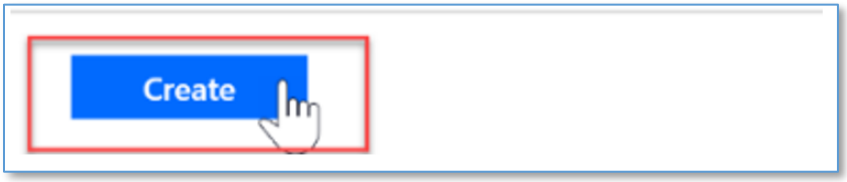
1. Select the Intune blade > **Software Updates** > **Update Policies for iOS**, and then "**Create**"



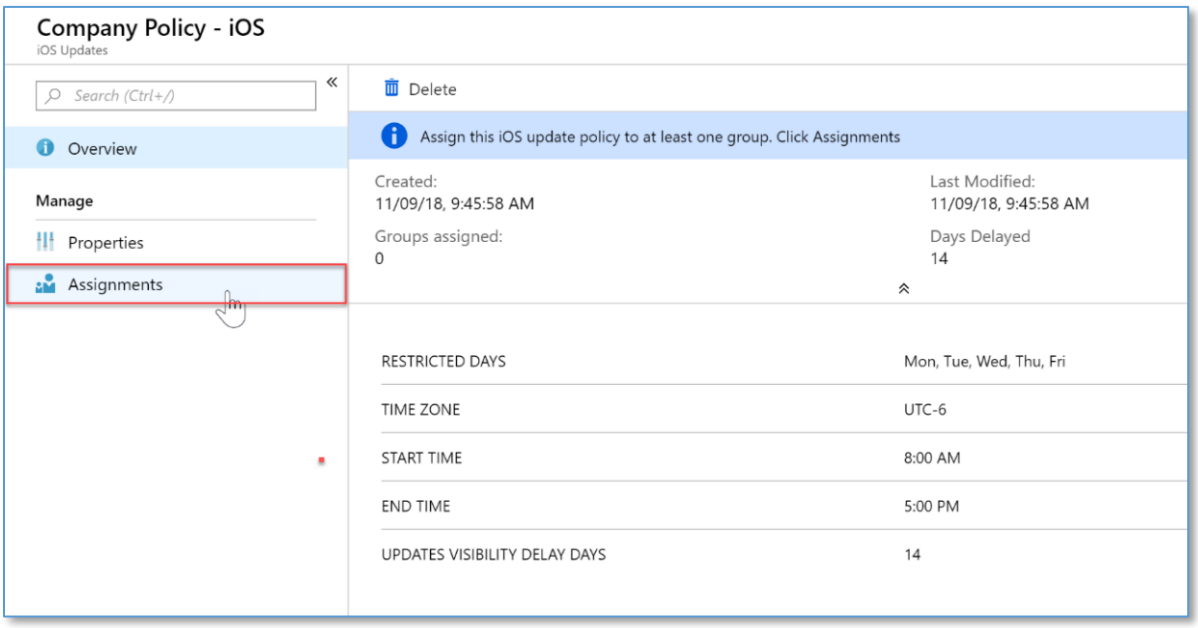
2. Give the policy a name and a description and then configure your settings. In my example I am disabling users from updating to the newest iOS during the work week and during work hours. iOS updates are also deferred for 2 weeks:



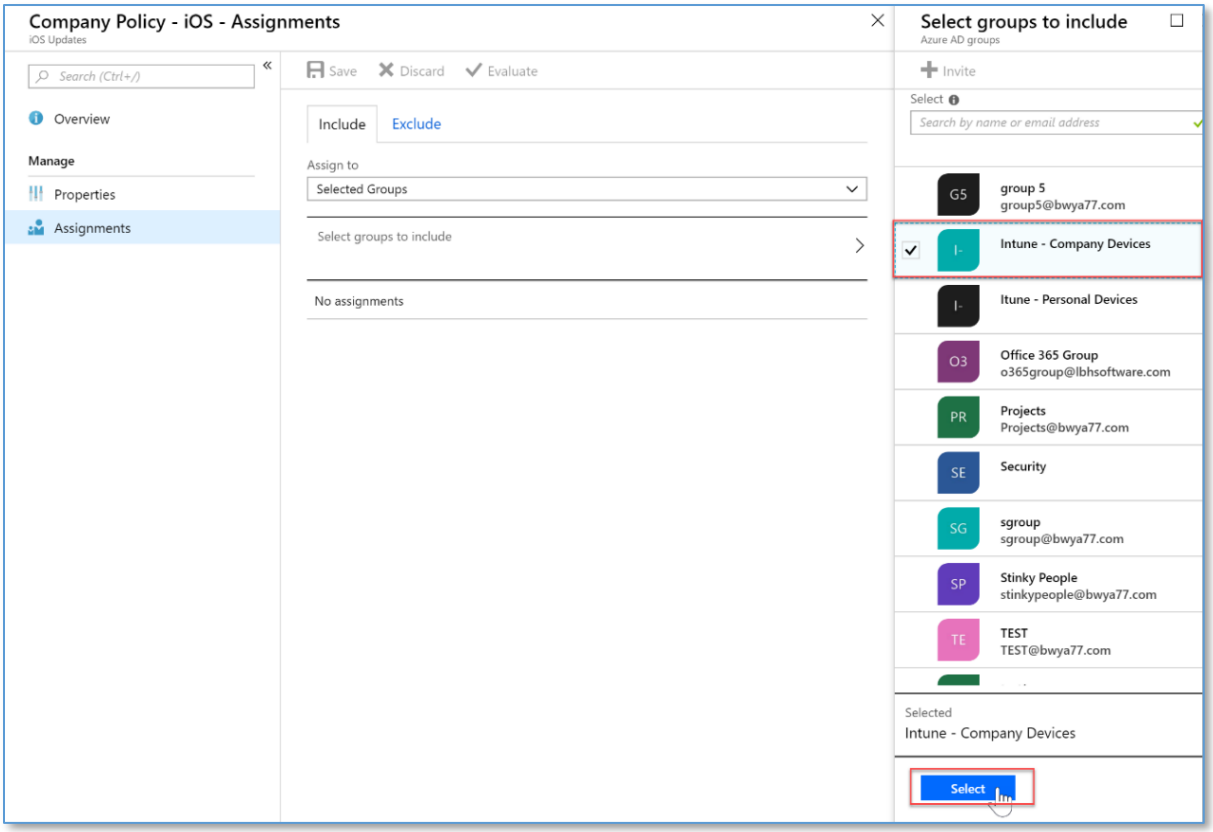
3. Once you have your policy set to your liking, press the **Create** bottom of the blade:



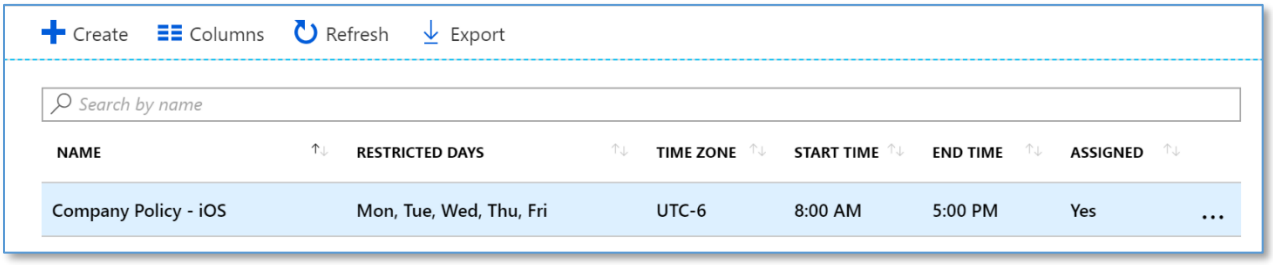
4. Click "**Assignment**" to assign your policy to groups or devices.



In my example I will apply this policy to Company Devices only:



5. You will now see your newly created policy:

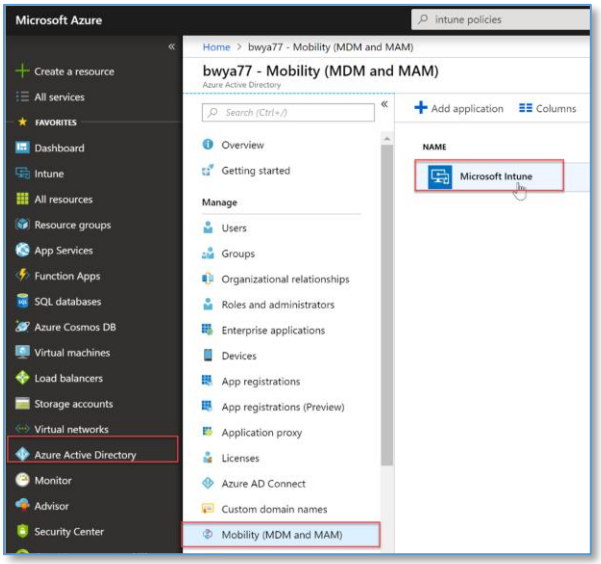


7. Device Enrollment

Enable automatic enrollment for Windows 10

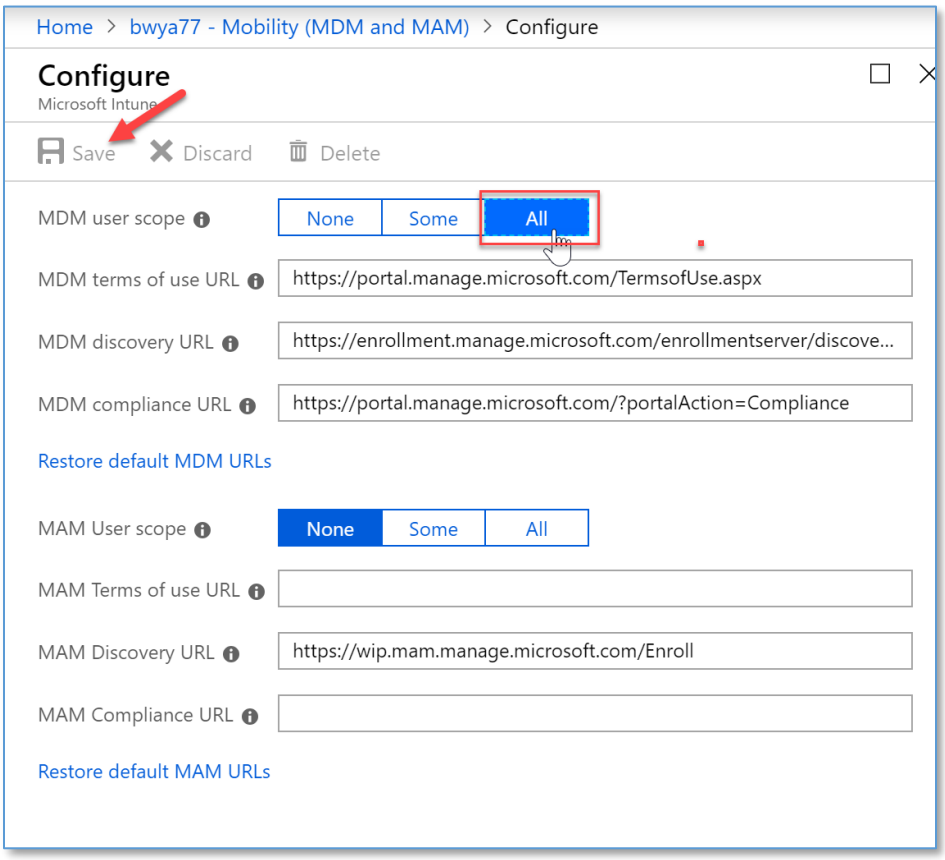
Automatic enrollment lets users enroll their Windows 10 devices in Intune. To enroll, users add their work account to their personally owned devices or join corporate-owned devices to Azure Active Directory. In the background, the device registers and joins Azure Active Directory. Once registered, the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

1. In the Azure Portal select **Azure Active Directory** and then click "**Mobility (MDM and MAM)** and select "**Microsoft Intune**":



2. Configure MDM User scope. Specify which users' devices should be managed by Microsoft Intune. These Windows 10 devices can automatically enroll for management with Microsoft Intune.

   - None – MDM automatic enrollment disabled
   - Some – Select the Groups that can automatically enroll their Windows 10 devices
   - All – All users can automatically enroll their Windows 10 devices

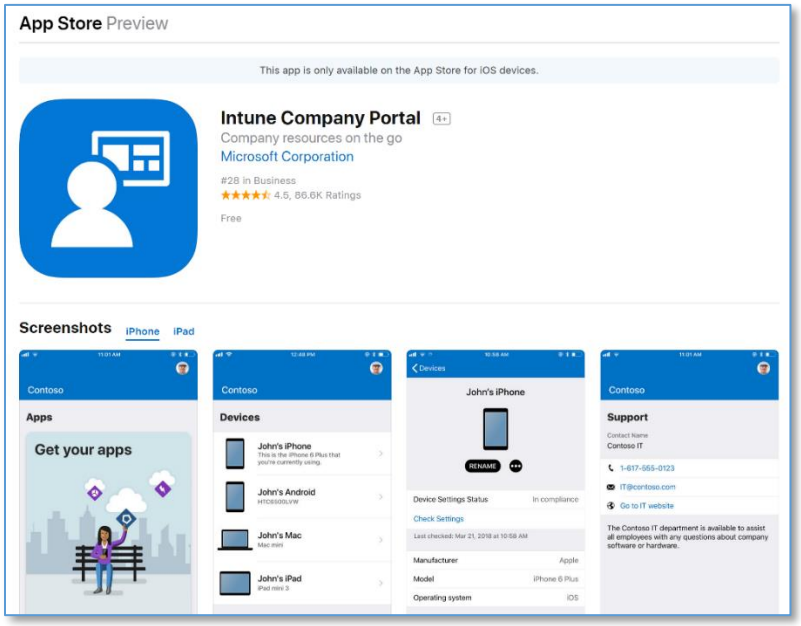


Important:

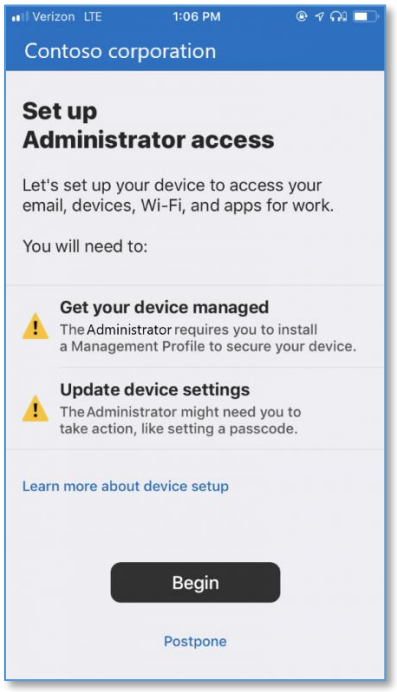
If *both* InTune Mobile Application Management (MAM) user scope and automatic MDM enrollment (MDM user scope) are enabled for a group, MAM takes precedence. In that case, only MAM is applicable to users in that group when they workplace join personal device. When MAM applies, devices are not automatically MDM enrolled.

Enable automatic enrollment for iOS

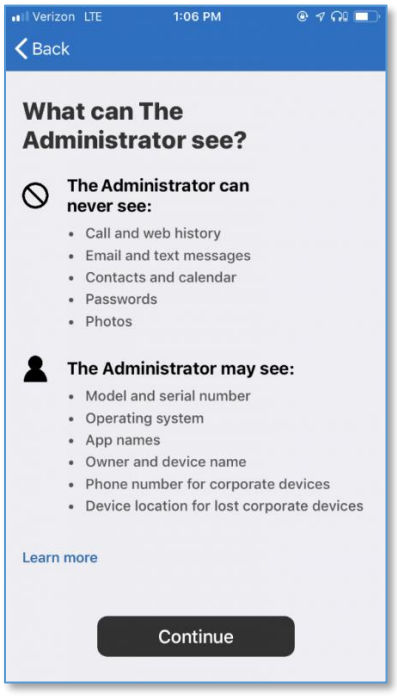
1. Users must download and install the Company Portal from the iOS App Store



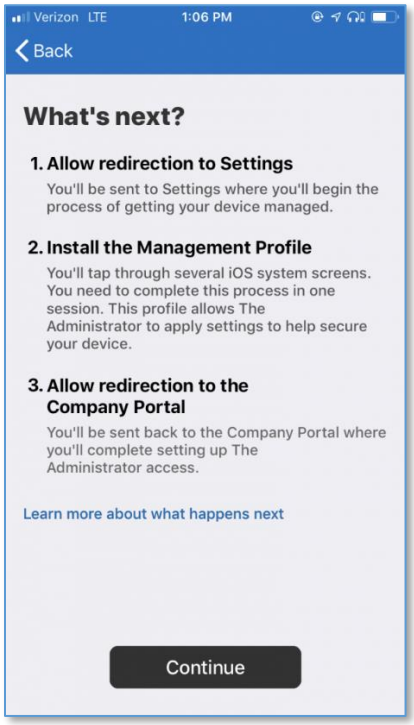
2. Once they launch the application and sign in they can begin to Intune enrollment process:



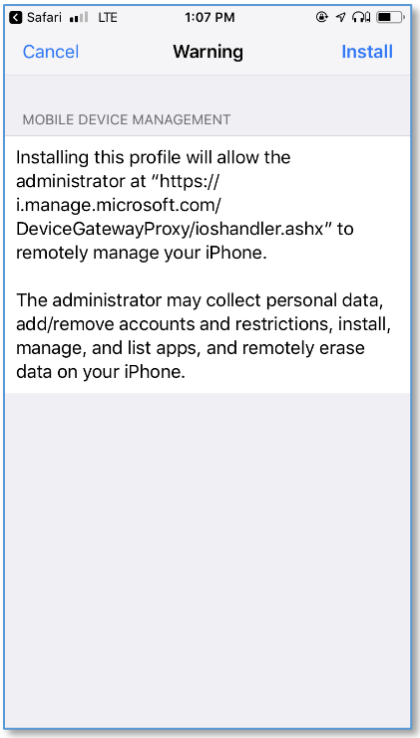
3. The application will show the end user the permissions the IT Administrator will have on the device:

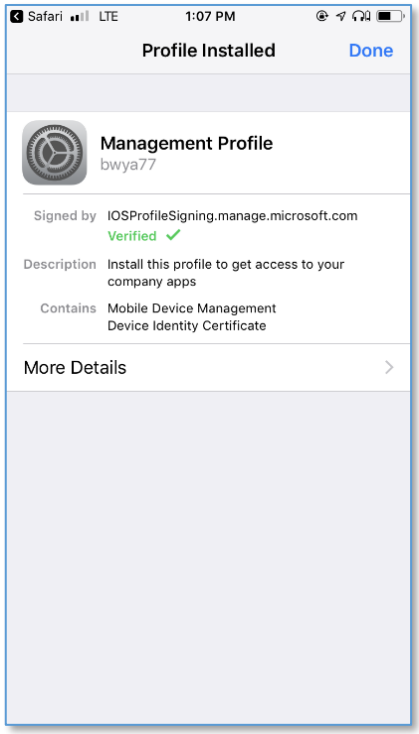


4. They will then be shown the step by step instructions that the application will take to enroll the device:

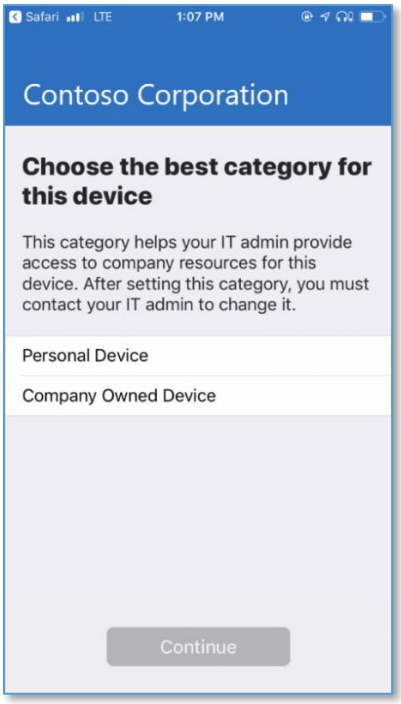


5. An MDM iOS Profile will be installed on the device:

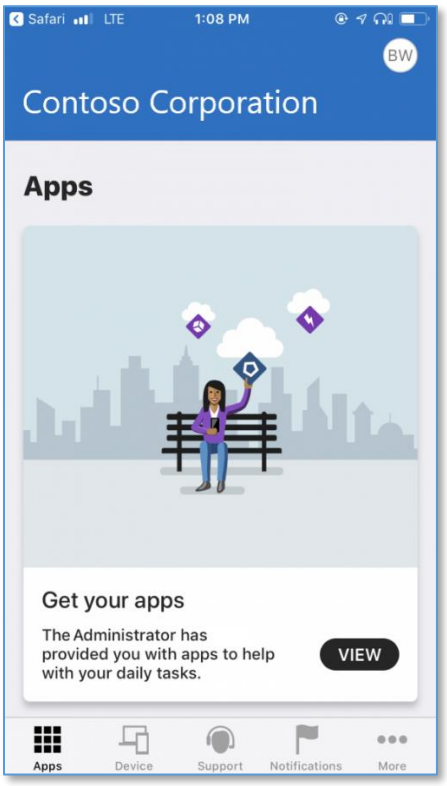




6. And finally, the user will select a category (set up earlier) to put their device under. This allows for a better administrator management experience:



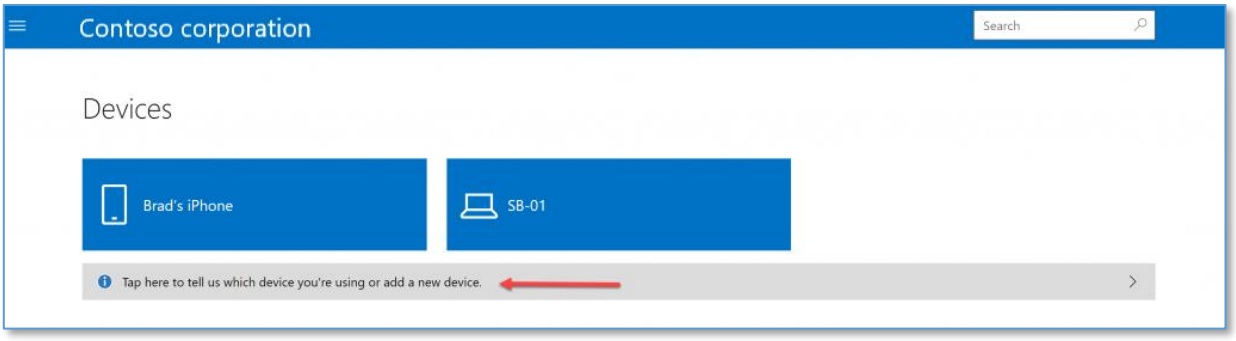
The Company Portal will show the end users any available apps you have granted them, all of their Intune devices, support options we set up previously and notifications:



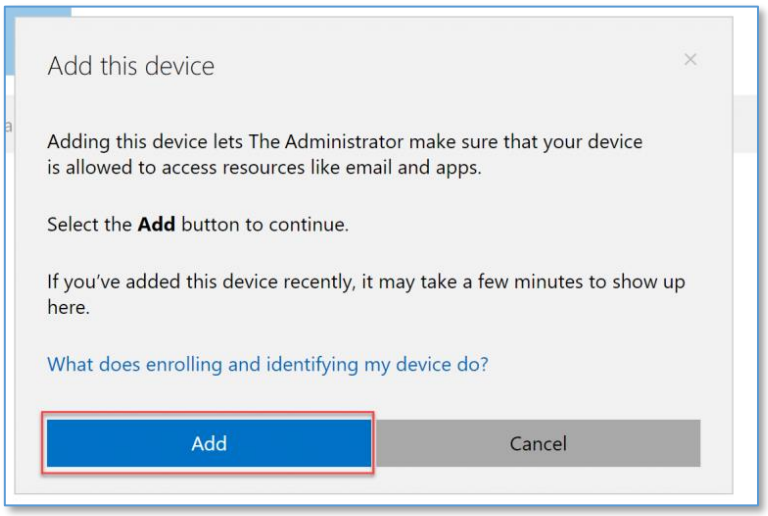
Enrolling Windows devices manually

Windows users can install the Company Portal from the Windows store, use the web Company Portal, or use the Windows Settings app to enroll their Windows devices into Intune.

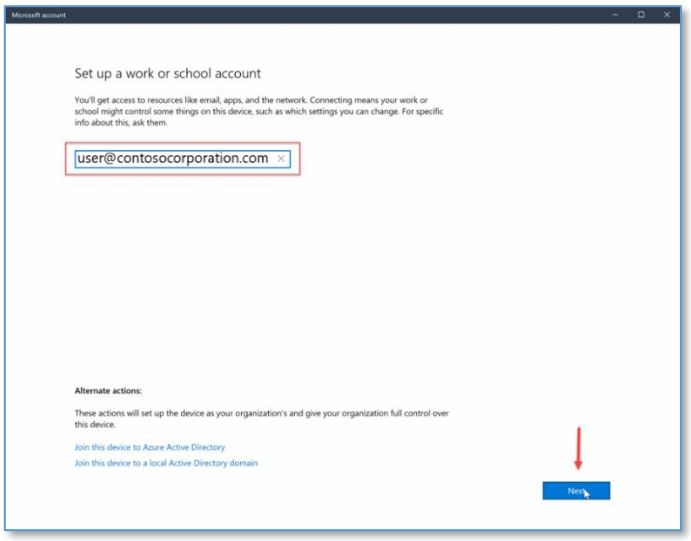
1. Navigate to the online Company Portal at https://portal.manage.microsoft.com
2. Once the user signs into the Company Portal they can add a device under Devices



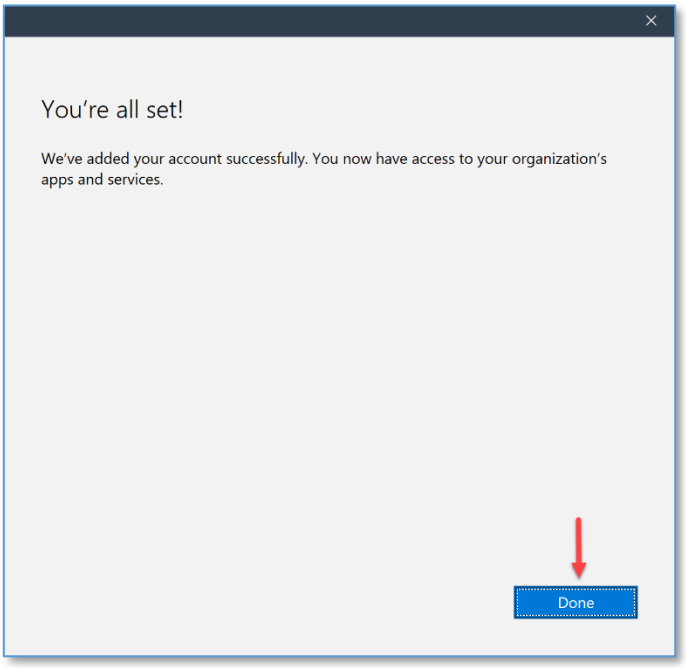
3. Click "**Add**"



4. Have them sign in and then press **Next:**

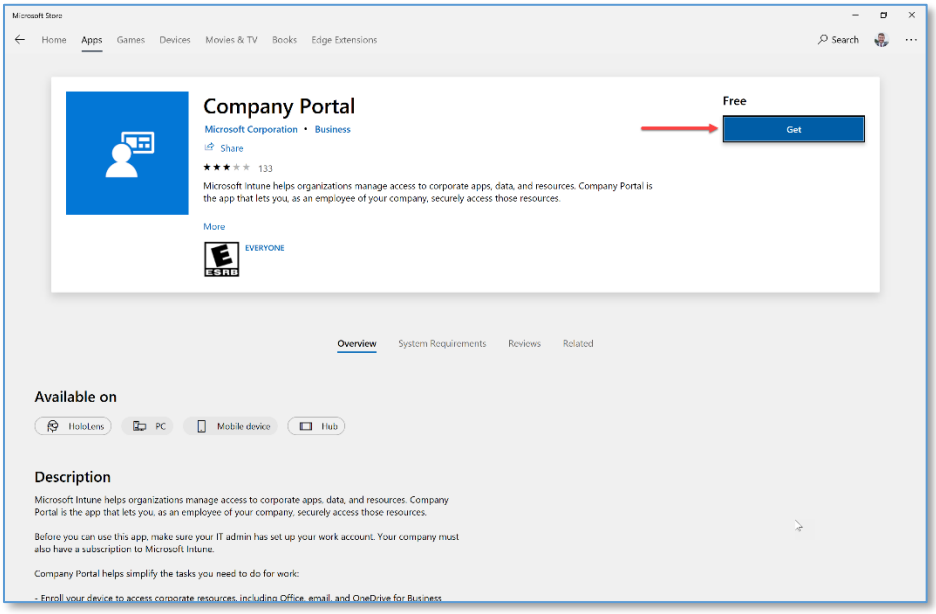


5. The user will be prompted to enter their account password and then press "**Sign In**". Once complete they will be prompted with a successful message.

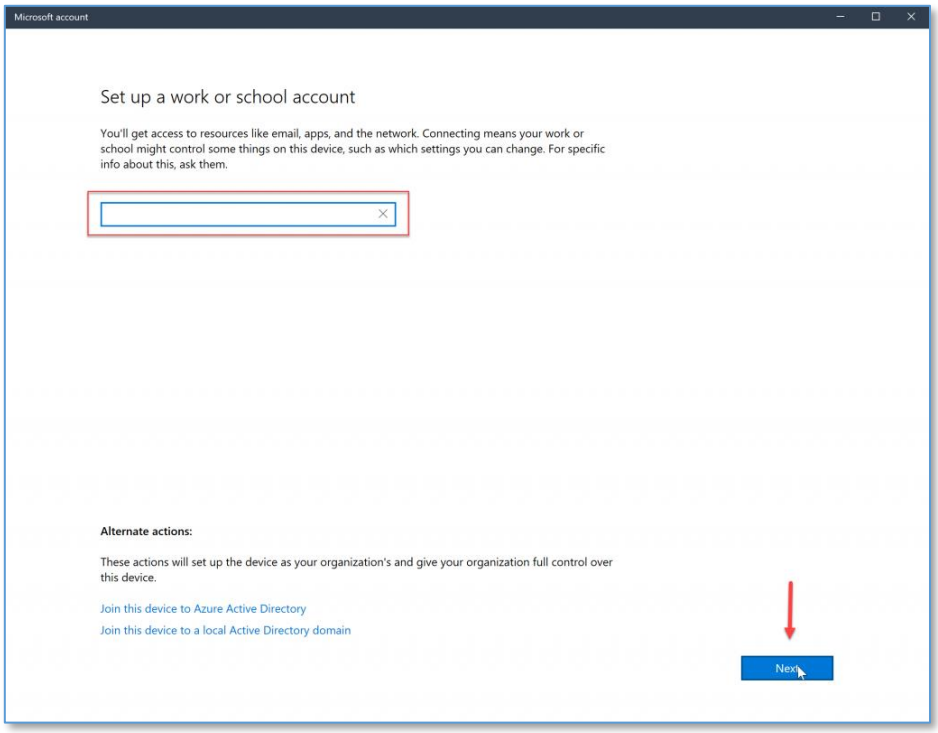


Microsoft Store App

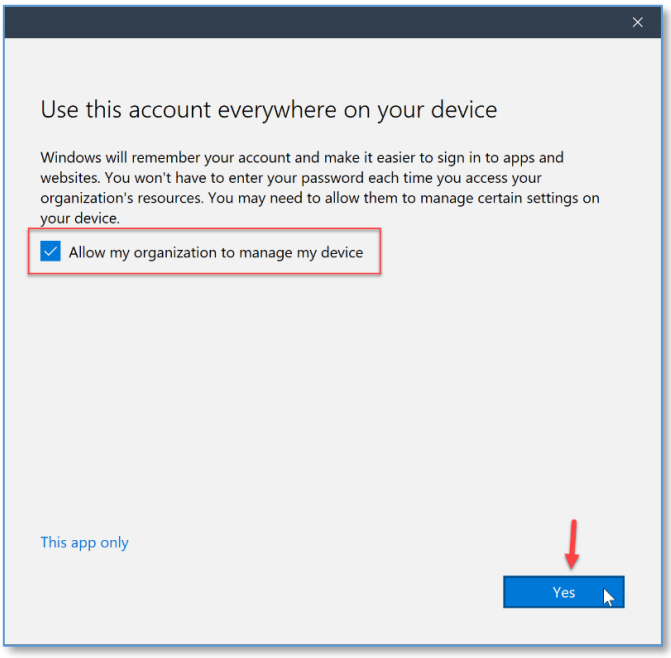
Have your users download and install the Company Portal application from the Microsoft Store:



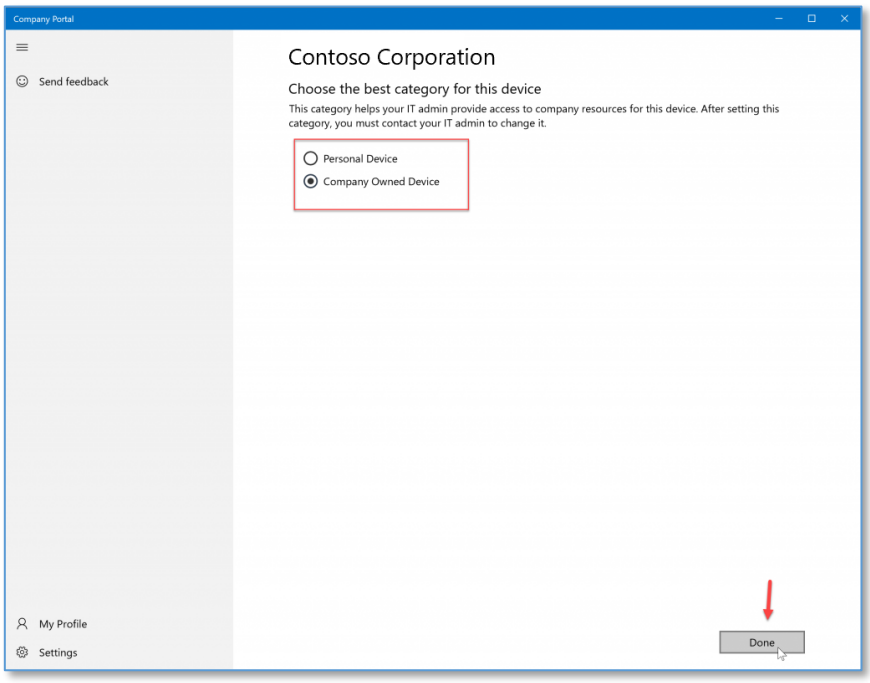
They will be prompted to sign in, then click **Next**:



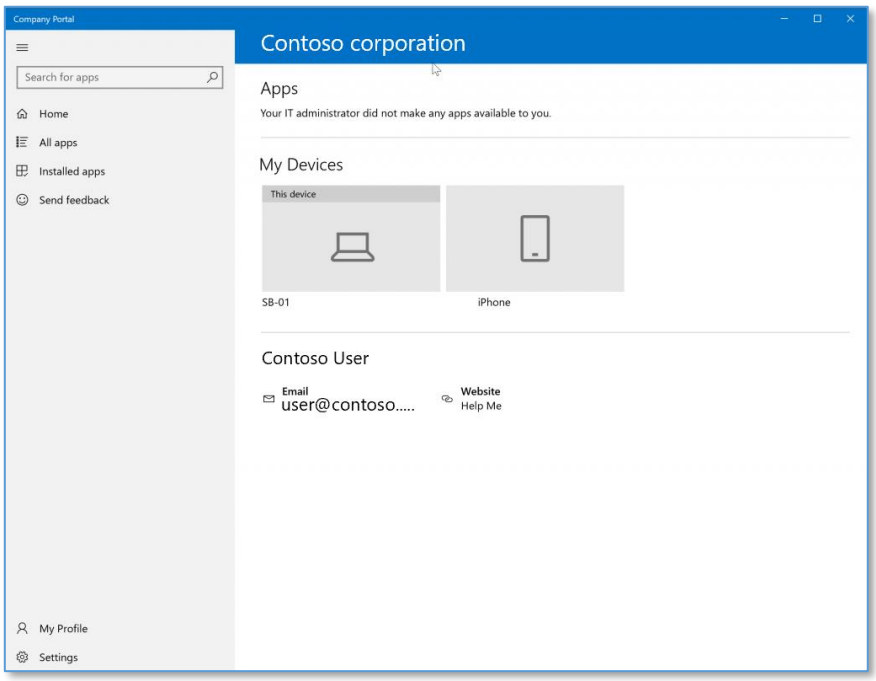
Check "Allow my organization to manage my device" and then click Yes



Finally, the Company Portal will prompt them to select a device category that we set up earlier



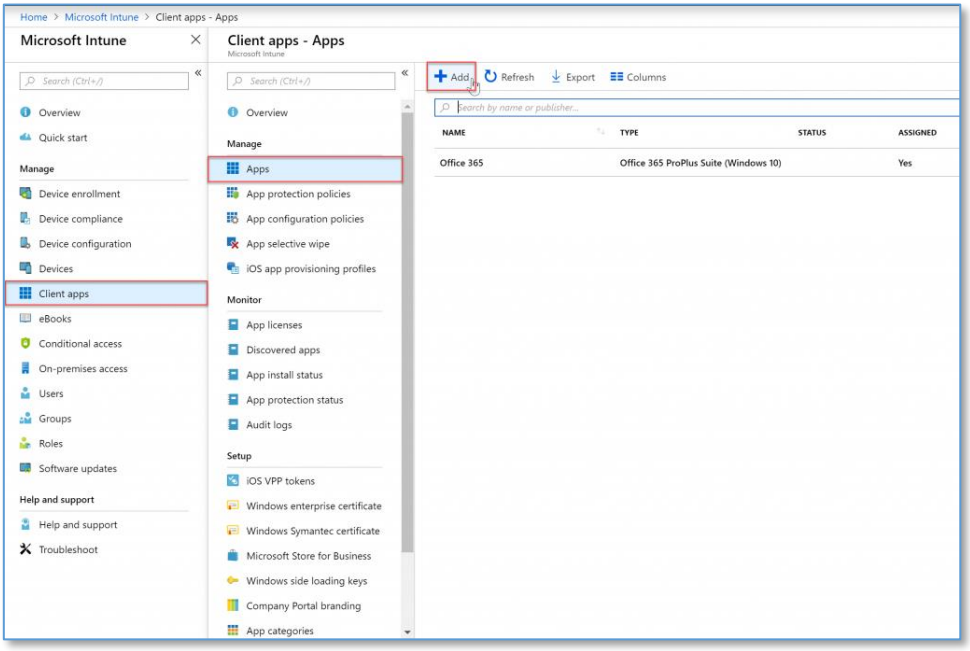
The Company Portal will now show the newly enrolled device:



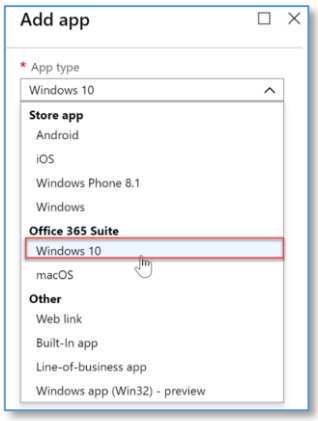
Deploy Client Apps to Managed Intune Devices

The Company Portal allows an administrator to push, install, uninstall, and make available, applications for end users. Applications can include Office 365 apps, web apps, Microsoft Store apps, iOS Apps and more. The Company Portal will only display applications that are relevant to the device they are on, (i.e. if they are on an iPhone it will not display your published applications for Windows even if the device is in the same group.)

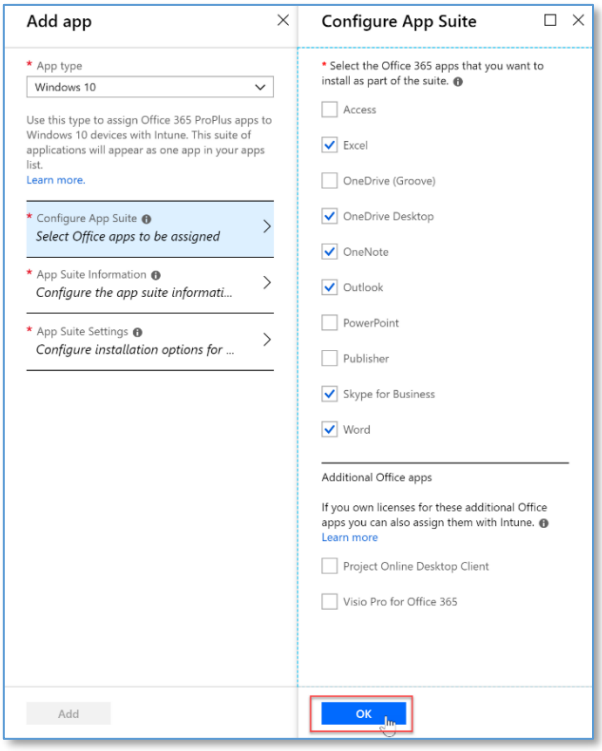
1. Expand the Intune blade in the Azure portal, go to "**Client Apps**", "**Apps**" and then select "**Add**"



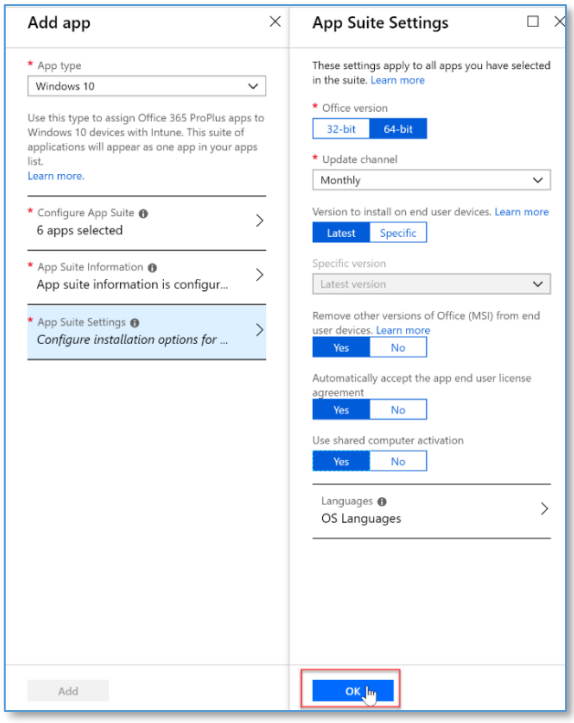
2. In my example, I'm deploying Office 365 ProPlus, so I select Windows 10 under Office 365 Suite:



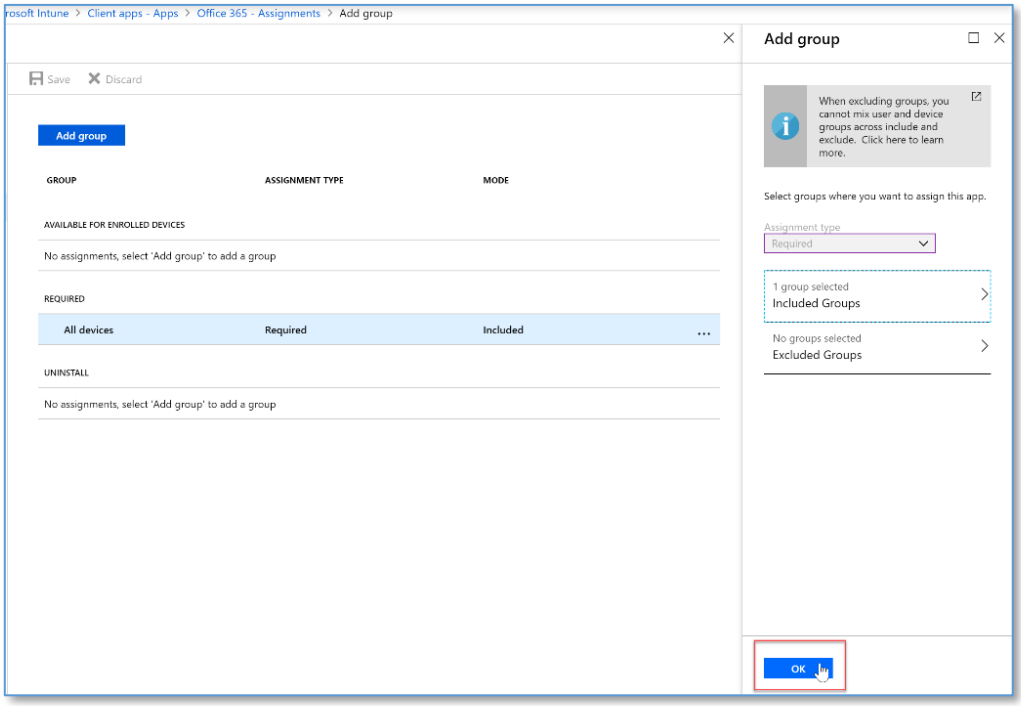
3. Configure the app settings to fit your company needs:



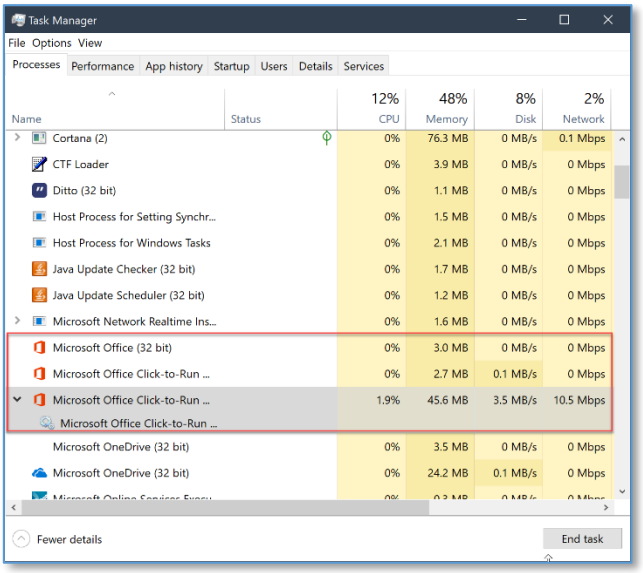
4. We can even configure the update options, EULA, and more:



5. I will make this application required for all users in my assignments setting:

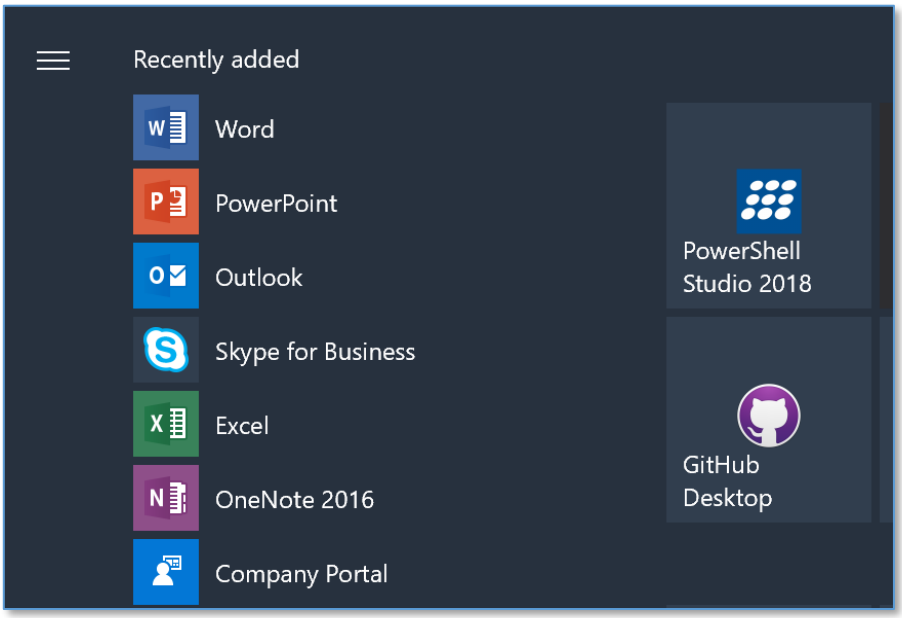


6. After a little bit I can see that Office is installing on my end user machine in Task Manager:

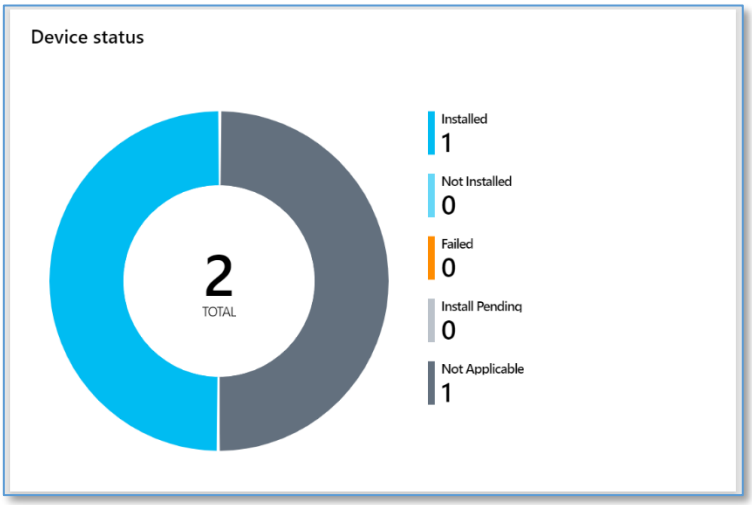


- If I had not made the app required and just made it available, end users could choose to install it from the Company Portal:

7. Once the install is complete, I can check the start menu to see all of my newly installed applications:



8. In the Intune portal under my applications, I can see that I have Office 365 ProPlus successfully installed on 1 device, and not applicable on 1 device (iOS):



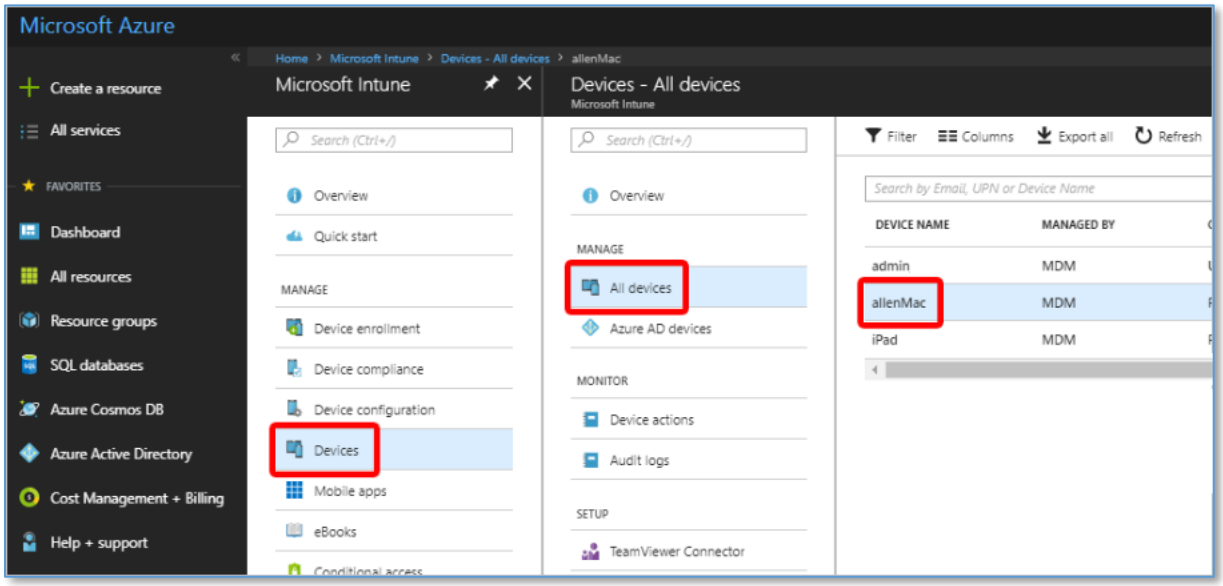
8. Device Actions

Intune also allows you to remotely manage many aspects of a users device. Using remote actions from the Intune portal, you can restart devices, reset passcodes, locate lost or stolen devices, and more.

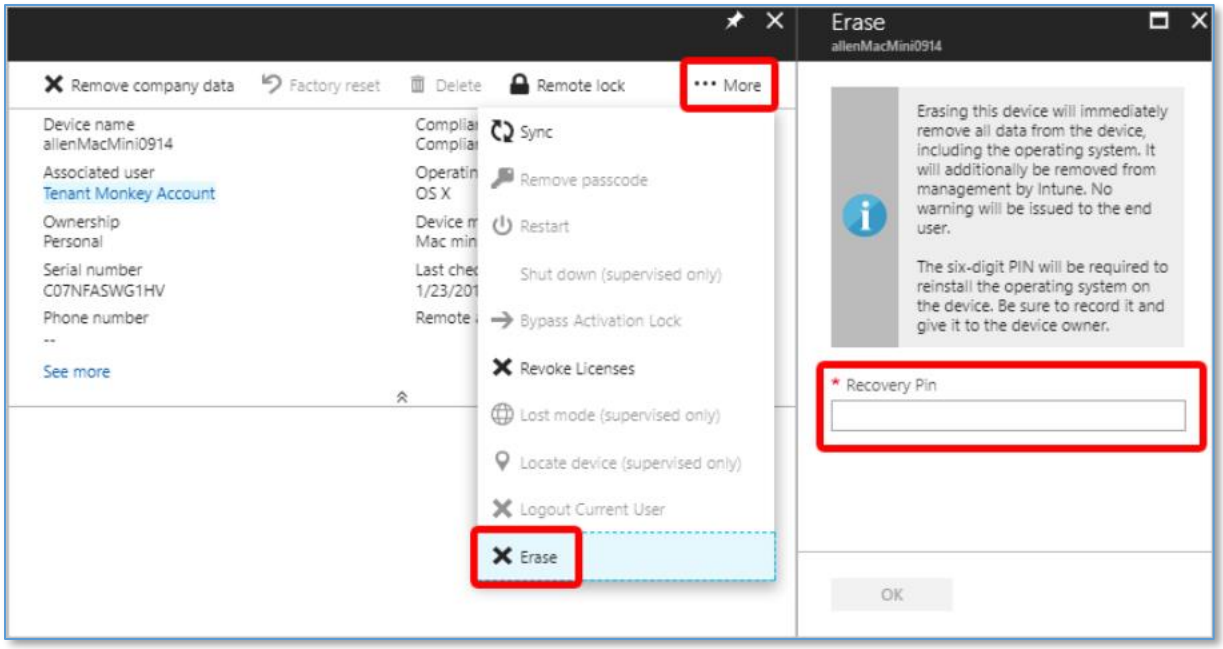
Remotely erase data from a device

In the following example, we'll force a stolen macOS device to erase it's data and operating system. Further, we'll secure it so that a 6-digit PIN must be entered, before the OS may be re-installed:

1. In **Intune** in the Azure portal, click **Devices** > **All devices** and select the device to erase. In our example, it is a macOS device called "alienMac":



2. Click **More** > **Erase** > and provide a 6-digit number as the **Recovery Pin**. This is a pin that you give to the user so that they can re-install the operating system on the device, if it's recovered. Be sure to make a note of this pin because it won't be visible after the erase action completes:



3. Click **OK**, and the device will erase itself, then lock to the Recovery Pin.

9. ATP and Intune Integration

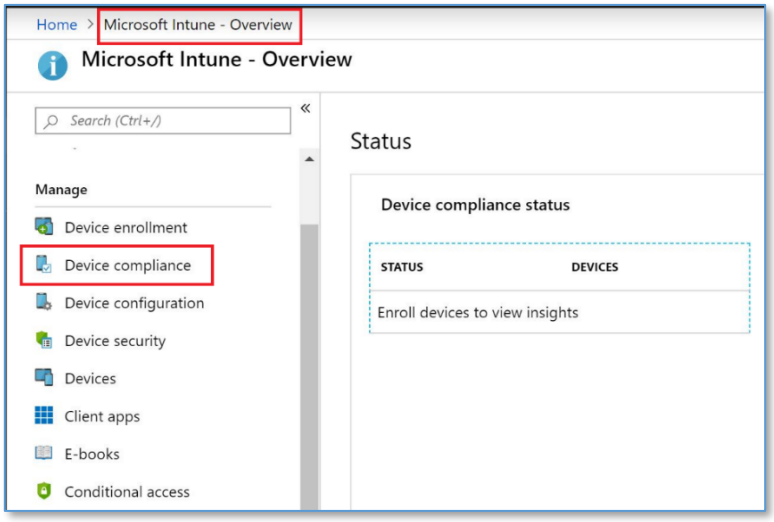
You can integrate Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) with Microsoft Intune as a Mobile Threat Defense solution, to help prevent security breaches and limit the impact of breaches within an organization. Microsoft Defender ATP works with devices that run Windows 10 or later.

To be successful, you use the following configurations in concert:

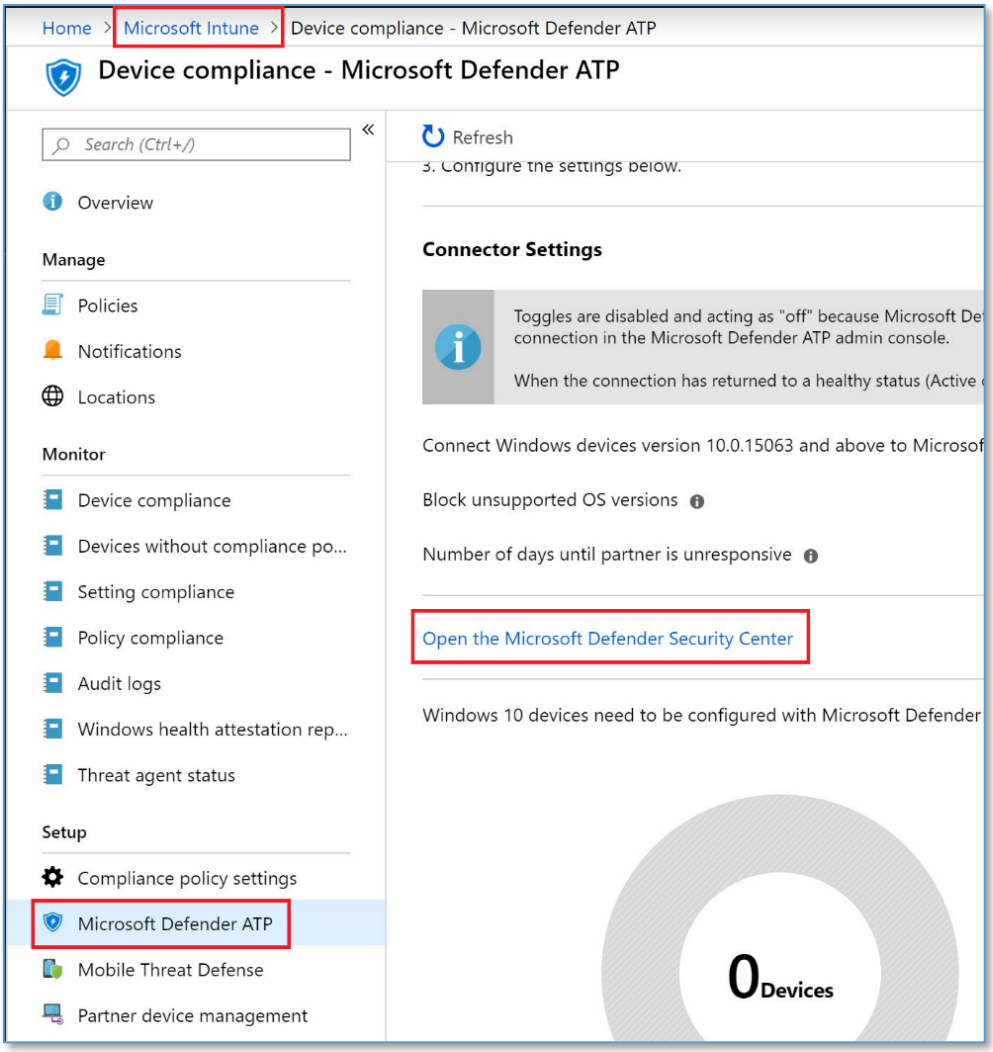
- Establish a service-to-service connection between Intune and Microsoft Defender ATP. This connection lets Microsoft Defender ATP collect data about machine risk from Windows 10 devices you manage with Intune.
- Use a device configuration profile to onboard devices with Microsoft Defender ATP. You onboard devices to configure them to communicate with Microsoft Defender ATP and to provide data that helps assess their risk level.
- Use a device compliance policy to set the level of risk you want to allow. Risk levels are reported by Microsoft Defender ATP. Devices that exceed the allowed risk level are identified as non-compliant.
- Use a conditional access policy to block users from accessing corporate resources from devices that are non-compliant

Enable Microsoft Defender ATP in Intune

1. Sign in to Intune and select **Device compliance**:

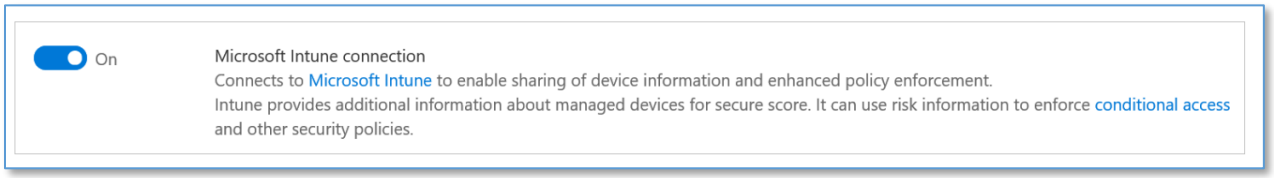


2. Select **Microsoft Defender ATP**, and then below Connector Settings, select **Open the Microsoft Defender Security Center**:



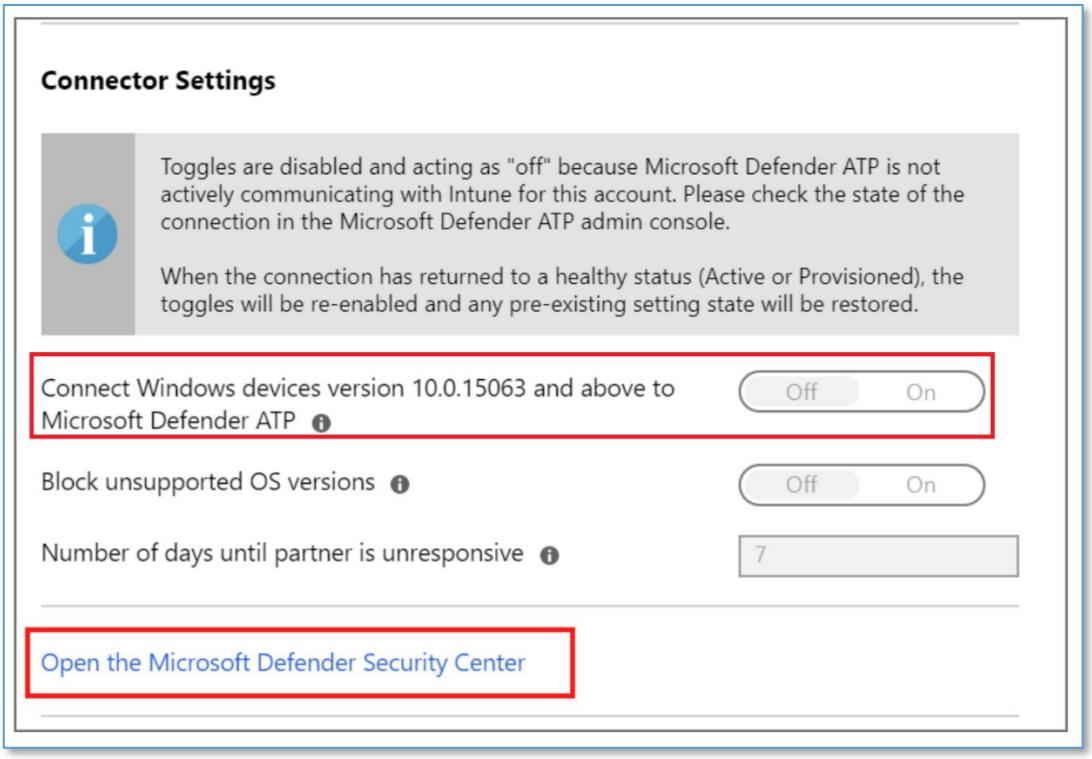
3. In Microsoft Defender Security Center, select **Settings** > **Advanced features**.

4. For Microsoft Intune connection, select **On,** then click **Save preferences**:



5. Go back to Intune, **Device compliance** > **Microsoft Defender ATP**.

6. Set Connect Windows devices version 10.0.15063 and above to Microsoft Defender ATP to **On**.



7. Select **Save**.

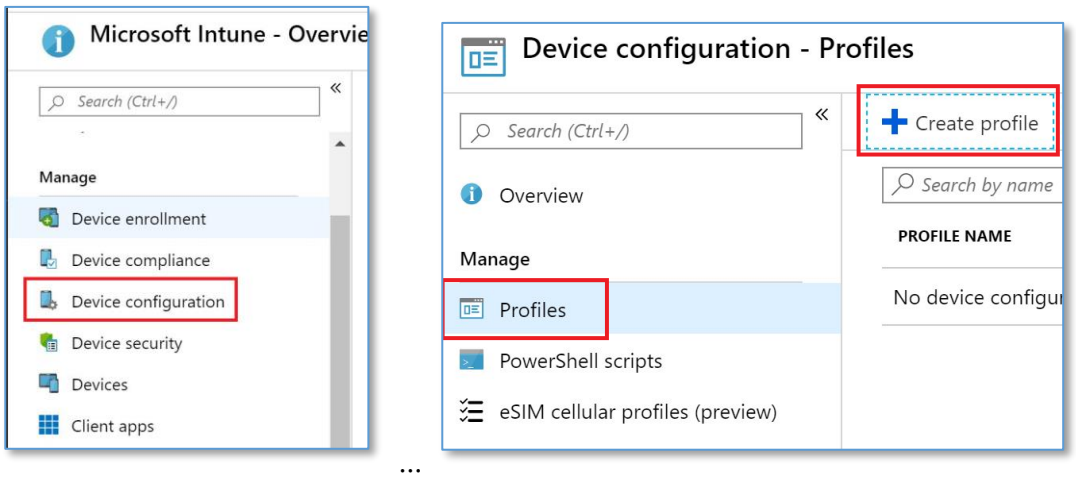
On-board devices by using a configuration profile

After you establish the service-to-service connection between Intune and Microsoft Defender ATP, you onboard your Intune managed devices to ATP so that data about their risk level can be collected. To on-board devices, you use a device configuration profile for Microsoft Defender ATP.

When you established the connection to Microsoft Defender ATP, Intune received an ATP onboarding configuration package from Microsoft Defender ATP. This package is deployed to devices with the device configuration profile. The configuration package configures devices to communicate with Microsoft Defender ATP services to scan files, detect threats, and report the risk to Microsoft Defender ATP.

Create a device configuration profile

1. Sign in to Intune and select **Device Configuration** > **Profiles** > **Create profile**:



...

2. Enter a **Name** and **Description**.

   - For **Platform**, select **Windows 10 and later**
   - For **Profile type**, select **Microsoft Defender ATP (Windows 10 Desktop)**.

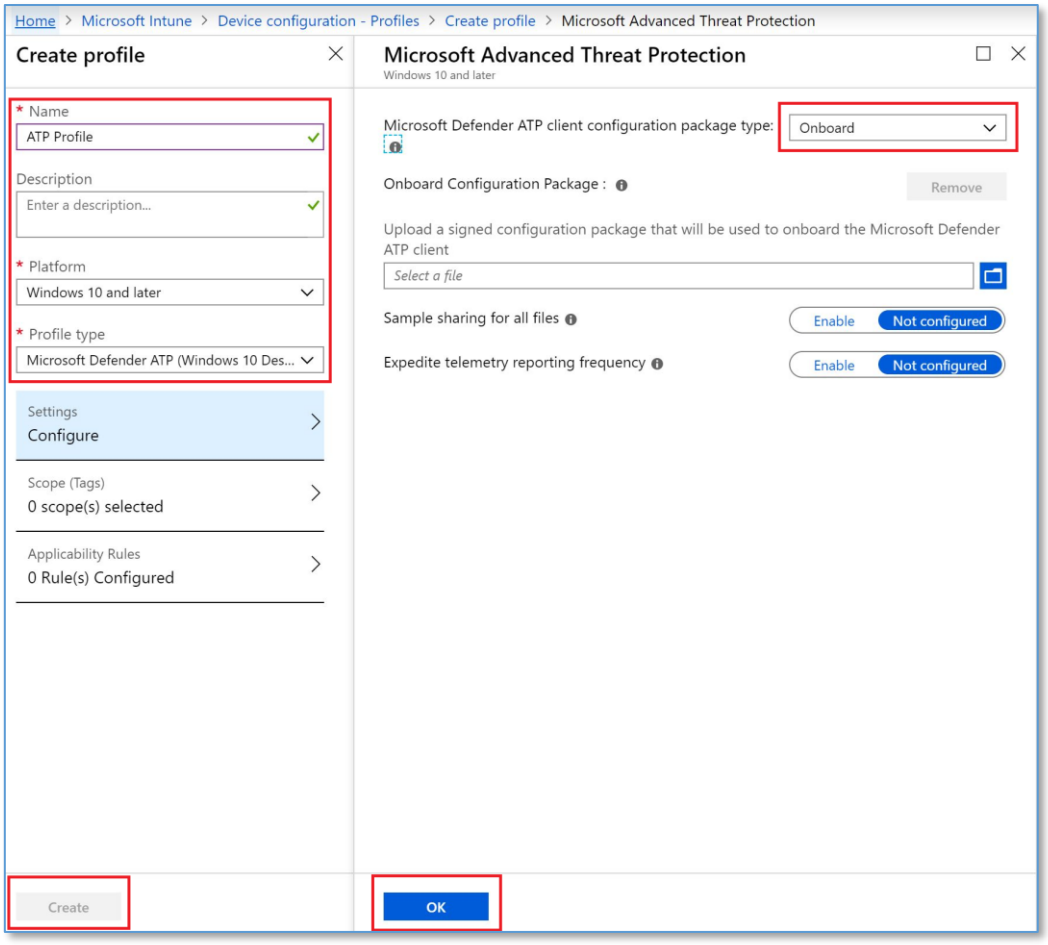
   Configure the settings:

   - **Microsoft Defender ATP client configuration package type**: Select **Onboard** to add the configuration package to the profile. Select **Offboard** to remove the configuration package from the profile.

     Note -

     If you've properly established a connection with Microsoft Defender ATP, Intune will automatically **Onboard** the configuration profile for you, and the **Microsoft Defender ATP client configuration package type** setting will not be available.

   - **Sample sharing for all files**: **Enable** allows samples to be collected, and shared with Microsoft Defender ATP. For example, if you see a suspicious file, you can submit it to Microsoft Defender ATP for deep analysis. **Not configured** doesn't share any samples to Microsoft Defender ATP.
   - **Expedite telemetry reporting frequency**: For devices that are at high risk, **Enable** this setting so it reports telemetry to the Microsoft Defender ATP service more frequently.

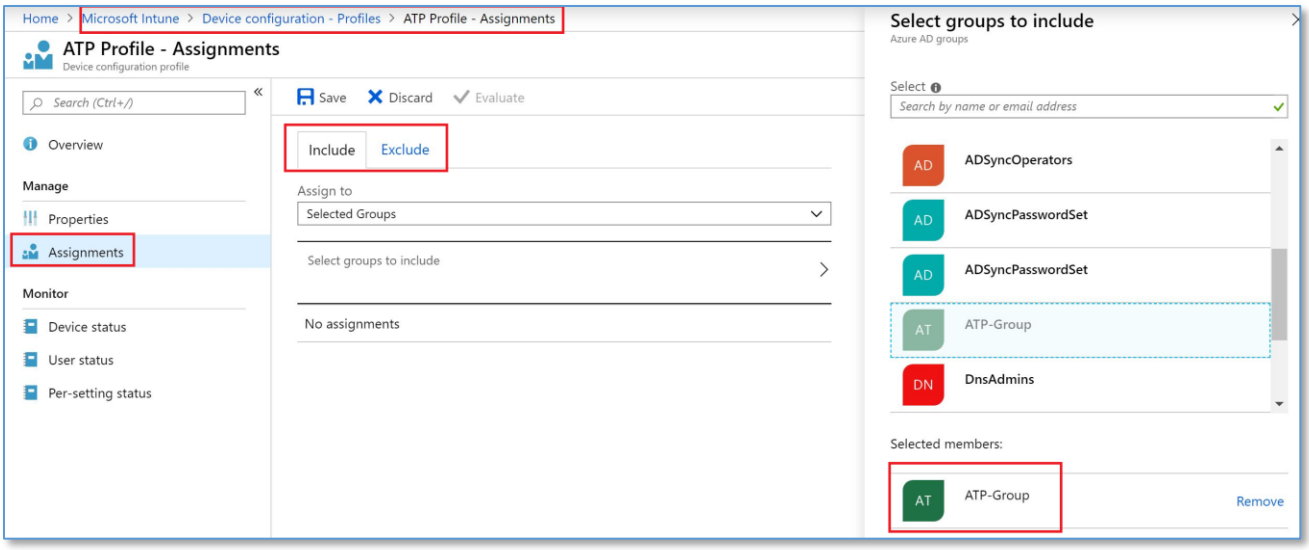


3. Select **OK**, and **Create** to save your changes, which creates the profile.

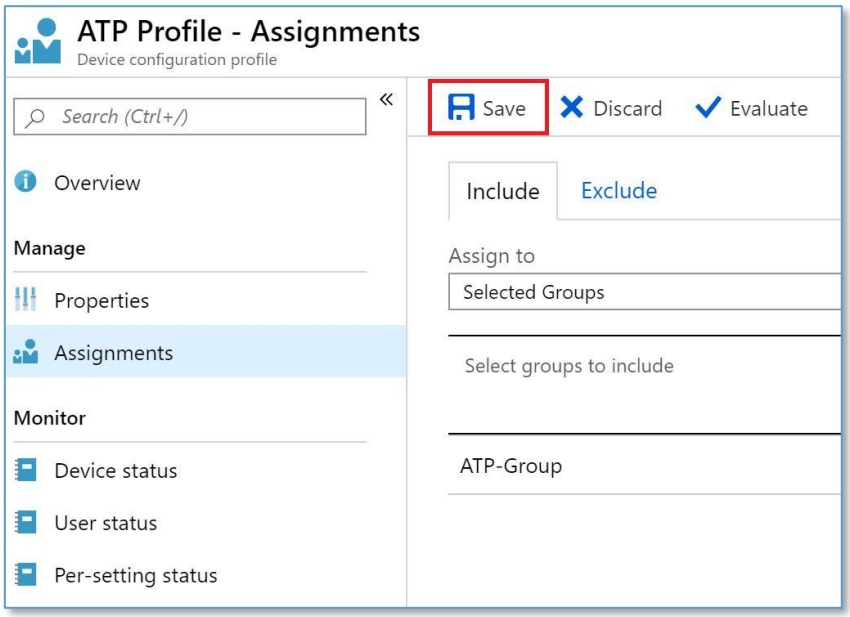
Assign a device profile

Assign the device configuration profile to devices you want to assess with Microsoft Defender ATP.

1. Sign in to Intune and select **Device configuration** > **Profiles**. All the profiles are listed.
2. Select the profile you want to assign > **Assignments**.
3. Choose to **Include** groups or **Exclude** groups, and then select your groups. When you select your groups, you're choosing an Azure AD group. To select multiple groups, hold down the **Ctrl** key, and select your groups.



4. **Save** your changes.

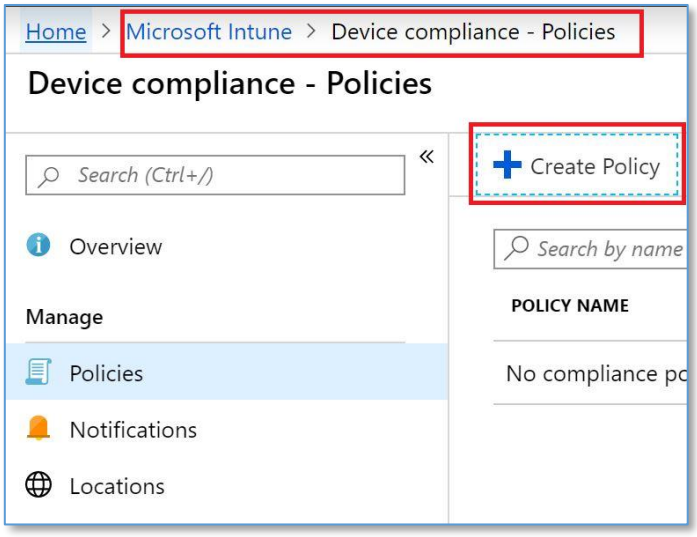


Create and assign a compliance policy

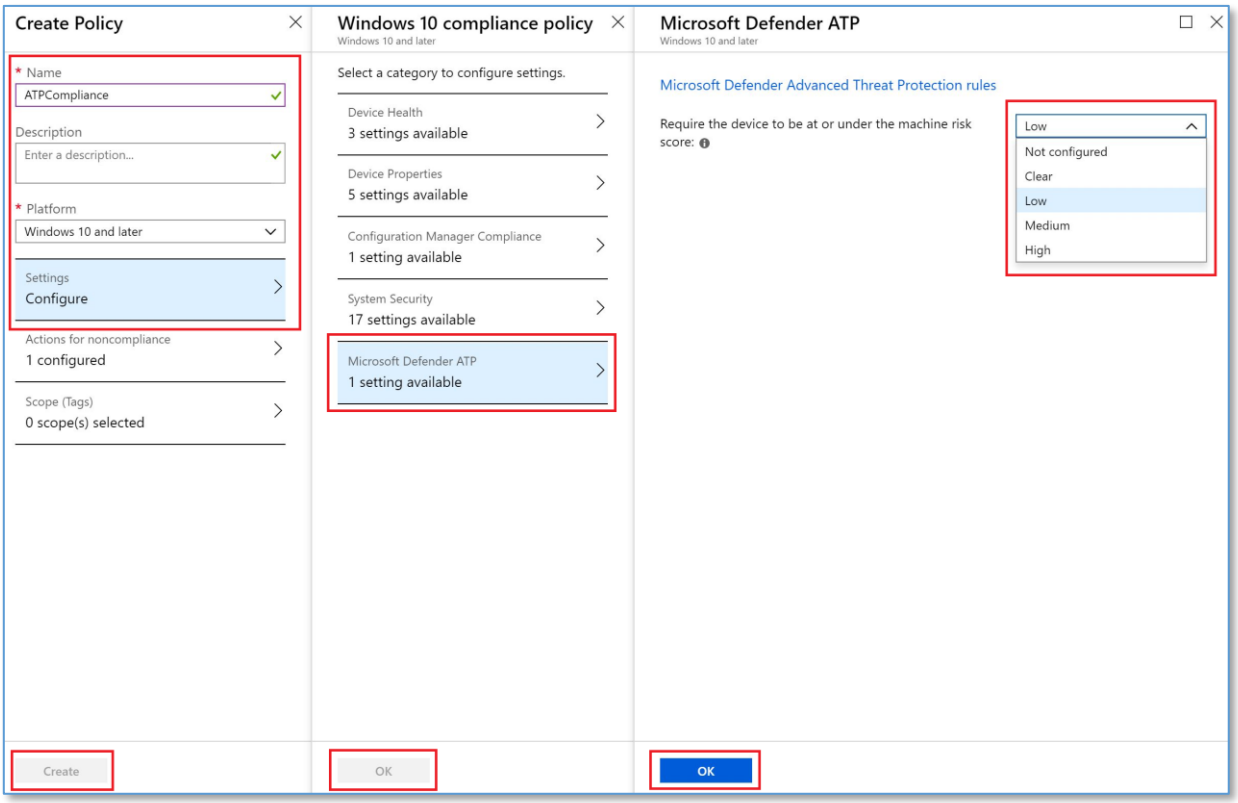
The compliance policy determines the level of risk that you consider as acceptable for a device.

Create the compliance policy

1. Sign in to Intune and select **Device compliance** > **Policies** > **Create policy**.



2. Enter a **Name** and **Description**.
3. In **Platform**, select **Windows 10 and later**.
4. In the **Microsoft Defender ATP** settings, set **Require the device to be at or under the machine risk score** to your preferred level.



Threat level classifications are determined by Microsoft Defender ATP.

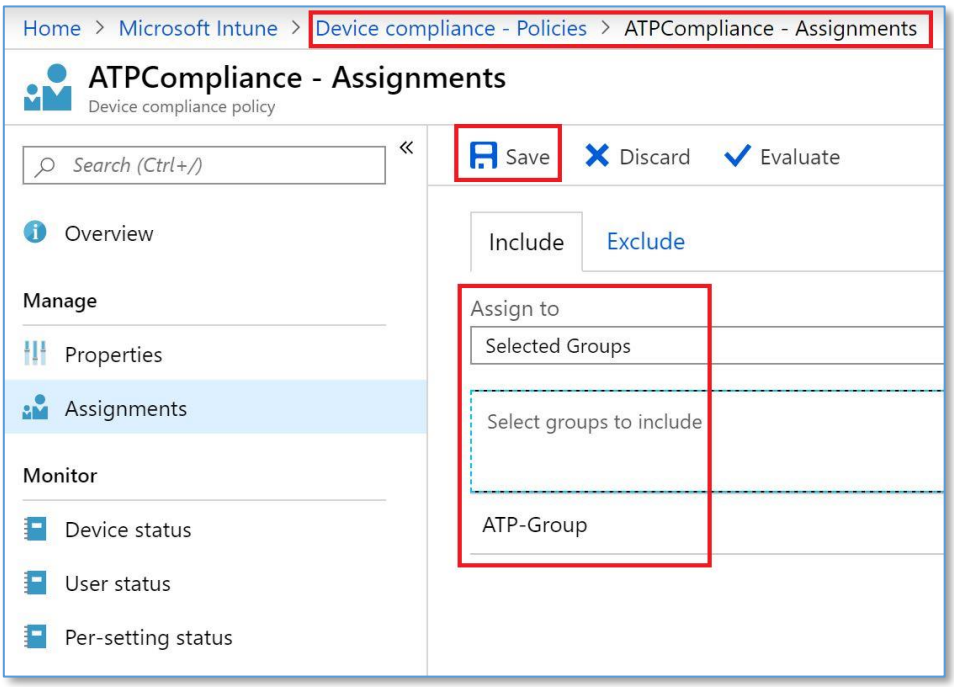
- **Clear**: This level is the most secure. The device can't have any existing threats and still access company resources. If any threats are found, the device is evaluated as noncompliant. (Microsoft Defender ATP users the value *Secure*.)
- **Low**: The device is compliant if only low-level threats exist. Devices with medium or high threat levels aren't compliant.
- **Medium**: The device is compliant if the threats found on the device are low or medium. If high-level threats are detected, the device is determined as noncompliant.
- **High**: This level is the least secure and allows all threat levels. So devices that with high, medium, or low threat levels are considered compliant.

5. Select **OK**, and **Create** to save your changes (and create the policy).

Assign the device compliance to user/groups

Once a policy is created, the next step is to assign the policy to your groups:

1. Choose a policy you created. Existing policies are in **Device compliance** > **Policies**.
2. Select the policy > **Assignments**. You can include or exclude Azure Active Directory (AD) security groups.
3. Choose **Selected groups** to see your Azure AD security groups. Select the user groups you want this policy to apply > Choose **Save** to deploy the policy to users.

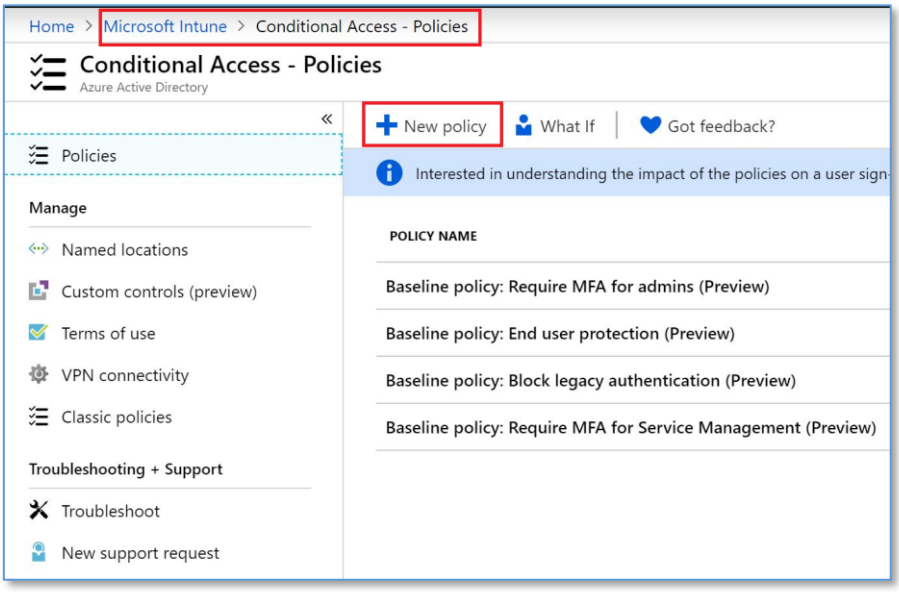


You applied the policy to users. The devices used by the users targeted by the policy are evaluated for compliance.

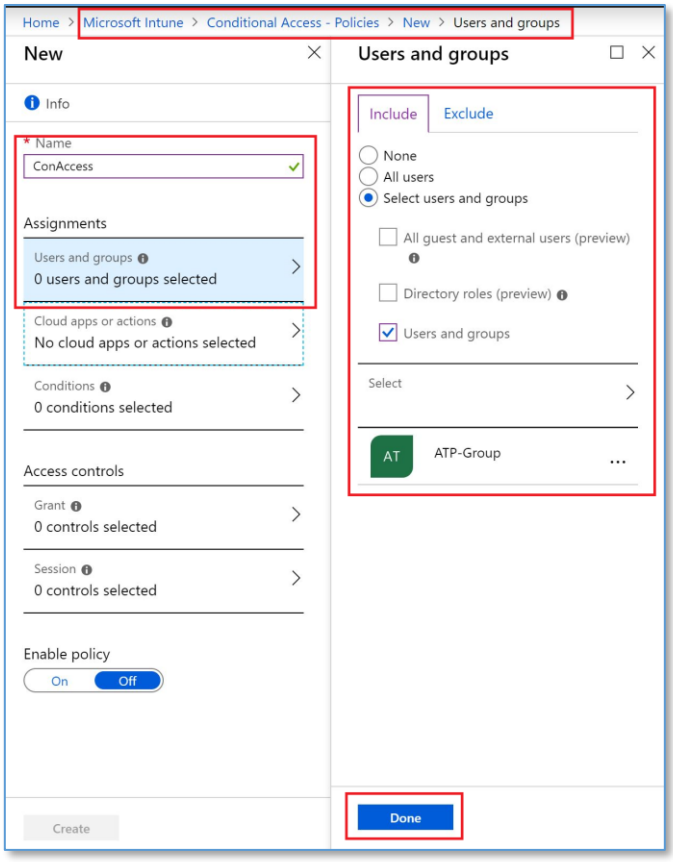
Create a Conditional Access policy

The Conditional Access policy blocks access to resources for devices that exceed the threat level you set in your compliance policy. You can block access from the device to corporate resources, such as SharePoint or Exchange Online.

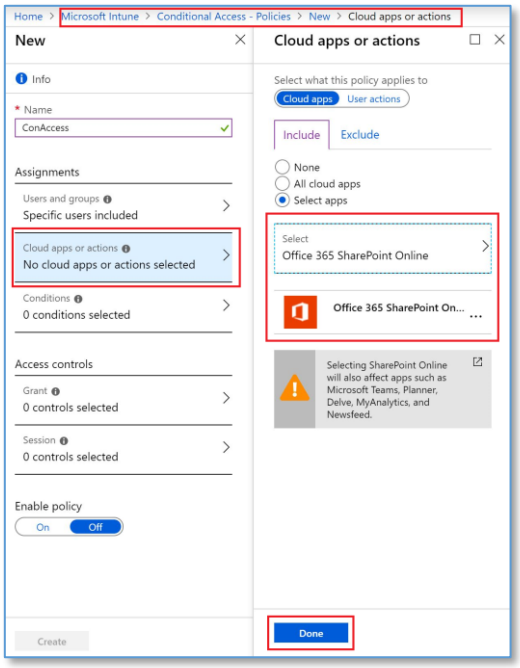
1. Sign in to Intune and select **Conditional Access** > **New policy**.



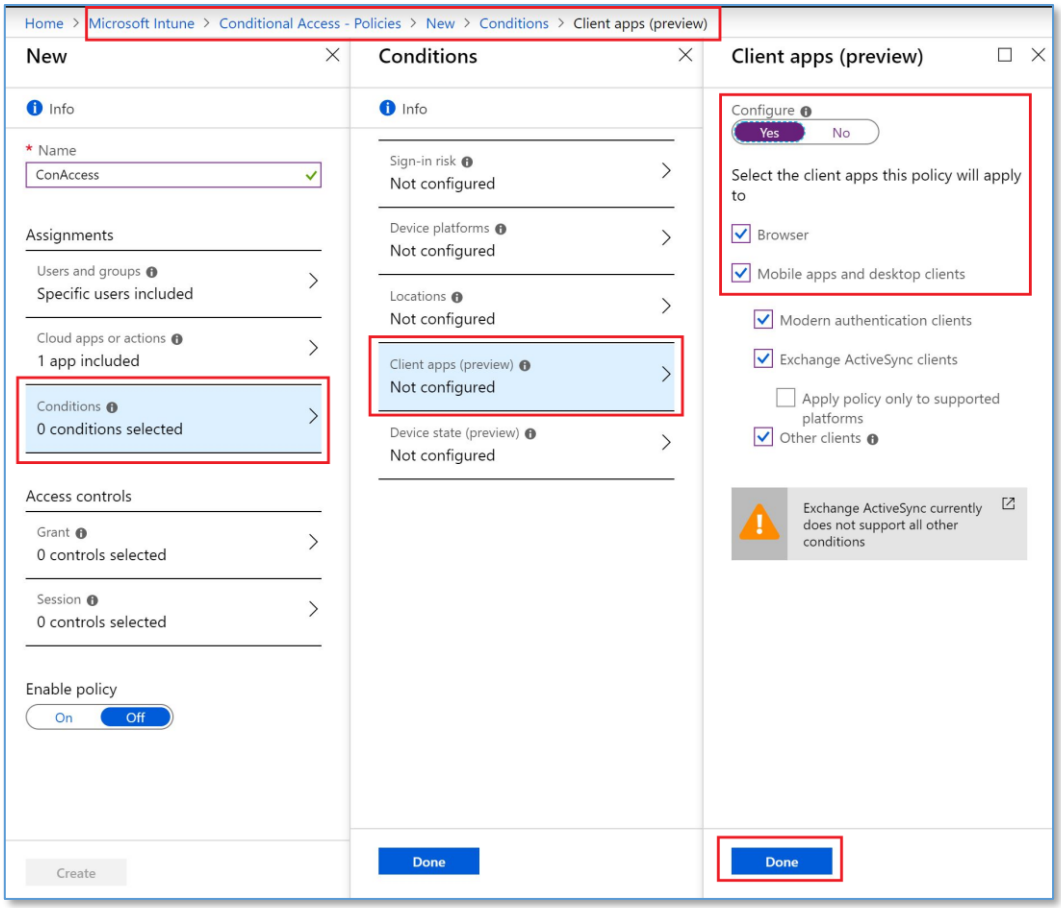
2. Enter a policy **Name**, and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy, and select **Done**:



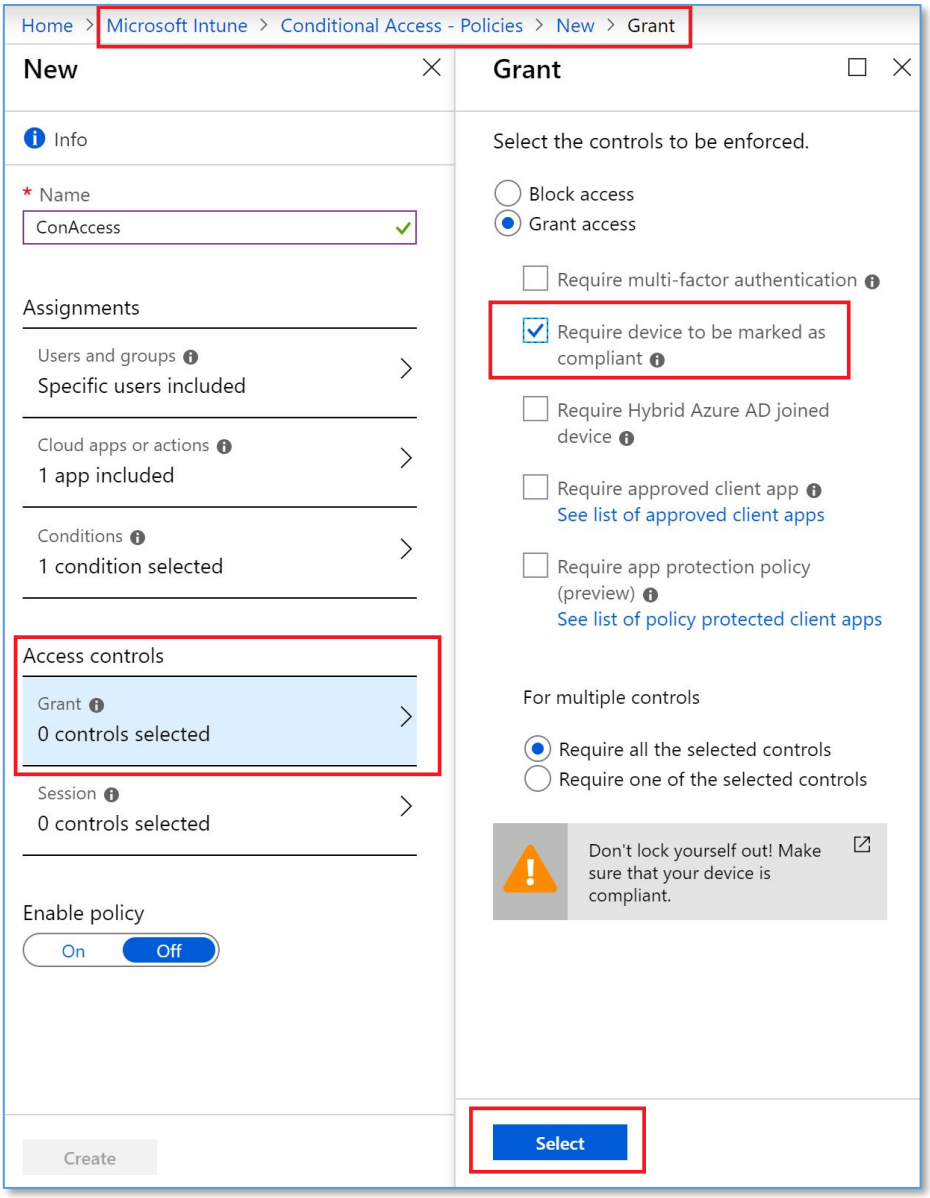
3. Select **Cloud apps**, and choose which apps to protect. In our example, we chose **Select apps**, **Office 365 SharePoint Online,** and **Office 365 Exchange Online**.



4. Select **Done** to save your changes.
5. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select Yes, and then enable Browser and Mobile apps and desktop clients:

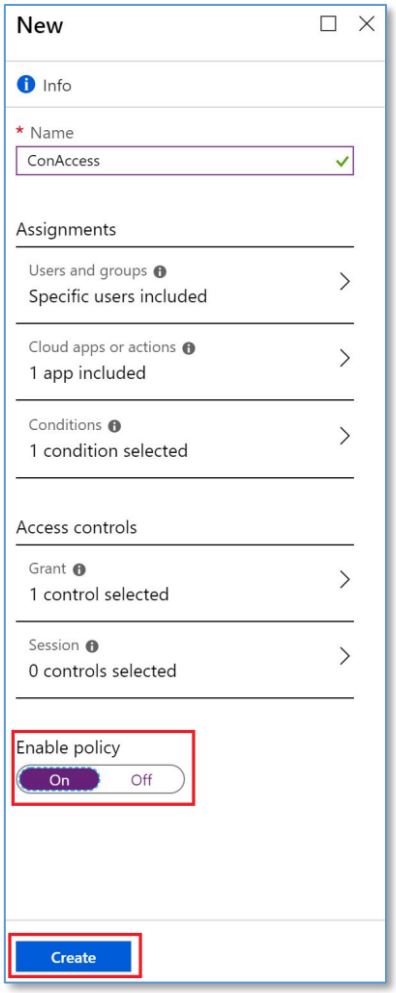


6. Select **Done** to save your changes.
7. Select **Grant** to apply Conditional Access based on device compliance. For example, select **Grant access**> **Require device to be marked as compliant**:



8. Choose **Select** to save your settings.

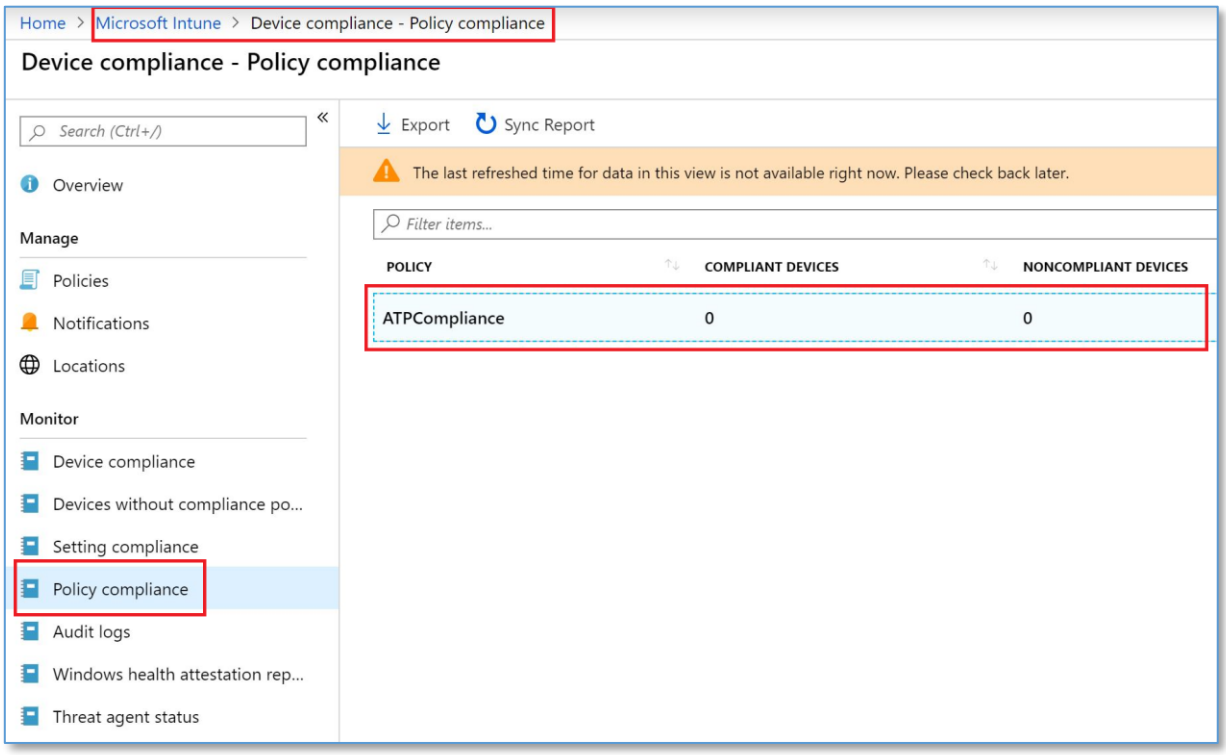
9. Select **Enable policy**, and then **Create** to save your changes.



Monitor device compliance

Next, monitor the state of devices that have the Microsoft Defender ATP compliance policy.

1. Sign in to Intune.
2. Select **Device compliance** > **Policy compliance**.
3. Find your Microsoft Defender ATP policy in the list, and see which devices are compliant or noncompliant.



10. Support

Opening tickets

In case of an issue for Windows Virtual Desktop go to the Azure Portal and open a technical ticket based on your existing support plan at https://azure.microsoft.com/en-us/support/create-ticket/

Look for Service under **COMPUTE** and select **Windows Virtual Desktop-Preview**. You will find options to create tickets for the WVD service itself and for Office:

For Office issues you can file tickets during public preview in the Azure Portal when using Office in context of Windows Virtual Desktop.

Information you should provide for failed connection or management interactions when using the service:

- Use the diagnostics service to retrieve the **Activity ID** for failed connections or management interactions.
- Provide the approximate timeframe the issue happened

NOTE: This workflow will change post general availability.

Other resources you can leverage

Windows Virtual Desktop contains a number of knowledge articles as well as trouble shooting guides. Pay attention to the updated diagnostics chapter that provides Error scenarios you can mitigate: https://docs.microsoft.com/azure/virtual-desktop/overview

Exchange on our community forum on issues important to you for Windows Virtual Desktop: https://techcommunity.microsoft.com/t5/Windows-Virtual-Desktop/bd-p/WindowsVirtualDesktop

When setting up your environment you will be using other Azure Services. You can watch the health dashboard here to verify health state on any Azure service you are consuming: https://azure.microsoft.com/en-us/status/

11. Appendix

Device security and data protection

Basic Security

Windows Defender Antivirus Uses the power of the cloud, wide-optics, precise machine learning models, and behavior analysis to protect devices.

Windows Defender SmartScreen Checks for malicious apps and sites, warning and blocking users from accessing content that could harm their devices.

Windows Defender Firewall Protects against unauthorized access.

Advanced Security

Windows Hello Replaces passwords with strong two-factor authentication, providing instant access to your Windows 10 devices using fingerprint or facial recognition. (This is PIN only on a VM)

Windows Information Protection Protects enterprise apps and data against accidental data leak on enterprise-owned devices and personal devices.

Microsoft Defender Advanced Threat Protection Helps detect, investigate, and respond to advanced attacks on your networks. (Requires Windows E5 or M365 E5)