Guide to the Intune Best Practices Checklist

Alex Fields, ITProMentor.com
Updated: 07/15/2019

This resource corresponds to the Microsoft 365 Device Management (Intune) Best Practices Checklist, and is intended to be used as a baseline for provisioning new Microsoft 365 tenants according to best practices. The checklist is setup sequentially (i.e. the recommended implementation order).

Note: I have also provided scripts and JSON files via GitHub which will make importing the described policy set much quicker and easier (so they do not have to be re-created using the GUI as described here in this guide). Conditional access policies cannot (at the time of this writing) be imported from JSON.

Table of Contents

☐ Create security groups for Intune deployment rings

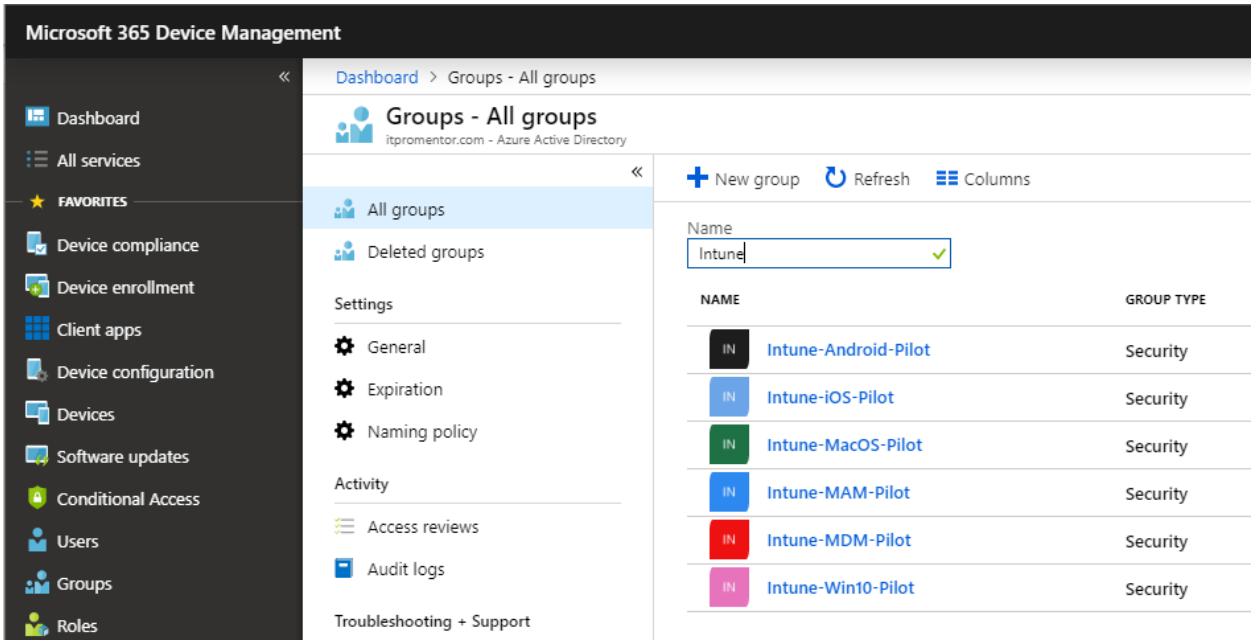
Before you get started, setup your pilot group, and any additional rings you want to have. Example of a common / typical small business deployment:

Group Name	User base included in group	Excluded from group
Pilot Group	Champions, power users	N/A
Broad Group (or All users)	Most of the user population	Pilot and Sensitive groups
Sensitive Group	Critical users, get new features last	N/A

Whenever you create a policy or configuration profile that you want to test, you can target the appropriate rings starting with the pilot group. Your needs may be different than this, for instance some small orgs only do a pilot and then straight to production (All users). But consider an additional group for "sensitive" users who should get policy changes and software updates last, after everyone else.

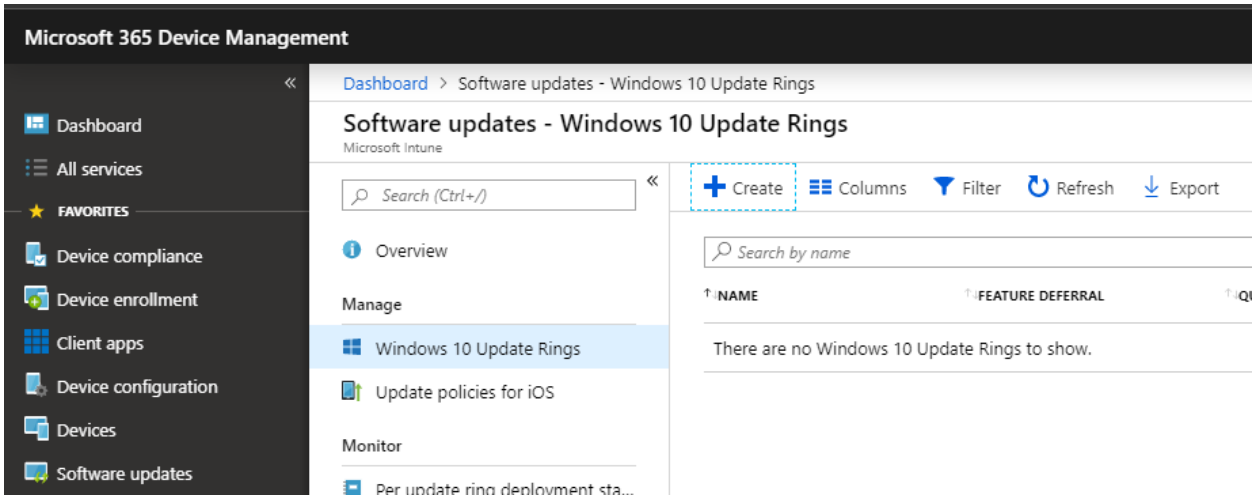
You may also create different pilot groups for different platforms or purposes (e.g. Intune-MacOS-Pilot or Intune-Android-Pilot to test settings changes first on these device types).

Go to **Groups > New group** to create security groups appropriate to your situation.



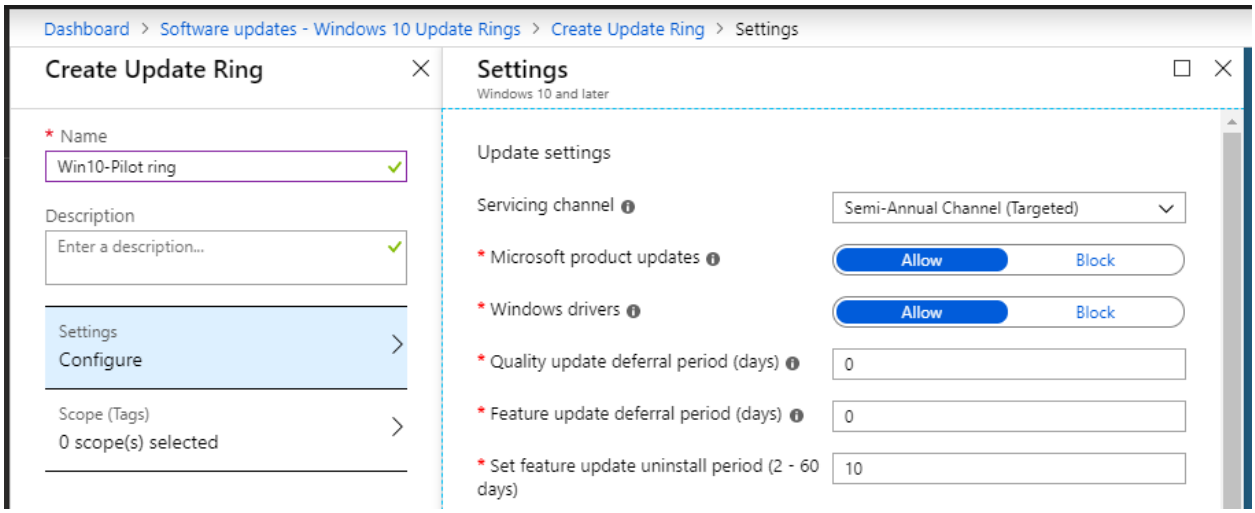
☐ Setup Windows 10 Software Update Rings

Navigate to **Software updates > Windows 10 Update Rings** and click **Create**.



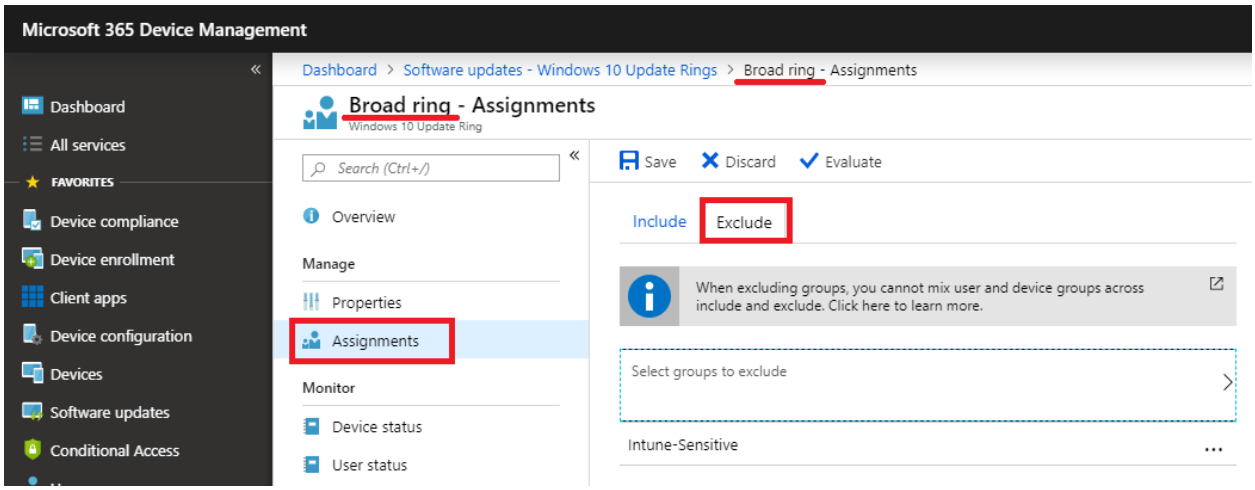
I recommend creating at least two update rings. Three if you have sensitive groups within the organization. Here is an example of the most typical deployment rings for a small business:

Adoption ring	Servicing channel	Defer feature updates	Defer quality updates
Pilot group	Semi-Annual (Targeted)	N/A	N/A
Broad group	Semi-Annual	60-120 days	7-14 days
Sensitive group	Semi-Annual	180 days	30 days



After you have constructed the rings, make your assignments. Click into any of the defined rings and choose **Assignments** from the left menu. Example of recommended assignments:

Adoption ring	Include groups	Exclude groups
Pilot group	Intune-Pilot	None
Broad group	All users	Intune-Pilot, Intune-Sensitive
Sensitive group	Intune-Sensitive	None

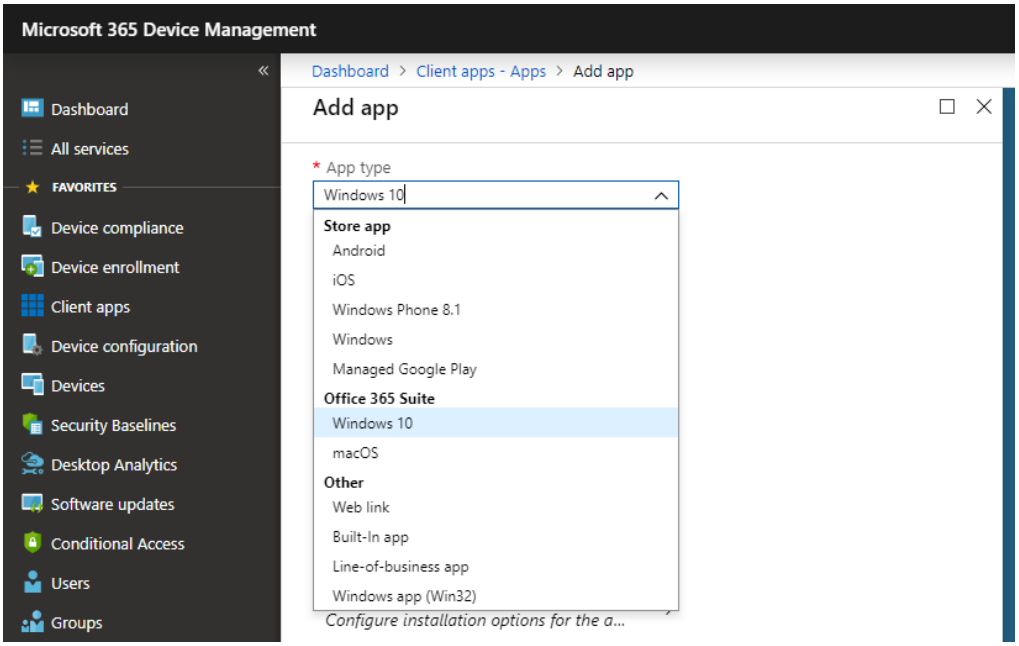


This way, any potential issues with updates can be discovered and hopefully remediated via earlier adoption rings, and before critical or sensitive users get them. The pilot group is always your canary in the coal mine but having the broad group in front of the sensitive users is still a recommended best practice, and will help you surface other / delayed issues.

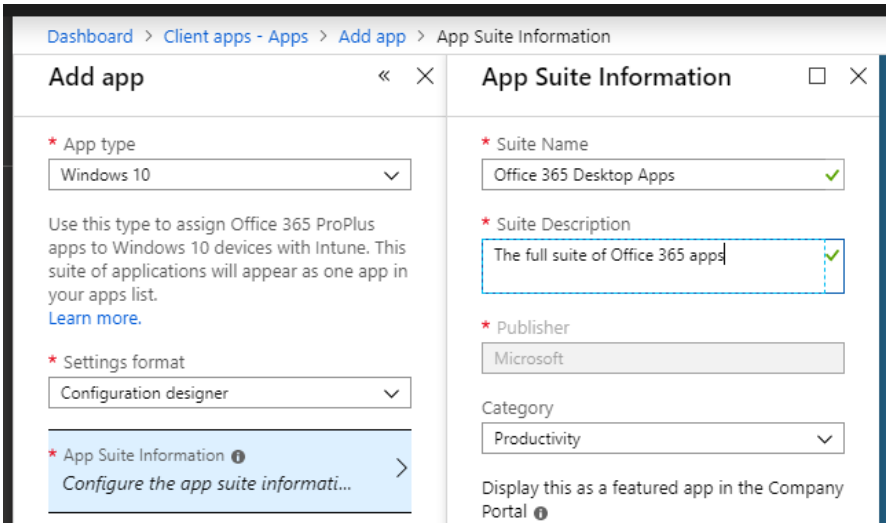
☐ Setup Office 365 app deployments for Windows 10

It is possible to push software packages to managed devices via Intune. Setup a policy that will automatically install the Office 365 desktop applications to newly enrolled devices.

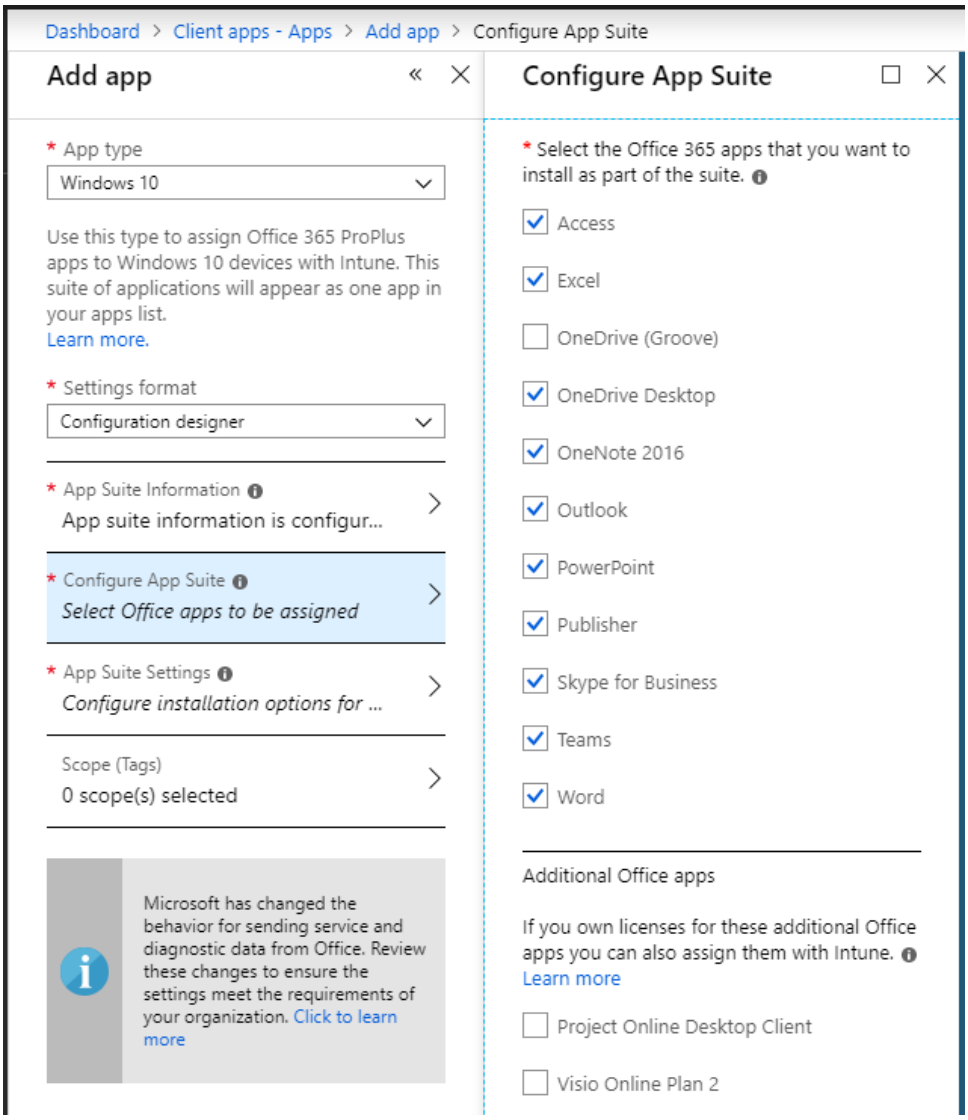
Go to **Client apps > Apps**. Click **+ Add.** Under App type, choose **Office 365 Suite > Windows 10**.



Leave the selection on **Configuration designer**. On the first blade, **App suite information**, give it a name and description similar to the below:



In the next blade, **Configure App Suite**, choose the applications you wish to include in the deployment. Notice that the good/useable version of OneNote (2016) is not included by default—so select that if you require it.



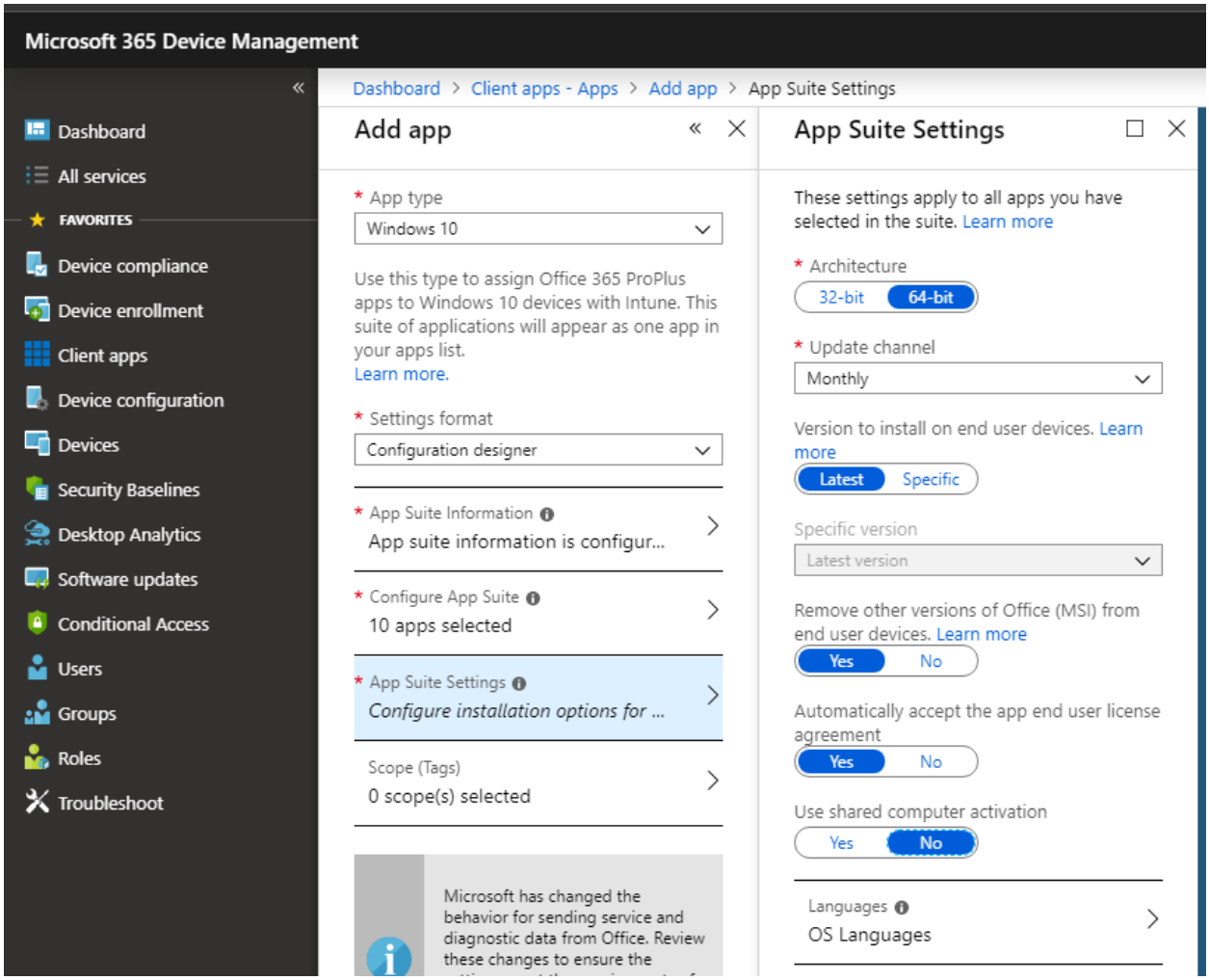
The **App Suite Settings** blade is where you will configure the frequency of updates, and some other options. Note that you can create more than one deployment, and target different adoption rings, which we defined earlier.

Remember that "targeted" releases always come ahead of non-targeted. You may wish to keep your broad ring on a more conservative release cycle (non-targeted). Example of recommended update rings:

Org's change tolerance	Pilot ring	Broad ring
Higher (creative, tech-savvy)	Monthly (Targeted)	Monthly
Mixed (both types present)	Monthly	Semi-Annual Channel
Lower (sensitive, critical)	Semi-Annual Channel (Targeted)	Semi-Annual Channel

Recommended settings for a typical deployment:

- **Architecture**: 64-bit
- **Update channel**: select according to change tolerance
- **Version to install**: Latest (in the selected channel)
- **Remove other versions of Office (MSI) from end user devices**: Yes
- **Automatically accept the app end user license agreement**: Yes
- **Use Shared Computer Activation**: Select **Yes** if multiple users login to the same machine
- **Languages**: Follows OS language by default, add other languages if needed

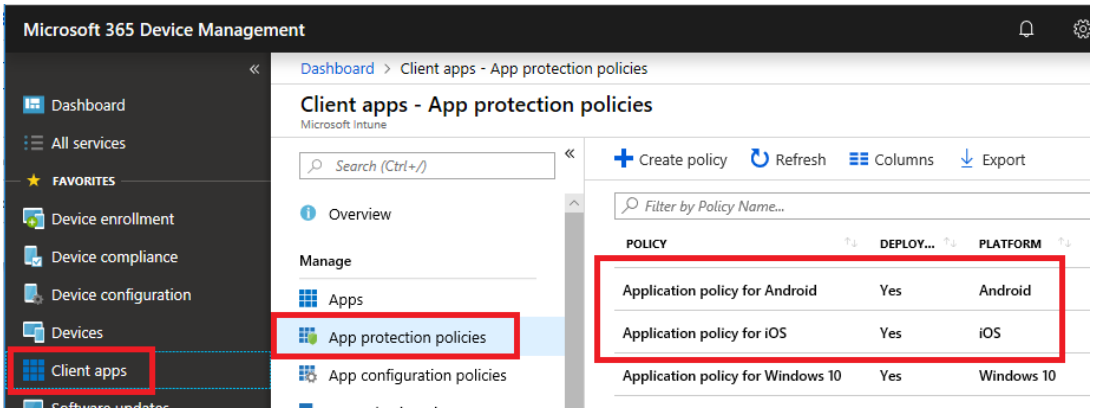


When you are done creating this deployment, go to **Assignments** and click **Add group**. Your assignment type should be **Required**. Then pick your Included and Excluded groups as needed. Example:

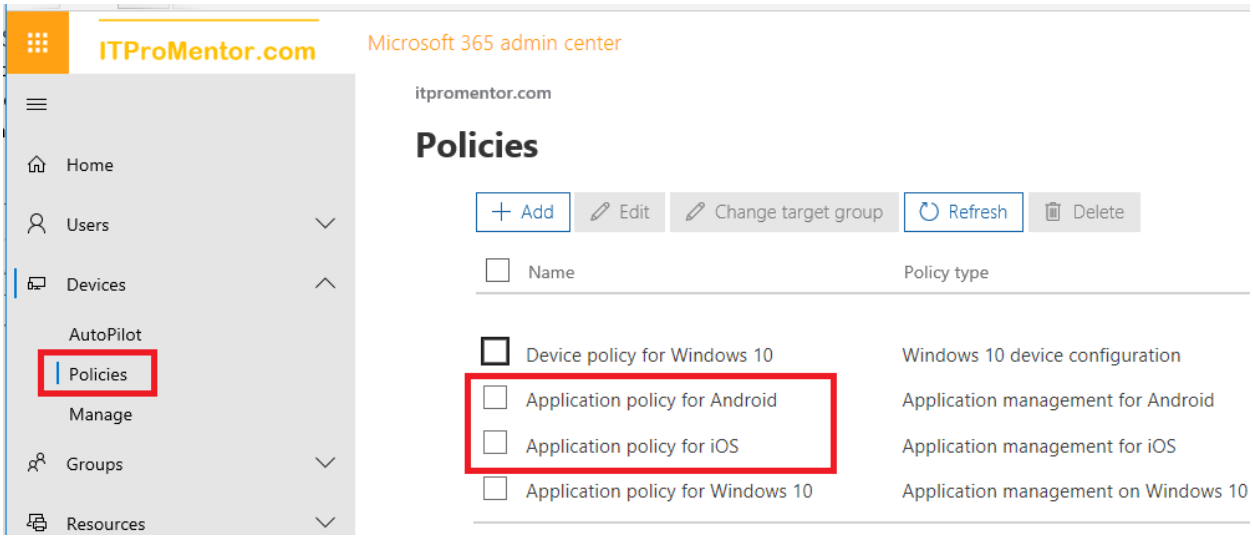
Adoption ring	Include groups	Exclude groups
Pilot group	Intune-Pilot	None
Broad group	All users	Intune-Pilot, Intune-Sensitive
Sensitive group	Intune-Sensitive	None

☐ Setup App protection policies (MAM)

Microsoft recommends using MAM policies for iOS and Android to protect managed applications, with or without MDM in place. MAM is a good way of enabling BYOD scenarios, without actually managing the devices themselves. Find MAM policies in the Device management portal, under **Client apps > App protection policies**.

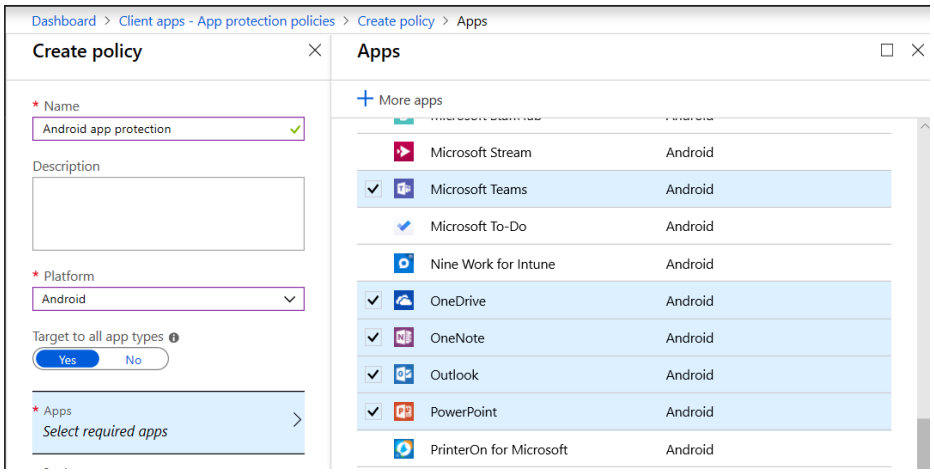


You can also configure these via the Microsoft 365 Admin center from **Devices > Policies**.



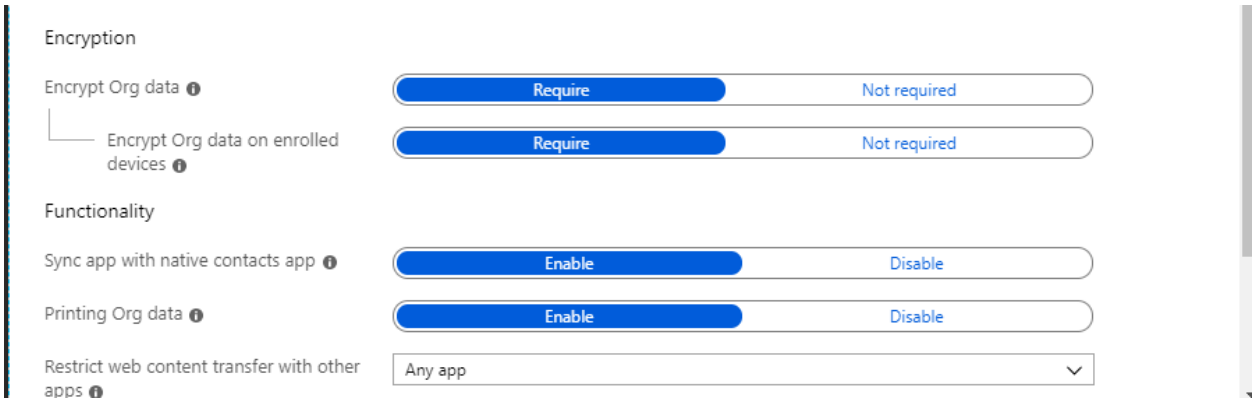
It is much quicker and easier to setup policies using the Microsoft 365 admin center, however you can go into more granular detail and see additional selections from the Device Management / Intune portal. I will describe the latter (Intune) as it allows us the most flexibility in policy design.

From **Client apps > App protection policies** choose **Create policy** if one does not yet exist. Give it a descriptive name such as **Android app protection**, selecting **Android** as the **Platform**, and then choose the **Apps** to which you want the protections to apply (e.g. Outlook, OneDrive, OneNote, Teams, etc.).

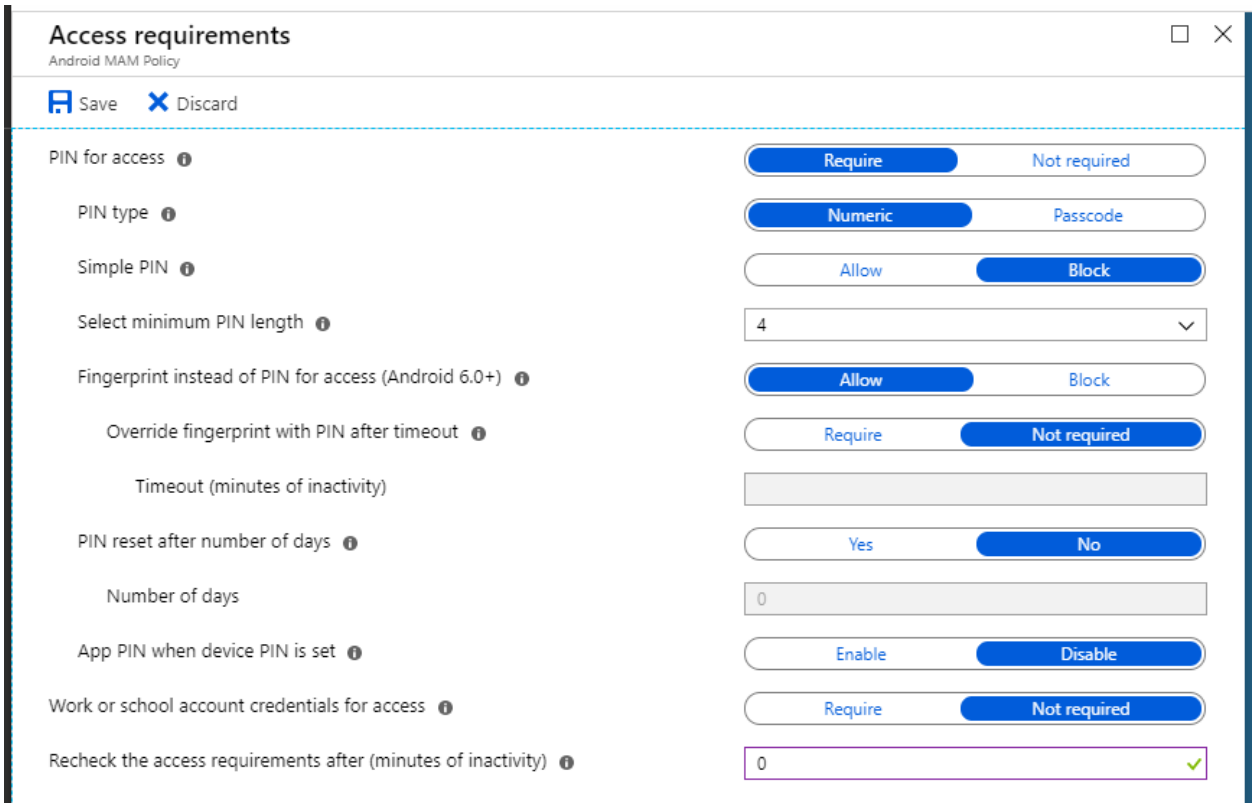


After selecting apps, choose **Settings** and then **Data protection**; make selections similar to the following for a good baseline, or manipulate as needed. **Data Transfer** settings:

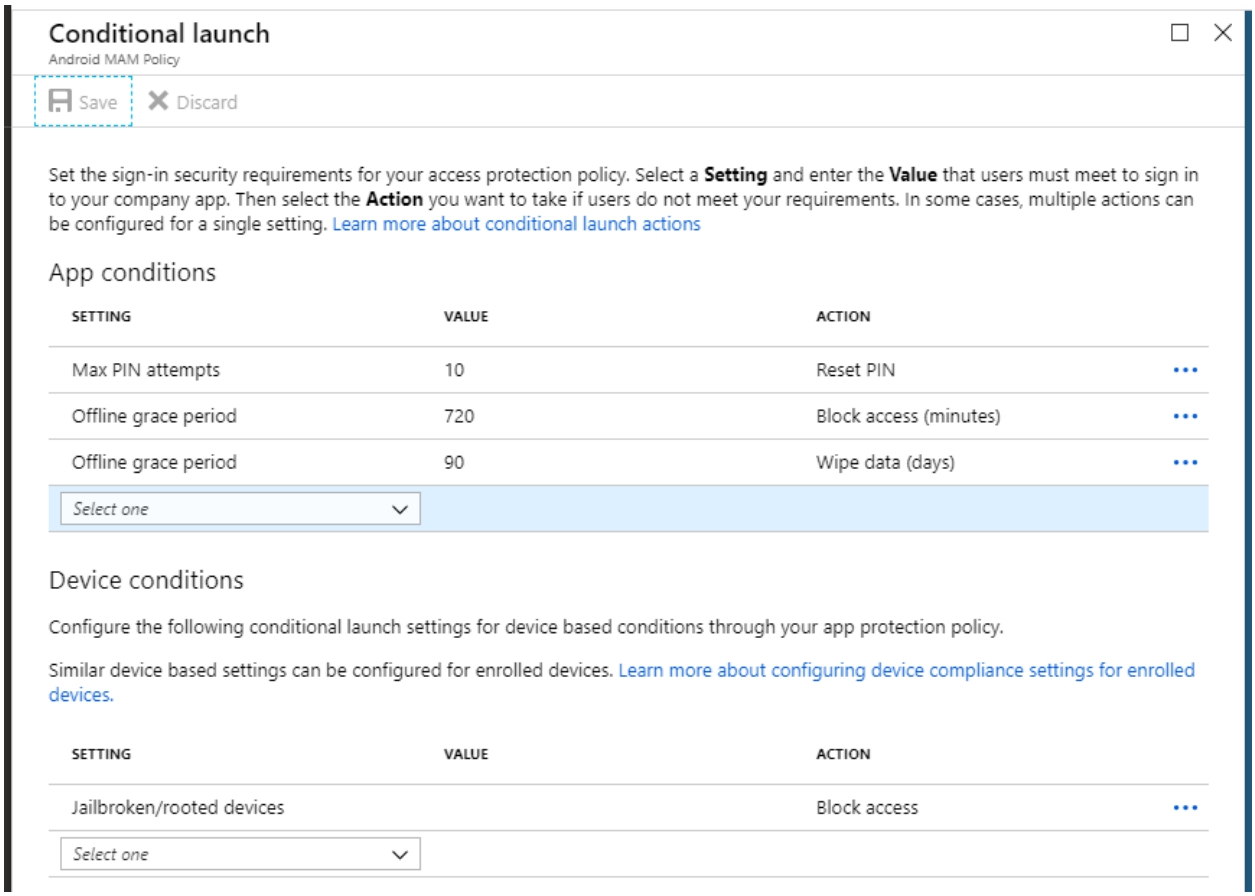
Data protection > Encryption and **Functionality** settings:



Next, configure Access requirements, similar to the following (recommended minimum):



Last, configure the **Conditional launch settings**:

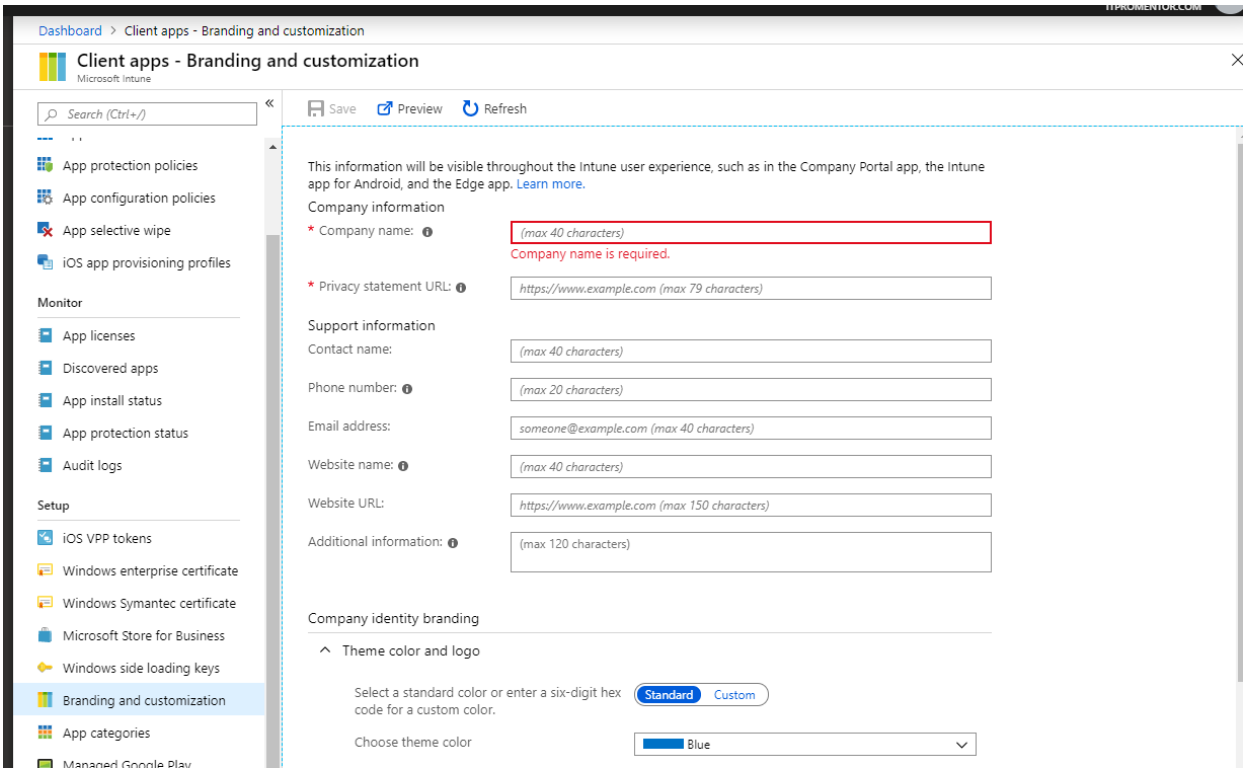


You can repeat this process, choosing nearly identical settings for iOS.

☐ Customize the Company Portal

As I have mentioned in other places, Microsoft has apparently not yet figured out how to make one central place for branding that applies to all areas in Microsoft 365. So if you have previously setup branding on your Azure AD sign-in page—that's not enough. You have to do it again for the Intune Company Portal app/website (and again for several other services in 365 besides). Hopefully Microsoft will unify the branding experience someday.

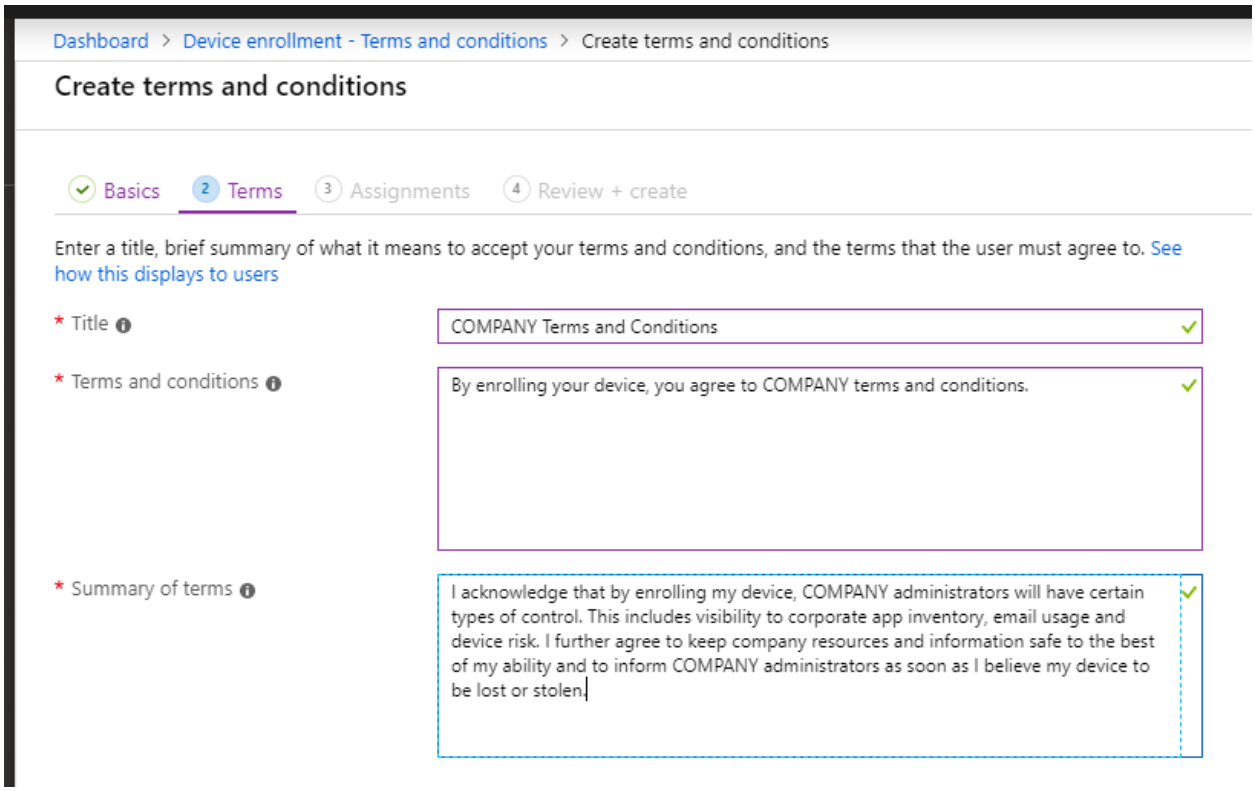
Until then, find these options under **Client apps > Branding and Customization**.



If you choose to complete this step, you will want at least your company name and a privacy statement that you can point users toward. Also, it is a good idea to include contact information for support. Down below you can upload a logo and customize the color schemes.

☐ Create the Company terms and conditions

When users enroll devices using the Company portal app, they will be prompted with the Company terms and conditions that you specify. Navigate to: **Device enrollment > Terms and conditions**.



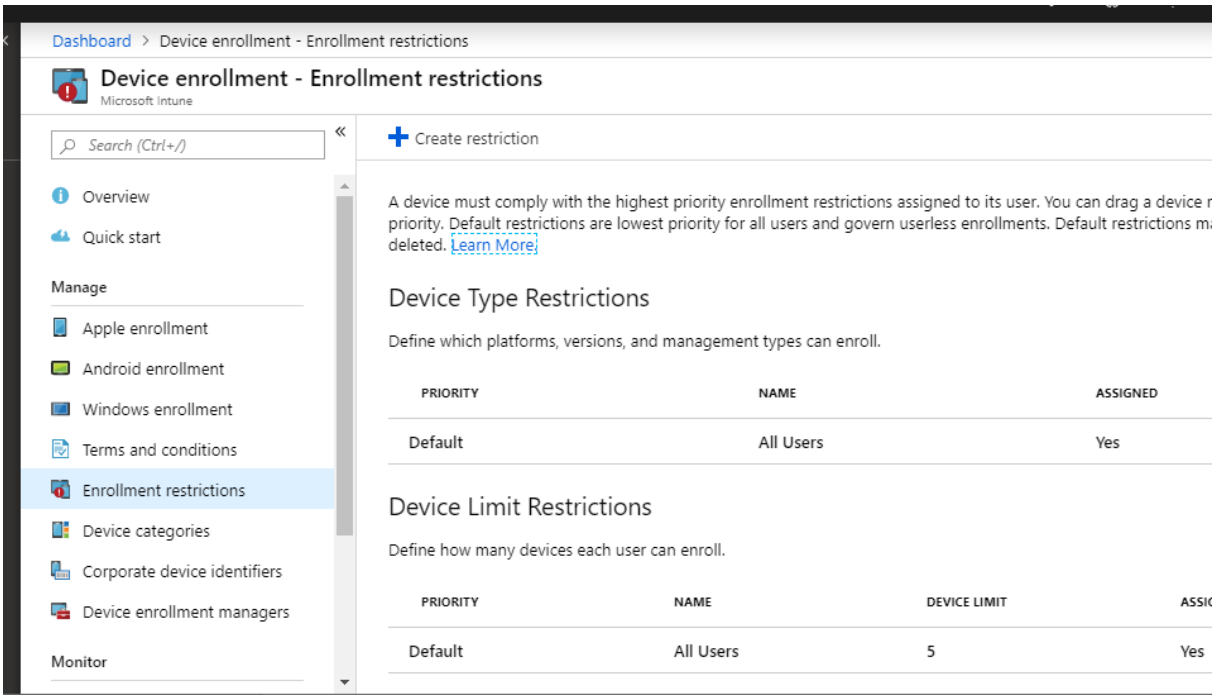
Sample text for the terms:

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

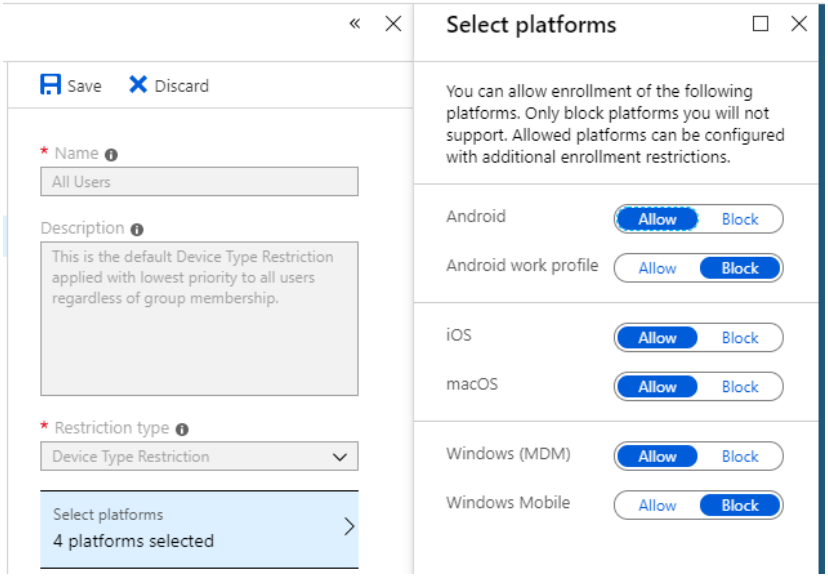
The above is taken from Microsoft's example, but you can make the terms your own.

☐ Configure Device enrollment restrictions

Navigate to **Device enrollment > Enrollment restrictions**.



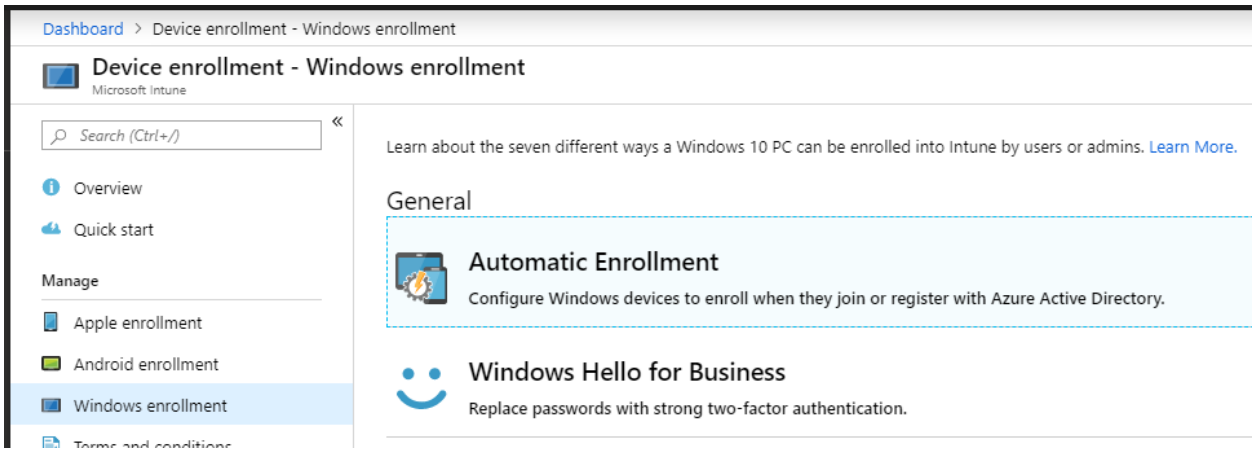
You will want to edit the default or create a new **Device Type Restriction**. Block any platforms that you do not intend to support. Example depicted below:



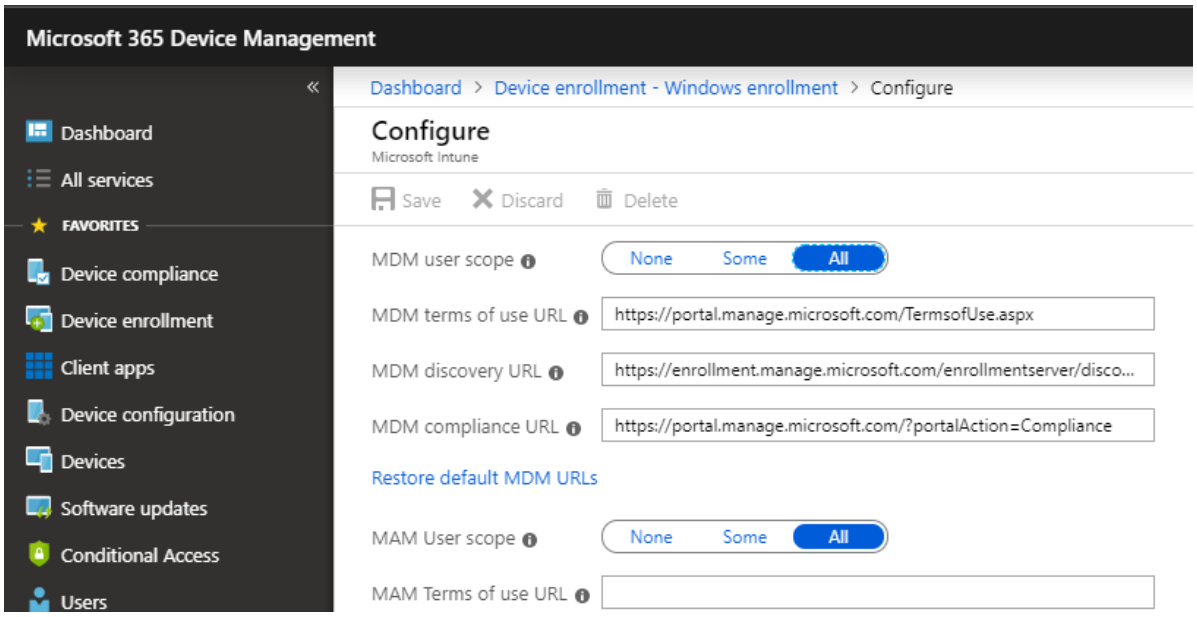
As for **Device Limit Restrictions**, I prefer setting this value to fewer than 5 devices per individual. When a user retires a device, it should be deleted from Intune so that they can enroll a different one.

☐ Configure Windows 10 automatic enrollment

Windows 10 devices have the ability to join Azure AD. When Azure AD join is performed, they can also be automatically enrolled into Intune for management.



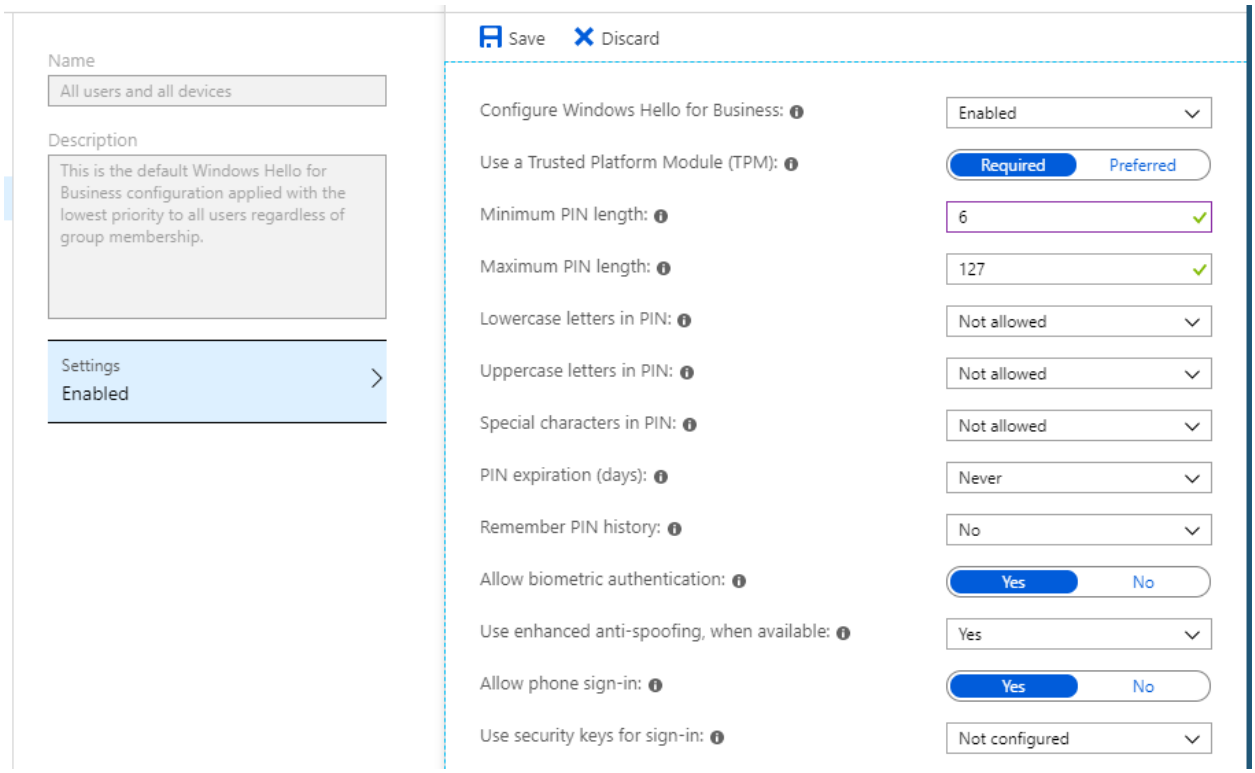
Navigate to **Device enrollment > Windows enrollment** and choose **Automatic enrollment**. Select **All** for both **MDM user scope**, and **MAM user scope**.



☐ Configure Windows Hello for Business

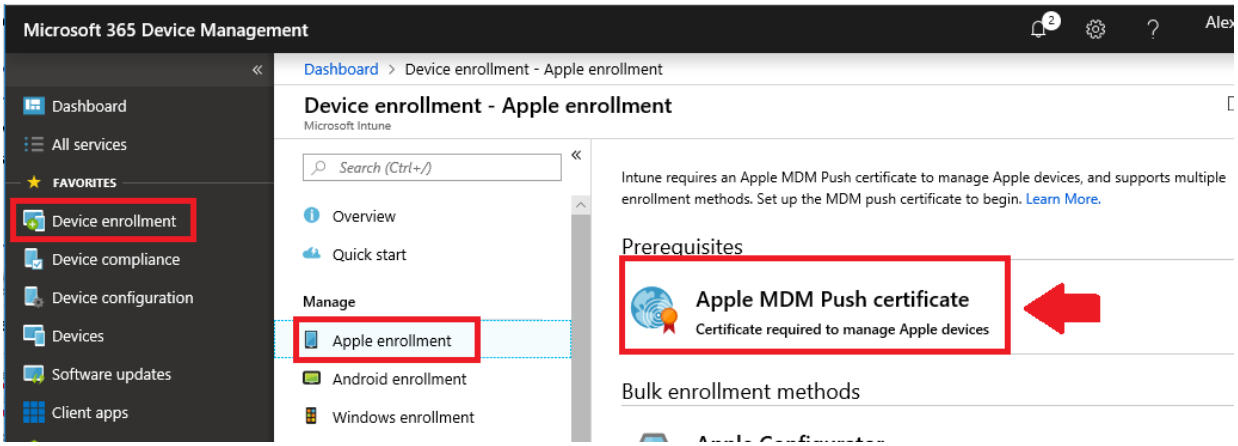
Windows Hello is a form of 2-factor authentication for signing into the local device, which is intended to replace traditional passwords. When enabled, users must choose a PIN for their device. Additionally, some devices offer the option to configure a biometric alternative such as a fingerprint or facial recognition (but PIN is still required also).

To require Windows Hello for enrolled devices, navigate to **Device enrollment > Windows enrollment > Windows Hello**. This example depicts a 6-digit PIN with no expiry:

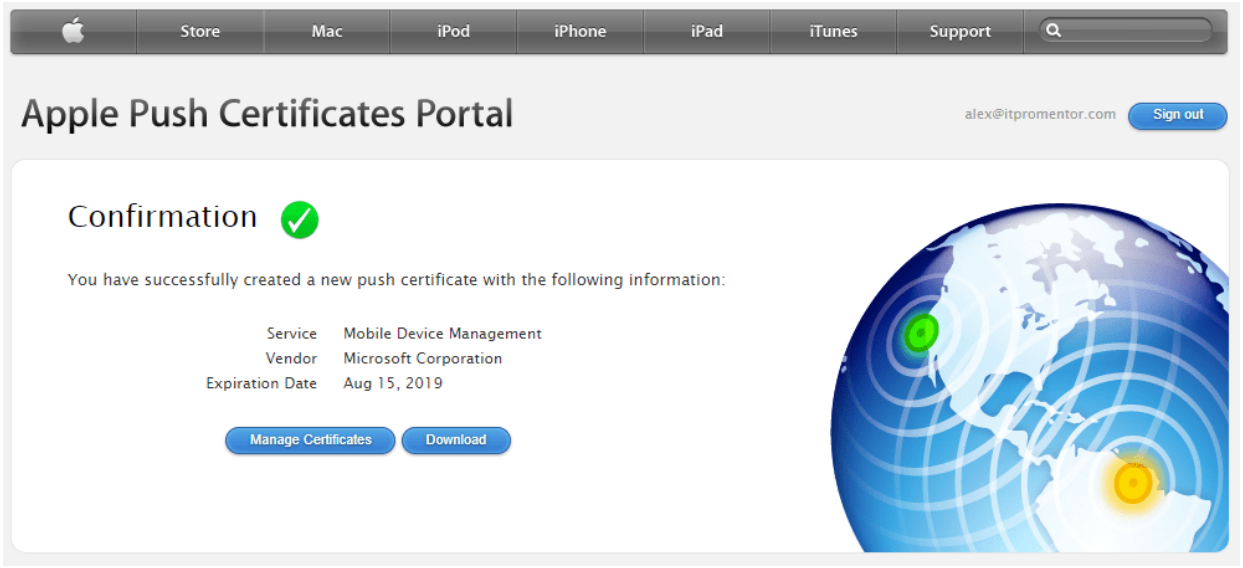


☐ Configure Apple MDM push certificate

Navigate to **Device enrollment > Apple enrollment > Apple MDM Push certificate**.



Simply follow the process laid out on this page—basically you just need to download the Certificate Signing Request from Microsoft, then hop over to the Apple portal, logging in with an Apple ID that is registered to an admin account at your organization. If you need to register a corporate email account with Apple and create a new ID, see [this article from Apple](#).

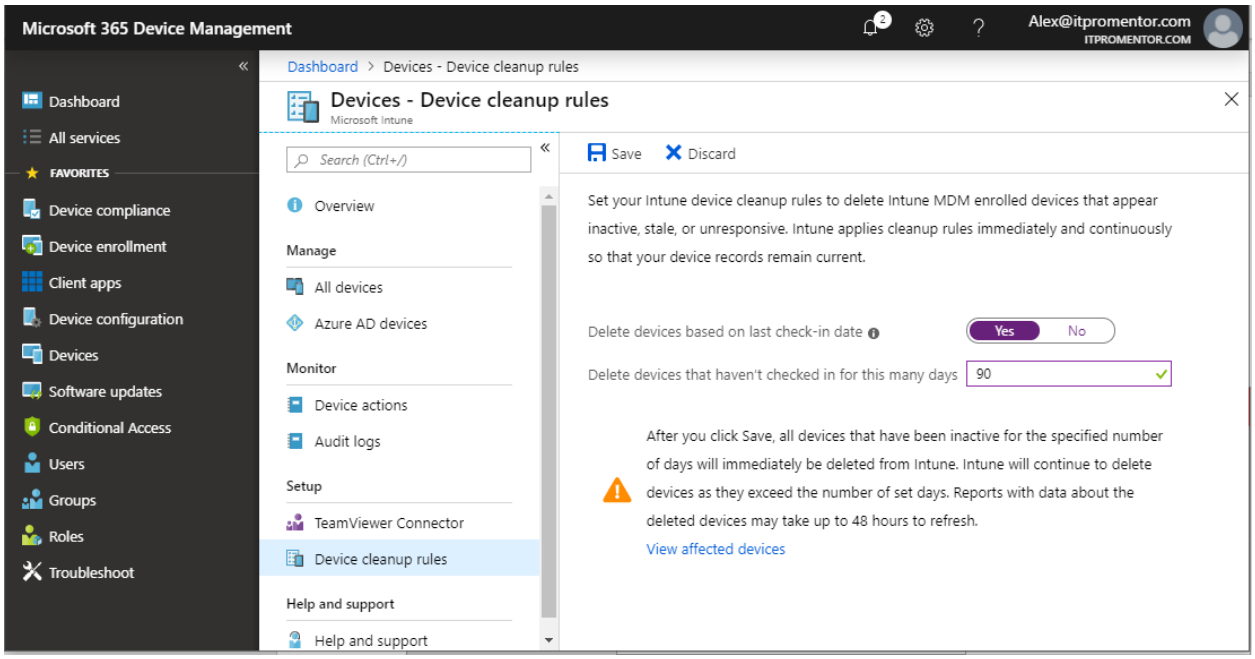


Upload the CSR to Apple, and then download the certificate that Apple provides you with. You will return to the Microsoft 365 Device management portal and upload the certificate, and you're done. Well, until next year when you need to renew it. Set yourself a reminder for this!

☐ Configure Device cleanup

Devices that have not checked in for 90 days or more are probably no longer valid devices. While you should have a retirement process in place, in case there are any devices missed, this rule will help you to clear out stale objects automatically (from Intune, but not Azure AD).

Go to **Devices > Device cleanup rules**. Make the following recommended selections:



- Delete devices based on last check-in date: **Yes**
- Delete devices that haven't checked in for this many days: **90**

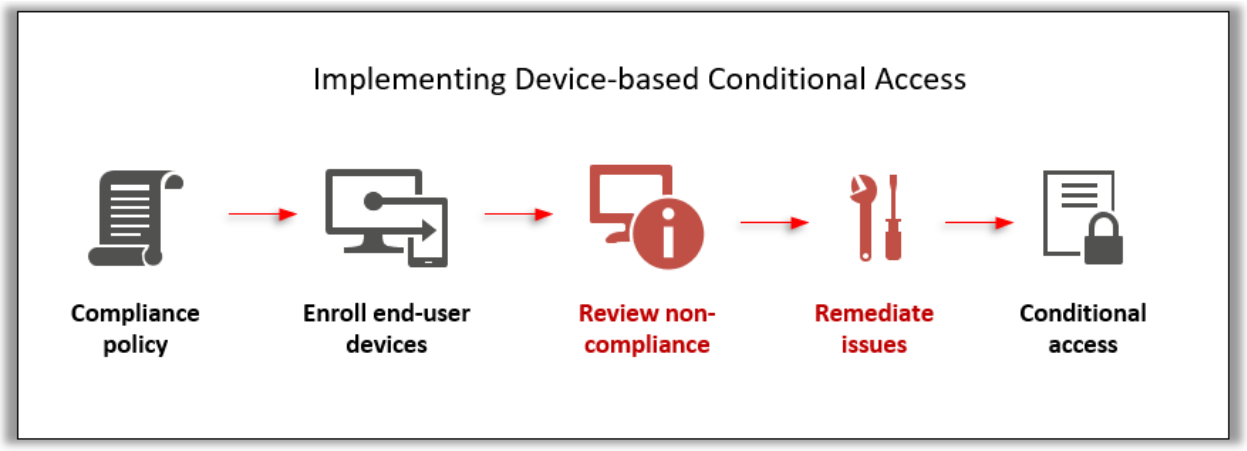
The impact of this setting is that devices which are deleted, if they still exist, would need to be re-enrolled if they were required to be re-initiated into the system.

Note: I haven't found this setting to be very consistent across tenants—sometimes I find devices that are past due. But I assume this bug will be worked out in time. Also see this article for advice on how to clean up stale devices in Azure AD. This would include devices enrolled into Intune, and others that are merely "registered" against Azure AD (unmanaged).

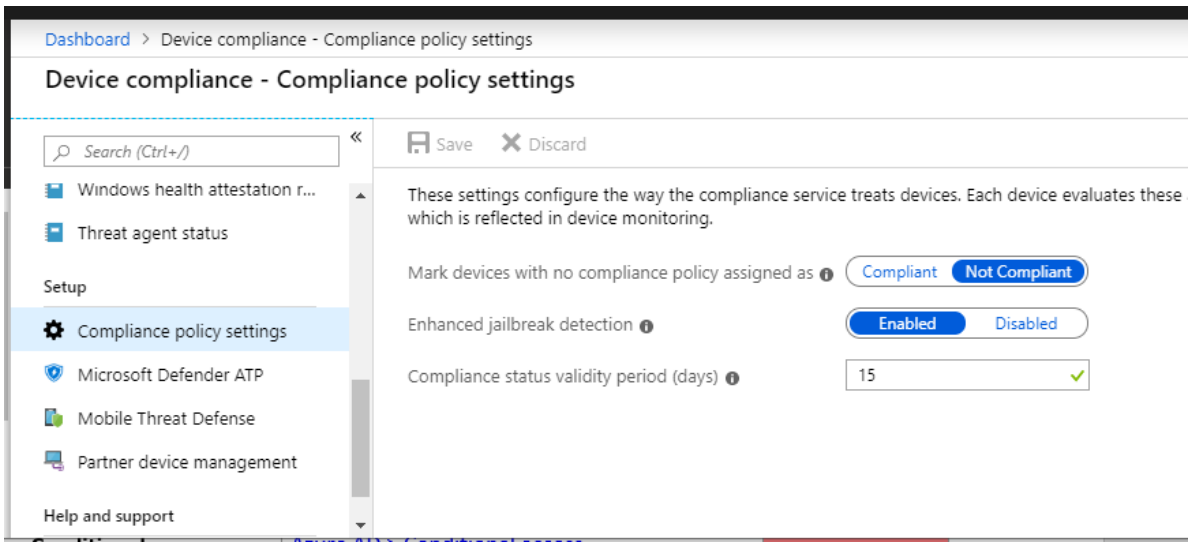
☐ Configure the default Compliance policy settings

Before you manipulate compliance settings, be sure that you do not have any device-based conditional access policies enabled. Review **Device management > Conditional access**. If you find any conditional access policies enabled which "**Require the device to be marked as compliant**" under the Access controls section, then disable them first. The reason being, you could accidentally lock out existing users/devices while manipulating live settings.

See this article for more details on the proper order for implementing device-based conditional access: https://www.itpromentor.com/device-ca-framework/



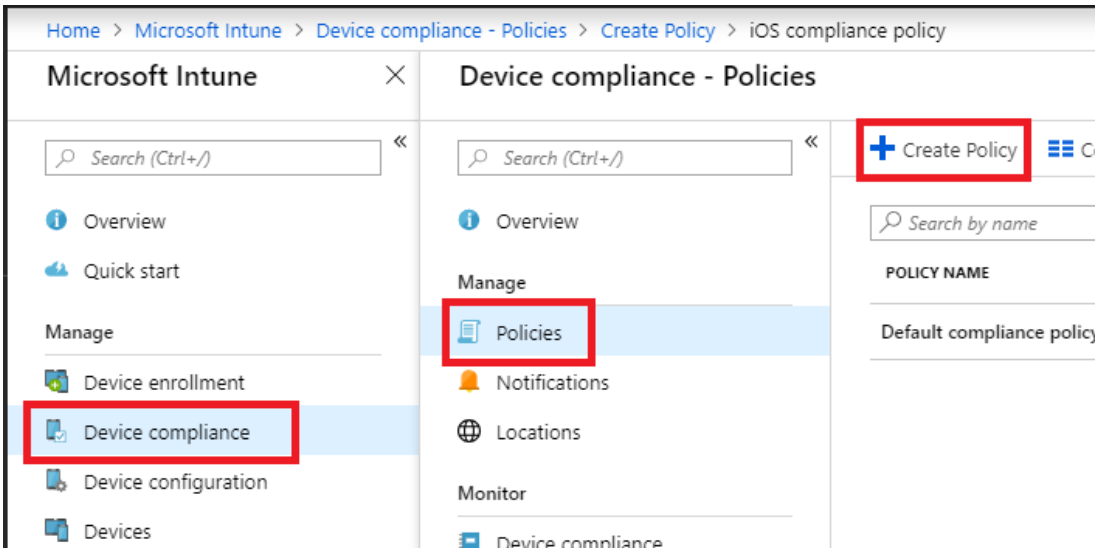
When you are ready to proceed, navigate to **Device management > Device compliance > Compliance policy settings**. Make the following recommended selections:



- Mark devices with no compliance policy assigned as: **Not compliant**
- Enhanced jailbreak detection: **Enabled**
- Compliance status validity period (days): **15**

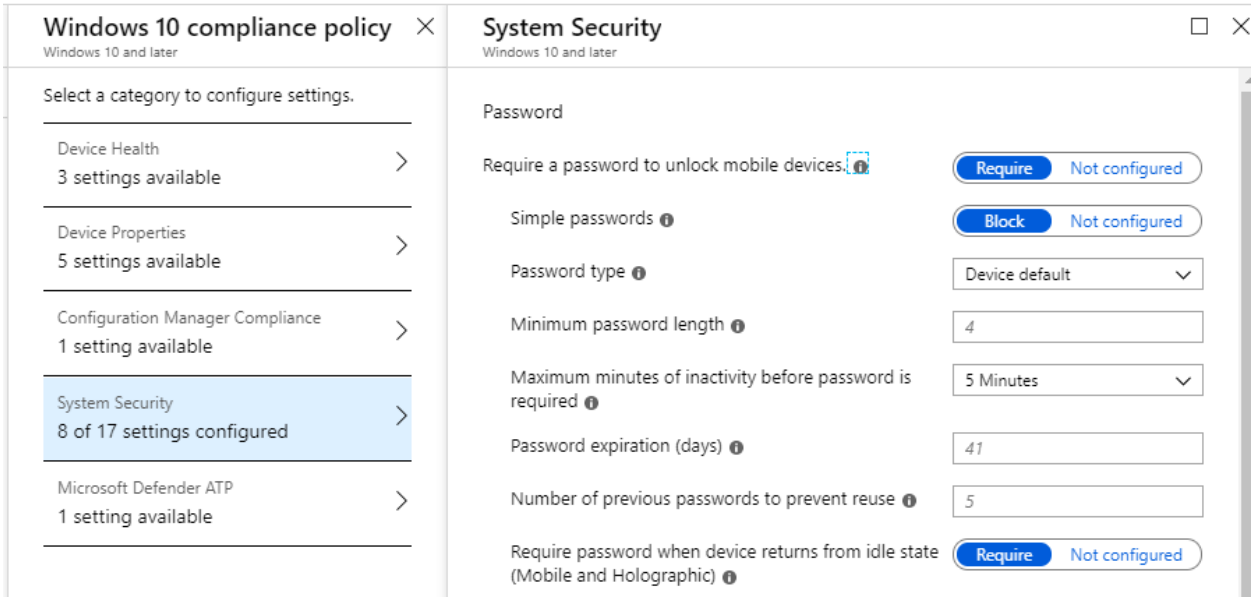
☐ Configure Device Compliance policies

This is a must. You will need to create one compliance policy for each platform that you intend to support and manage. Go to **Device compliance > Policies > Create Policy**.

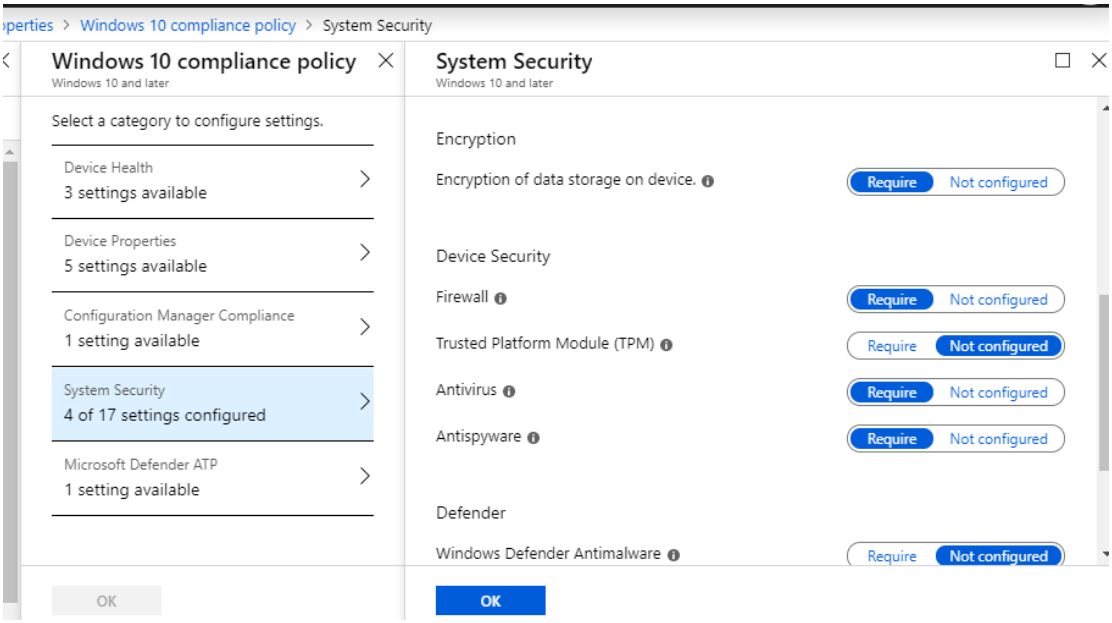


Windows 10 Compliance policy

Create a Windows 10 policy first. Remember that we are already enforcing a PIN via Windows Hello settings, however we have some additional controls here (under **Settings > System Security**). For example the ability to block simple passwords, and to set the maximum inactivity before screen lock (e.g. 5-15 minutes). Recommended minimum password configuration depicted below:



Further down, **Require** all of the following: Encryption, Firewall, Antivirus and Antispyware.

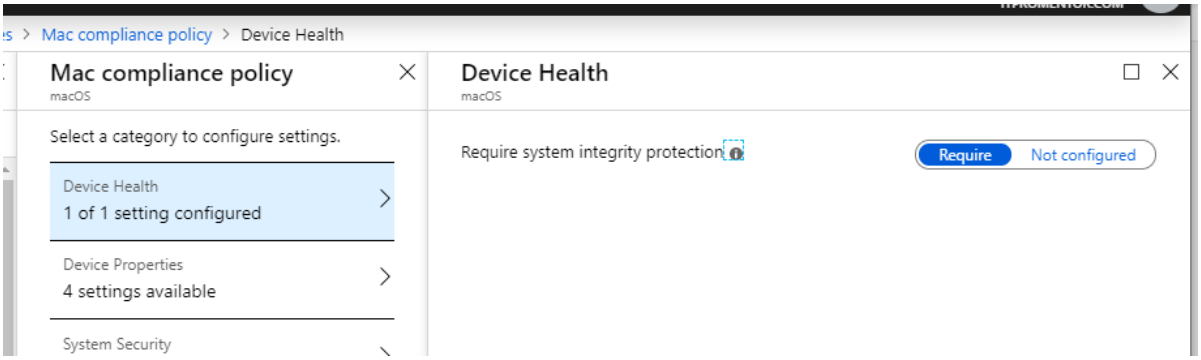


If your environment supports it, consider adding TPM. If you do not have another antivirus/antimalware solution that you manage, add the Windows Defender Antimalware requirement as well.

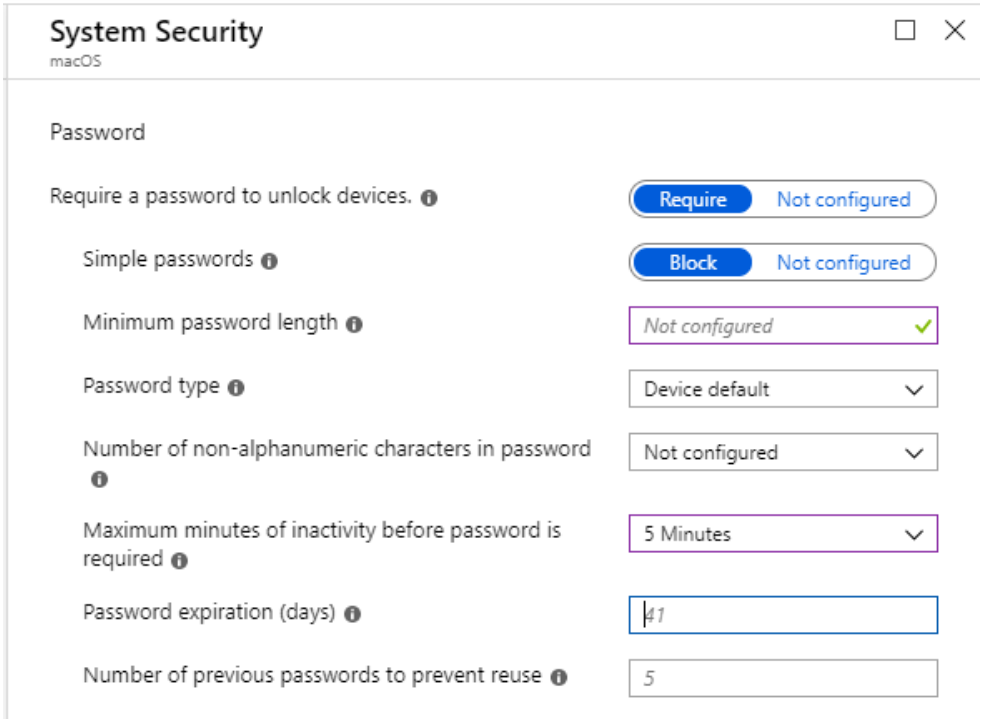
MacOS Compliance policy

Macs can also be subject to compliance and conditional access. Recommended *minimum* settings:

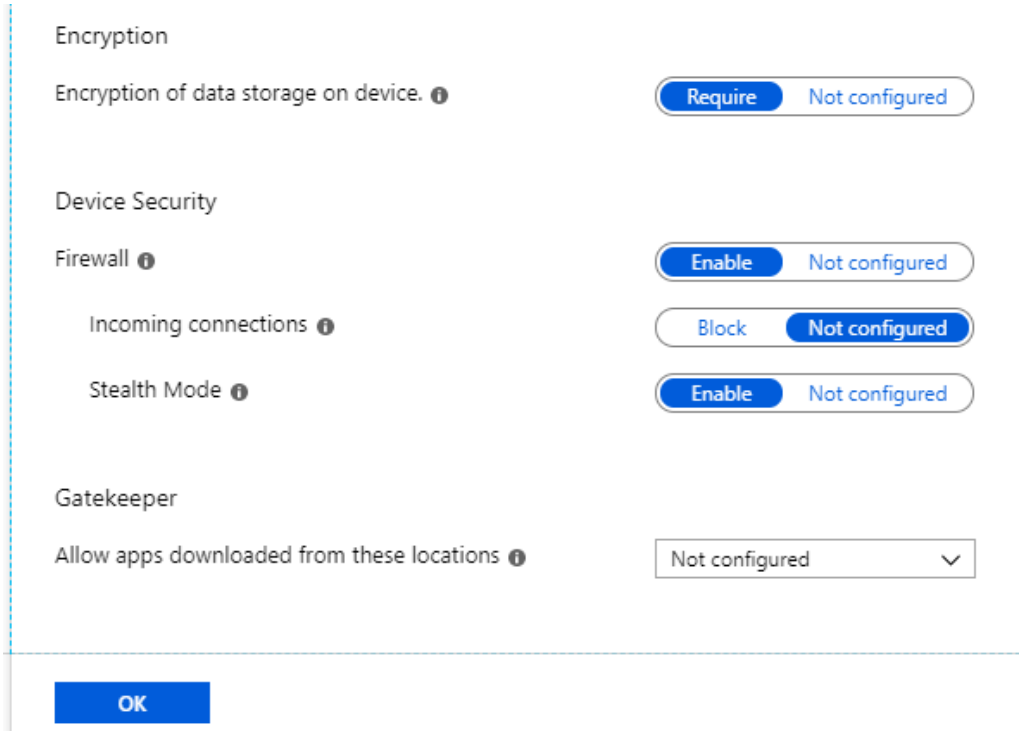
- **Settings > Device Health >** Require system integrity protection: **Require**



- **Settings > System Security >** Password:
  - Require a password to unlock devices: **Require**
  - Simple passwords **Block**
  - Maximum minutes inactivity… **5-15 Minutes**

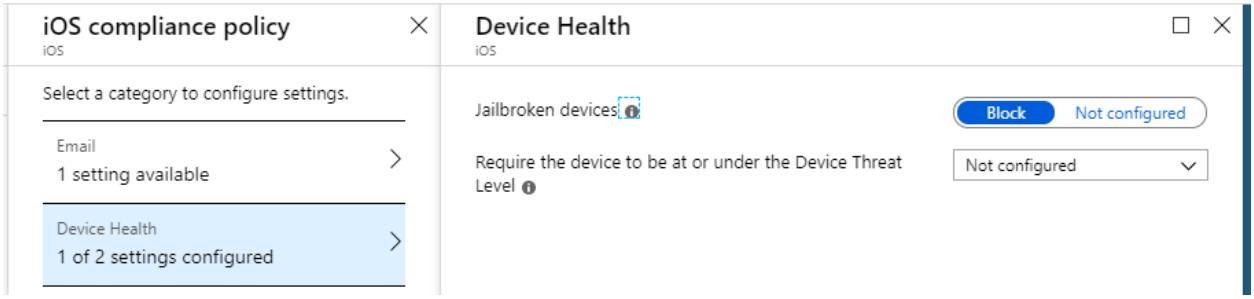


- Also **Require** *Encryption*, **Enable** the *Firewall*, and *Stealth Mode*.

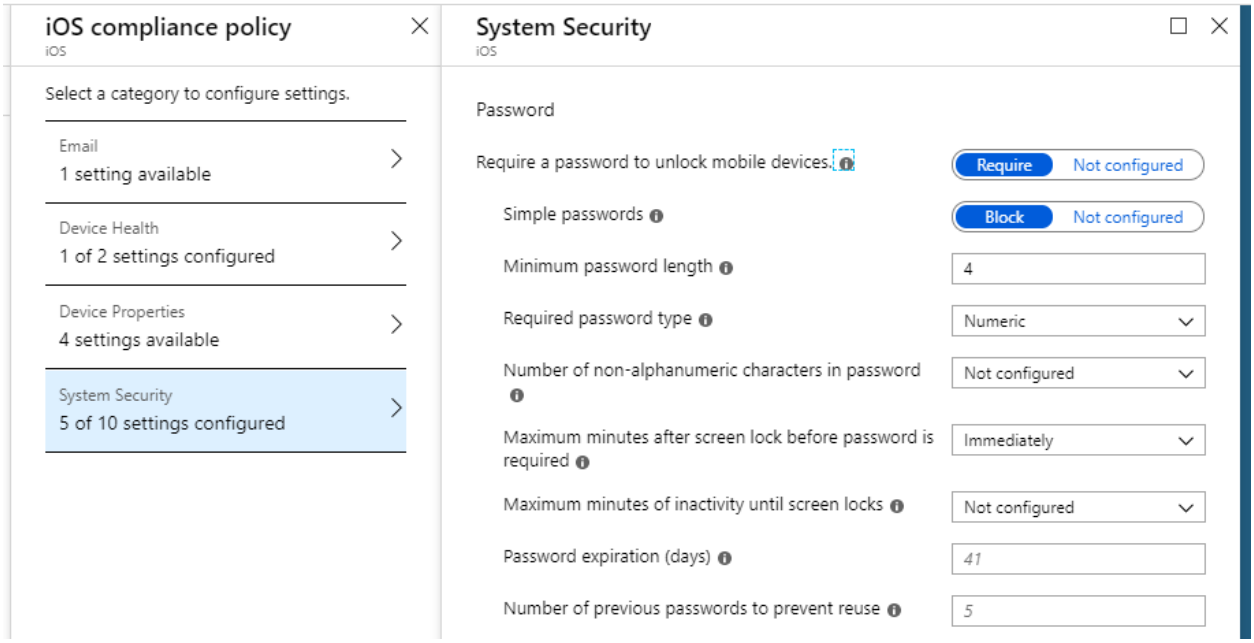


iOS Compliance policy

Recommended minimum configuration includes *Device Health* > *Jailbroken devices*: **Block**

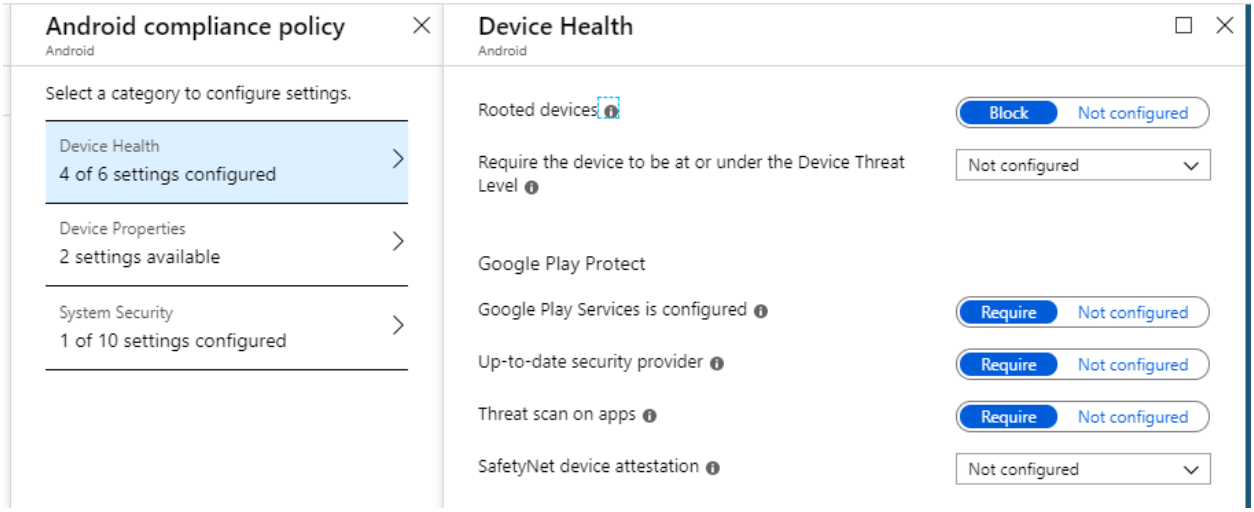


As well, under *System Security*: **Require** password, **Block** simple passwords, minimum length of **4** (**Numeric**) and *Maximum minutes after screen lock*… set to **Immediately**. Note that encryption is achieved automatically with iOS devices (you do not need to specify it, a PIN is sufficient).

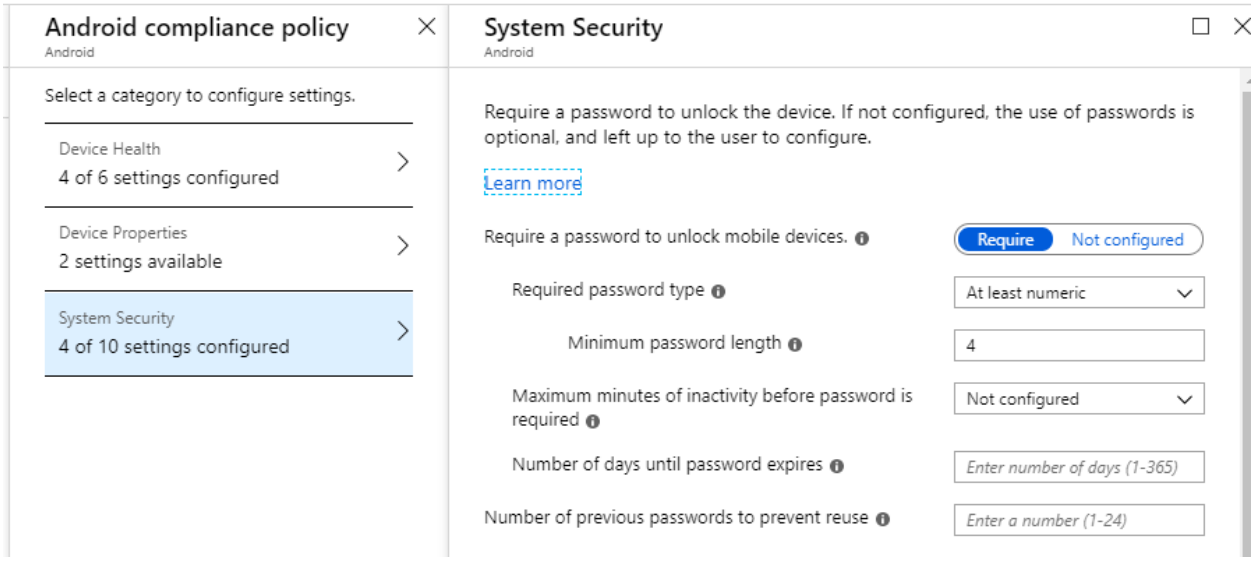


Android Compliance policy

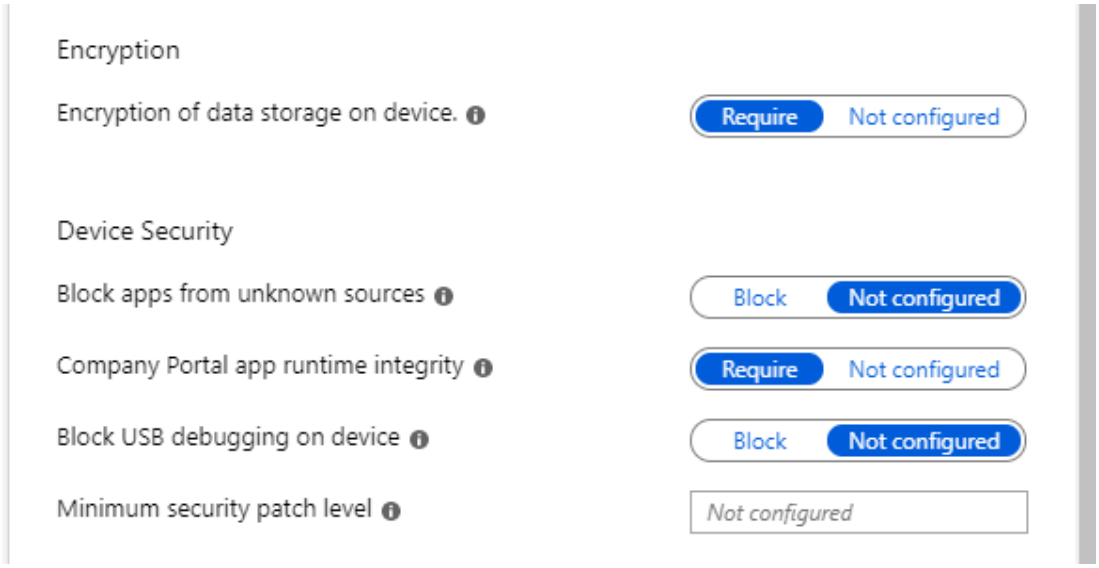
Recommended configuration settings:



Under *Device Health*, **Block** Rooted devices and **Require** Google Play Services. Under *System Security*, align password settings similar to **At least numeric**, and **4** digits:



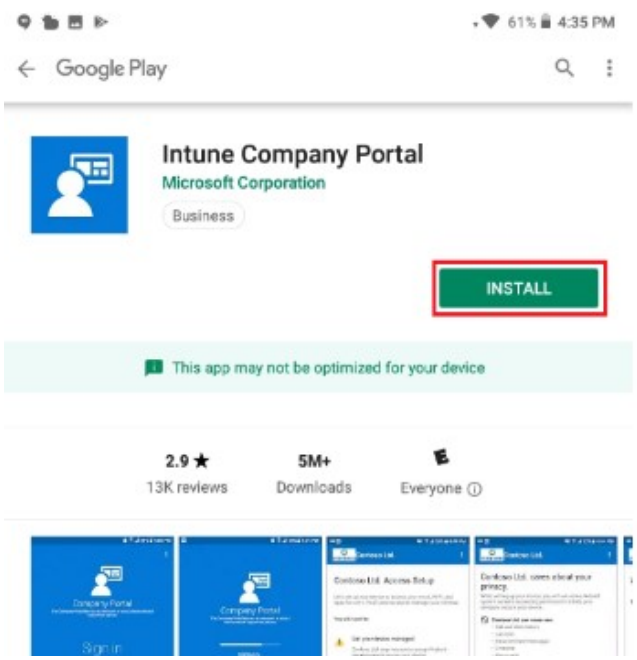
For the remaining *System Security* settings, configure similar to the graphic displayed below:

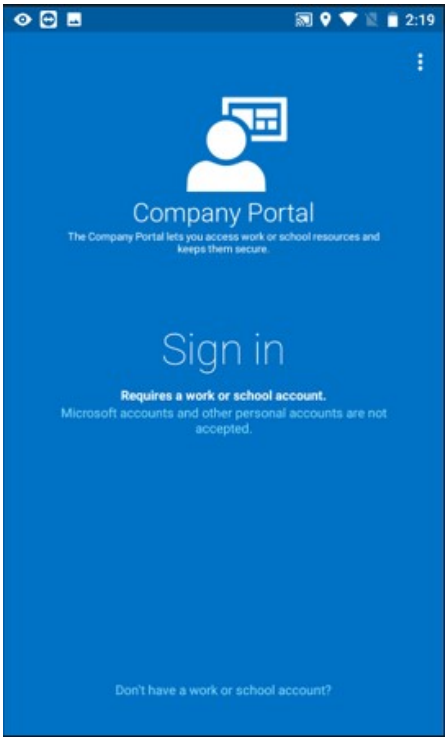


Require for both Encryption and Company Portal app runtime integrity.

☐ Enroll devices

The most common method for enrolling devices (of all types) is the Company Portal app. Simply go the app store on your device of choice and search for Company Portal app. Once you have the app installed, sign into the app using your Microsoft/Office 365 credentials to complete enrollment steps.

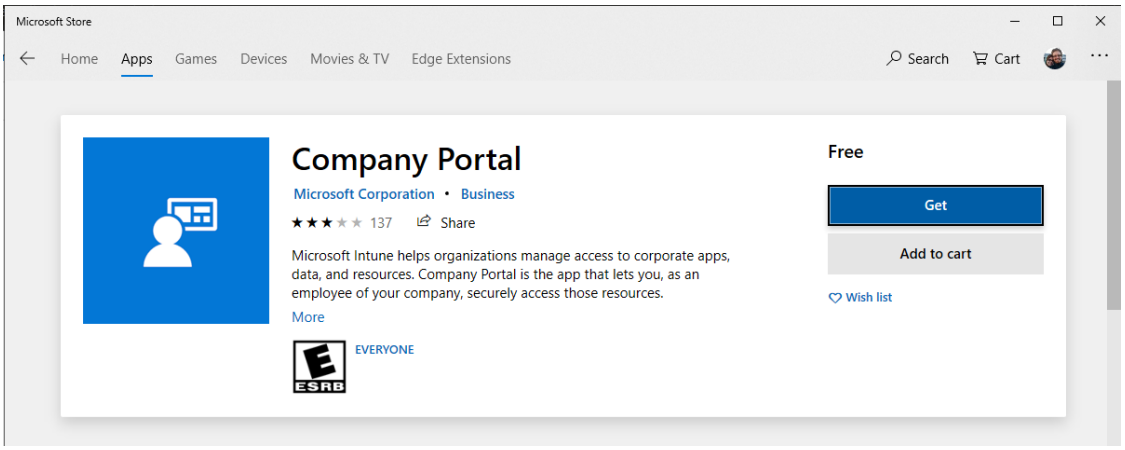




I will not go through all of the screens involved, but a fair warning: there are many prompts that the user must step through to enroll the device, always selecting options in the affirmative such as *Continue*, *Trust*, *Enroll*, *Accept*, *Install*, etc. Not fun. In iOS the user is even directed at one point to go into their Settings app, find the management certificate and click install there, then come back to the app. Yuck. Just one more reason to stick with MAM for mobile devices by default.

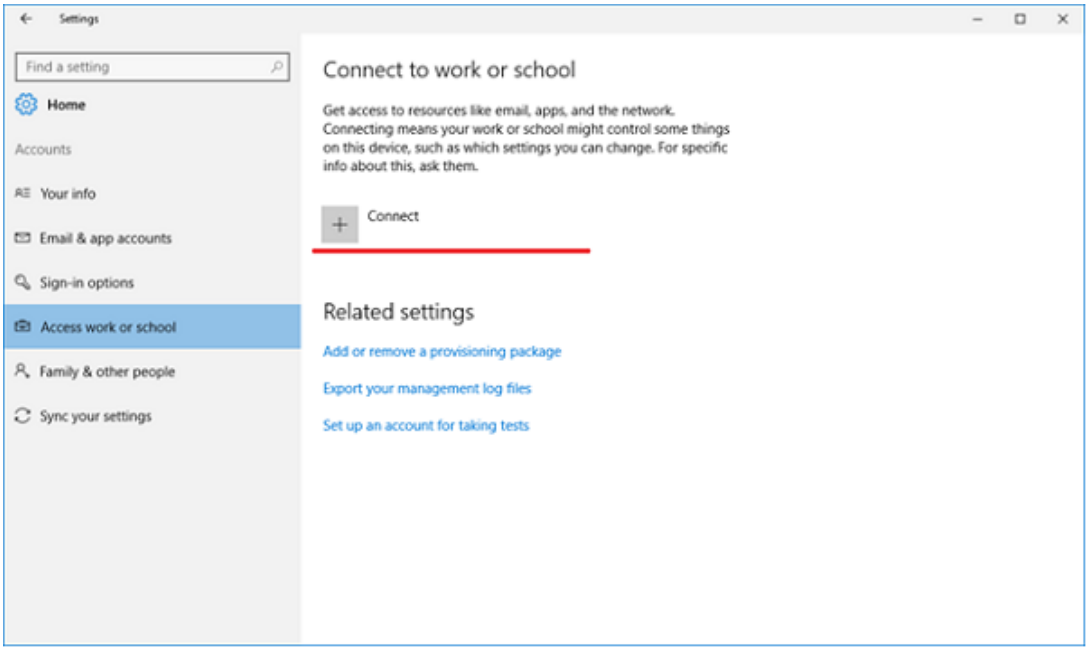
Windows 10 Enrollment options

There are many ways to enroll a Windows 10 device. And yes, the Company Portal app also works here.

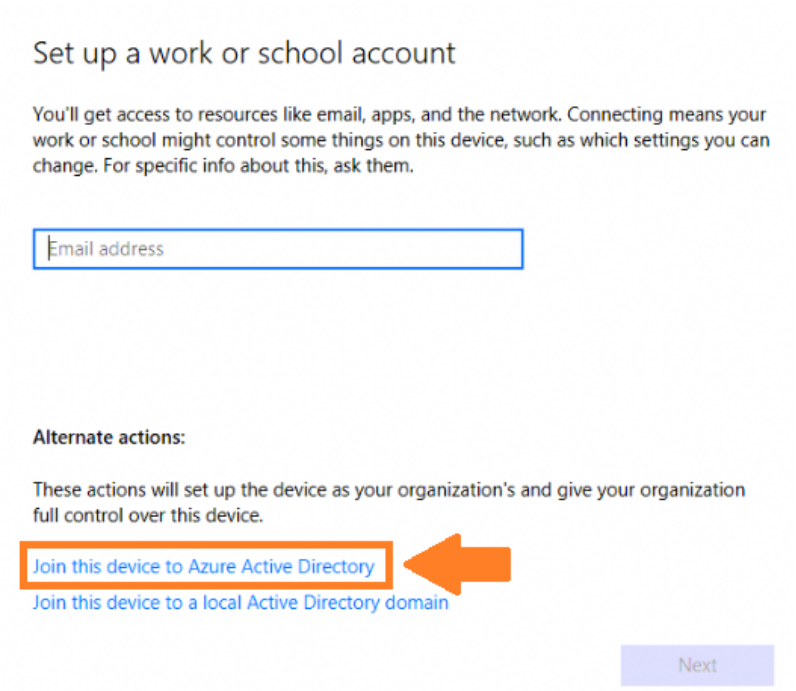


Enroll the device from Settings > Accounts

Another option if your device is part of an existing domain or workgroup, you can join the device easily from **Settings > Accounts > Access work or school**. Just choose **Connect** and sign-in using your corporate Microsoft 365 credentials.

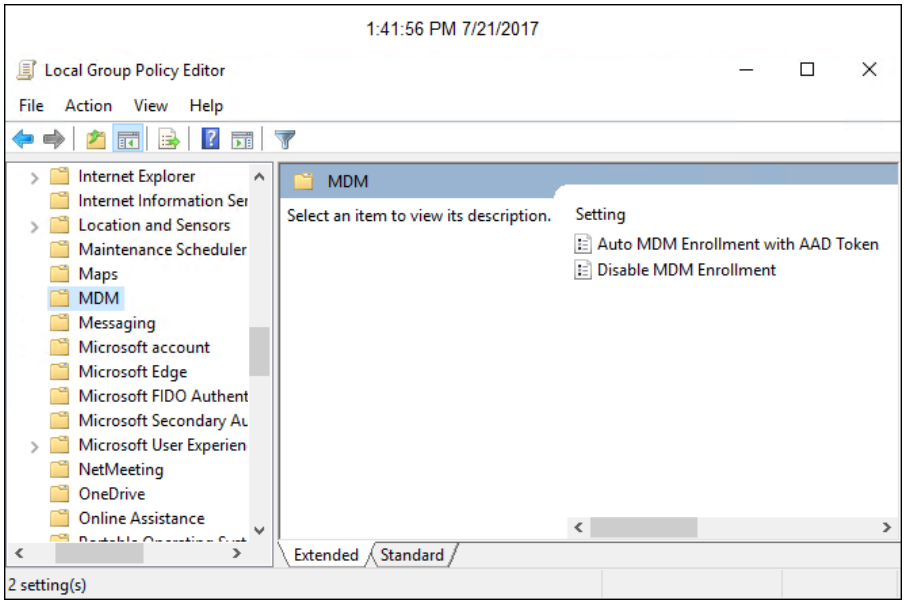


If the device is not domain-joined yet (still in a workgroup) then you can choose the option to Join Azure Active Directory instead, as shown (Azure AD Joined is the preferred configuration):



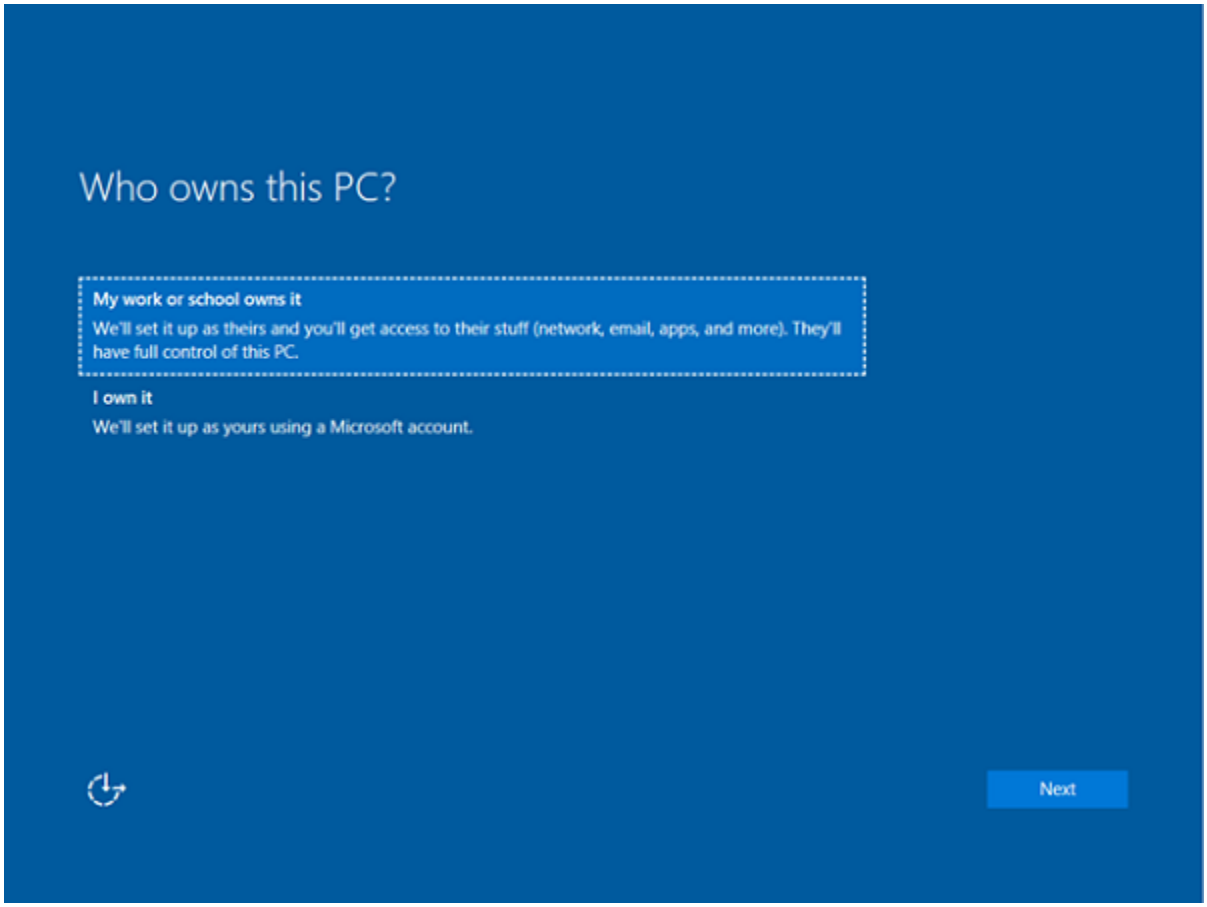
Group policy (hybrid)

If you have an existing on-premises AD, and assuming you're not able to get off of it yet for some crazy reason (but have you just tried it?), then you can use a Group policy (see this link) to initiate enrollment also. Note: This requires Azure AD Connect to be in place.



Out-of-Box Experience (OOBE) setup (preferred/recommended)

When a user gets a new device (or resets an old one), they can simply choose work or school when they set it up for the first time. Using their corporate credentials will join the device to Azure AD, and it will be enrolled into Intune. Any software assigned to the device will come down, etc.



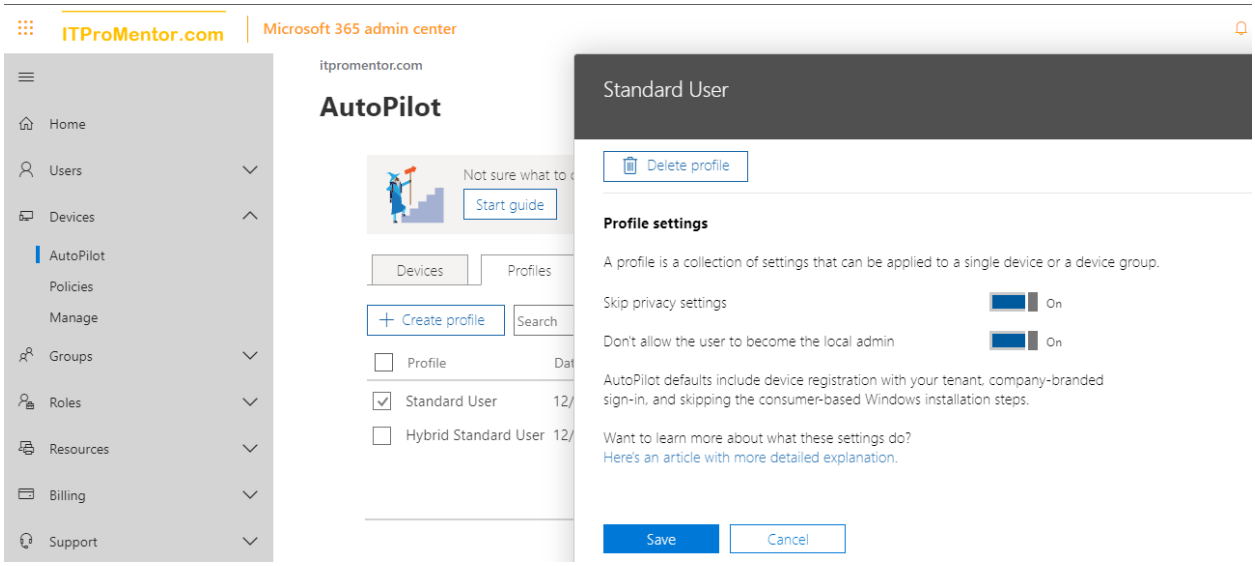
Windows 10 Autopilot

The only differences between the OOBE option I just described and Autopilot are as follows:

1. Autopilot can tell the device to skip past some of the first run experience screens (privacy)
2. You have the option to enforce *Standard* user, rather than letting the user be local Admin

And that's about it.

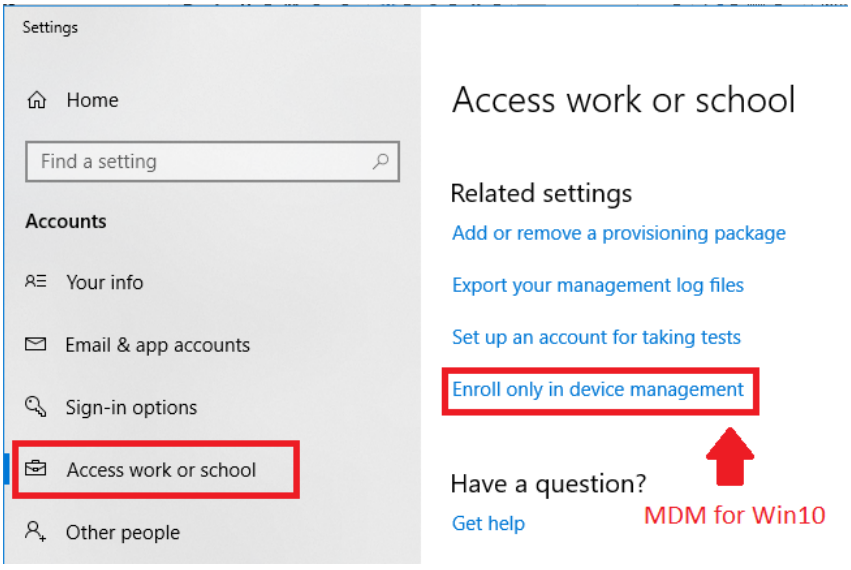
To configure Autopilot requires that you get unique device identifiers imported into Intune in advance. You'd want to get these from the OEM, but they can also be exported via PowerShell from the device. I honestly never do this, except in a lab.



You can basically create profiles, and then assign the imported devices (from CSV) to the profiles that have been created. To do this from the Microsoft 365 admin center is trivial (**Devices > Autopilot**). To do this from the Intune portal, just follow [this Microsoft article].

MDM Only (Do not use)

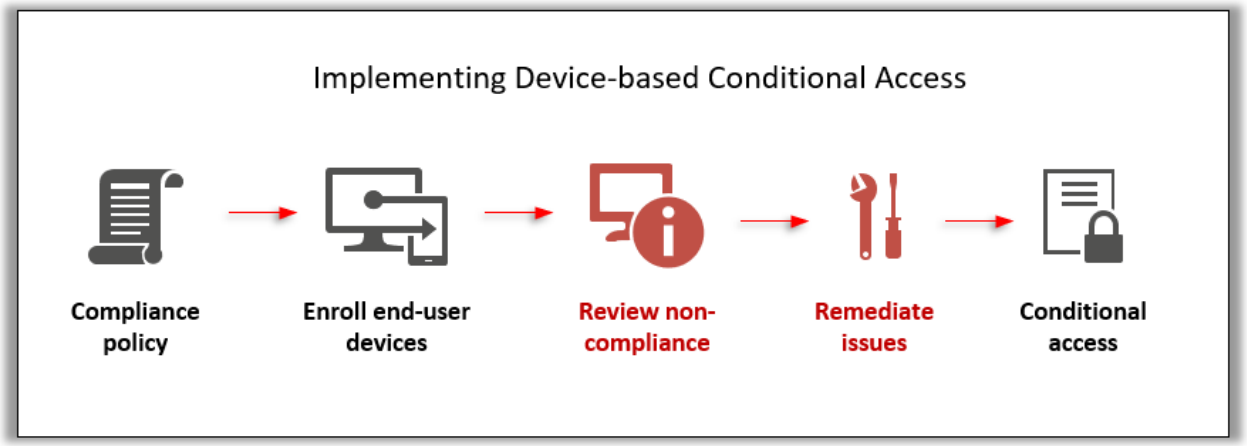
It is also possible for Windows devices to become MDM enrolled, without joining Azure AD. This would be more intended for a BYOD scenario. However, this option is not recommended as it does not support Conditional Access.



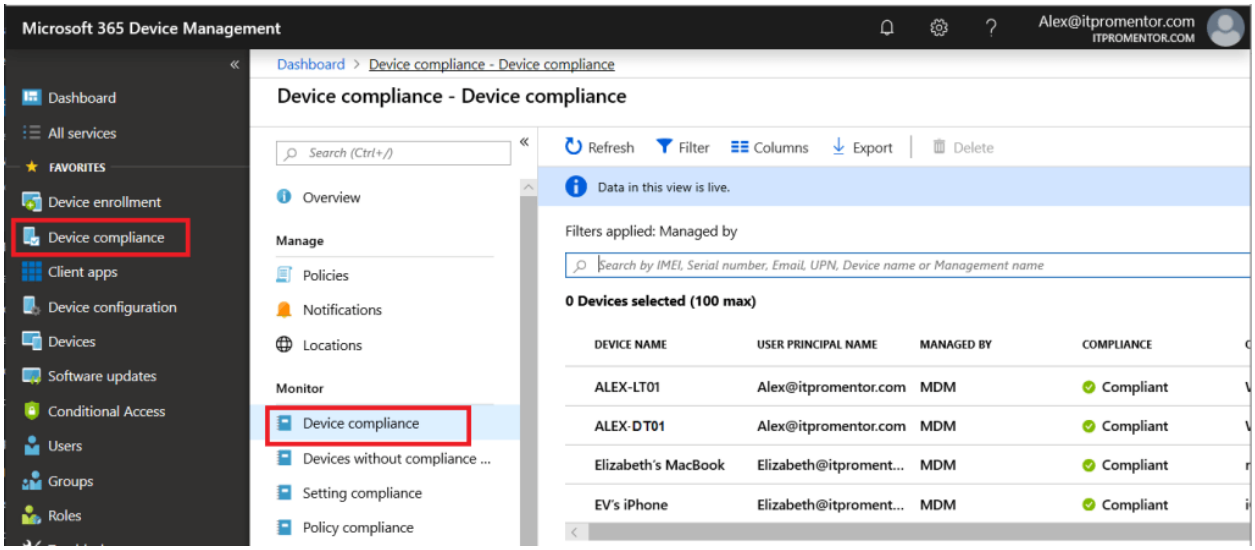
To manually enroll a Windows 10 device in "MDM only," go to **Settings > Accounts > Access work or school**. Find the link for **Enroll only in device management**.

☐ Verify compliance status of enrolled devices

It is only necessary to complete this step before the very first time you go to enable device-based Conditional access (in other words, any Conditional access policy using the control **Require device to be marked as compliant**). Devices joining subsequently will be required to meet the compliance before gaining access for the first time.



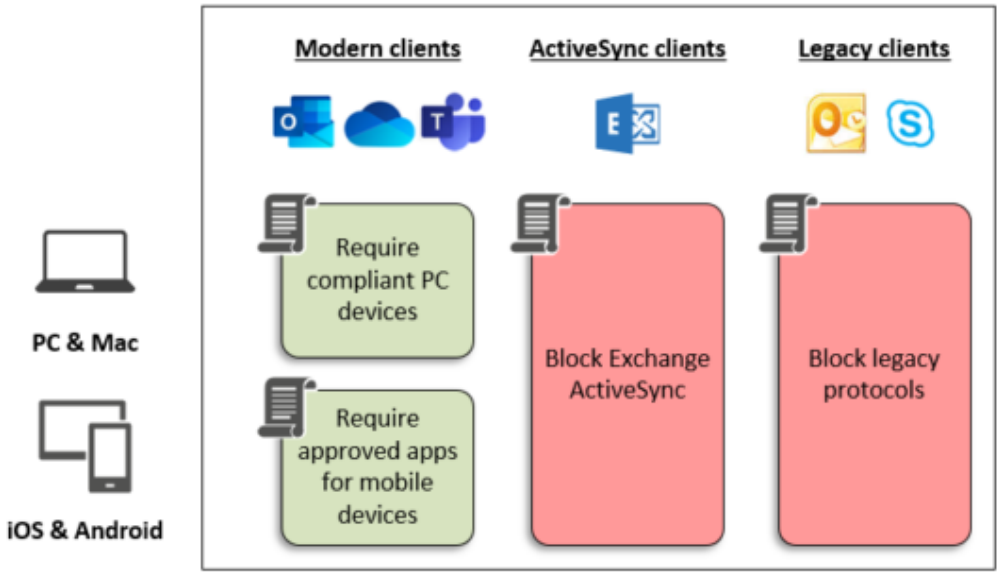
This is easy to do, simply go to **Device Compliance** and choose **Device compliance** again under *Monitor*.



Identify any devices which do not meet compliance. If you click on one of the devices then, you can pick **Device compliance** again under Monitor, and drill in to see which policies are failing or passing for that specific device. Remediate the issues on the devices before enabling Conditional access.

☐ Enable Conditional Access

I have written an entire guide on this topic, with an associated PDF of the policy design.



Refer to those resources for more details on how to set up a more comprehensive baseline. Here is a summary of the relevant policies with regard to devices and client apps managed by Intune:

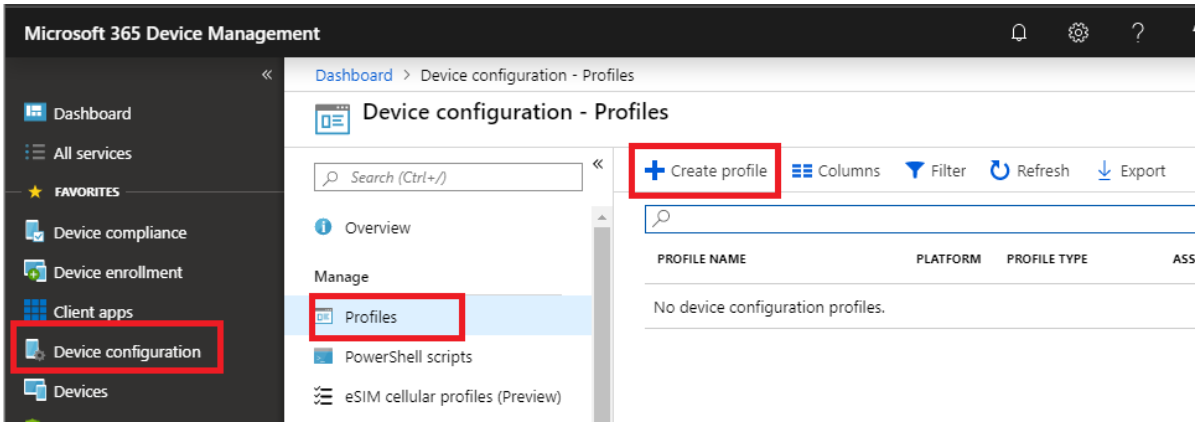
Policy	Assignments	Conditions	Access controls
Require compliant PC devices (MDM is required)	o Users > **All users** o Cloud apps > **All apps**	o Device platforms: **Windows** and **MacOS**; o Client apps: **Mobile apps & desktop clients** and **Modern authentication clients**	o Require device to be marked as compliant o Require one of the selected controls
Require approved apps for mobile devices (MDM is optional)	*same as above*	o Device platforms: **Android** and **iOS** o Client apps: *same selections as above*	o Require approved client app o Require one of the selected controls
Block legacy protocols	*same as above*	o Client apps > **Mobile apps & desktop clients**, **Other clients**	o Block access
Block Exchange ActiveSync	o Users > **All users** o Cloud apps > **Office 365 Exchange Online**	o Client apps > **Mobile apps & desktop clients**, **Exchange ActiveSync**	o Block access

☐ Setup Device Configuration profiles

Whereas compliance policies are linked with Conditional access, device configuration profiles are not—they have no bearing on whether a device is considered "compliant." Therefore they cannot be used as a bar to entry. However, once devices have been enrolled and brought under compliance, then you can use Device configuration to apply settings, similar to how a domain-joined PC in the past would have received policy settings via Group Policy.

For each platform, there exist multiple profile types (e.g. WiFi, VPN, Device restrictions, etc.) and many settings. The profiles you would typically build are almost entirely dictated by the needs of the organization. Do you require corporate WiFi keys to be pushed down to the client? Should end users be able to access the app store, or save to iCloud? Every environment is different and it is hard to say there is any single "best practice."

Nevertheless, I will discuss a handful of Windows 10 settings that I would recommend most small and mid-sized businesses at least review when implementing Intune for the first time. And before you ask: I have no opinion on MacOS/iOS/Android—I tend to find that the settings controlled via the compliance polices are "good enough" for these other platforms.

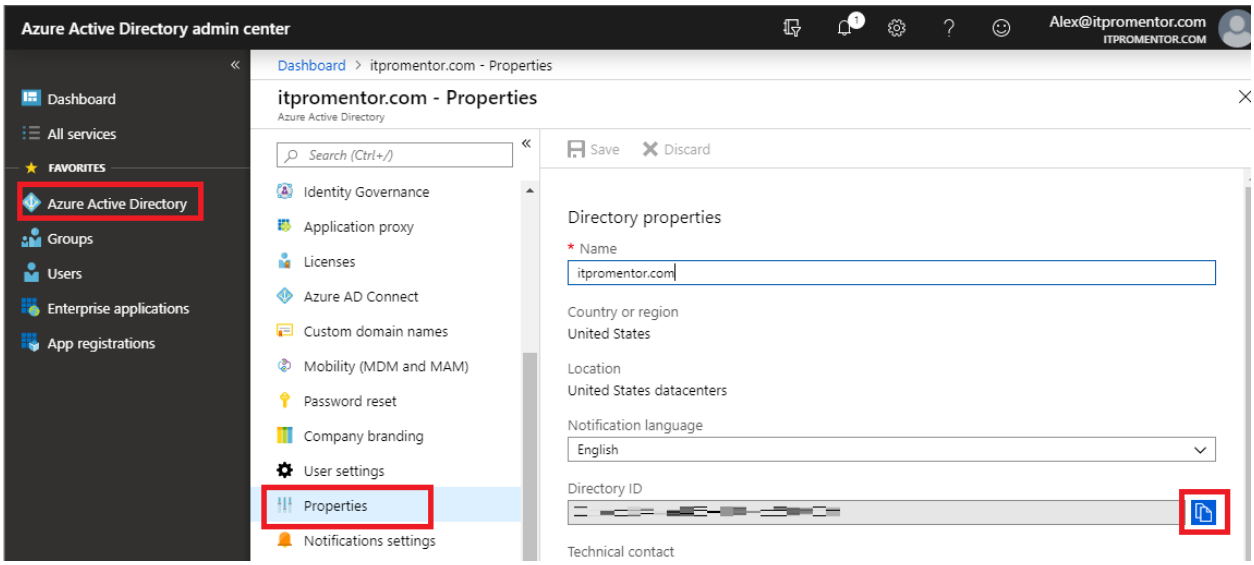


☐ Control the OneDrive for Business experience

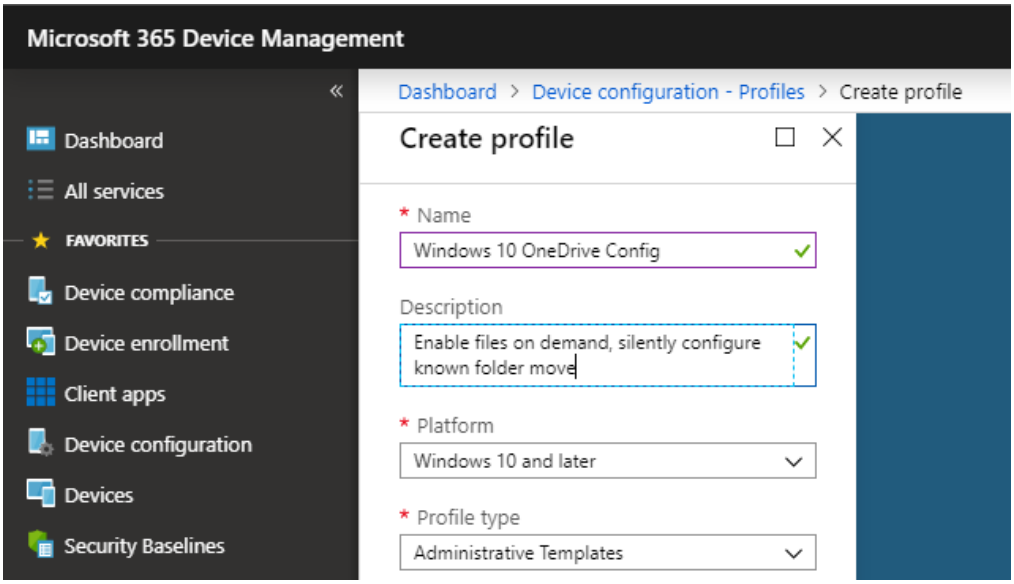
If you aren't using OneDrive in your organization yet, I encourage you to start—it's a fantastic app—one of my favorites in the whole Office 365 suite. To enable the best experience on Windows 10, you will want to setup:

1. Files On-Demand
2. Known Folder Move
3. Automatic sign-in using Windows credentials (this means users should be using their corporate Microsoft 365 account to sign into Windows, not a local account)
4. Automatically sync certain libraries

Before you begin fetch the tenant ID from **Azure AD admin center > Azure Active Directory > Properties** blade. Copy the **Directory ID**.

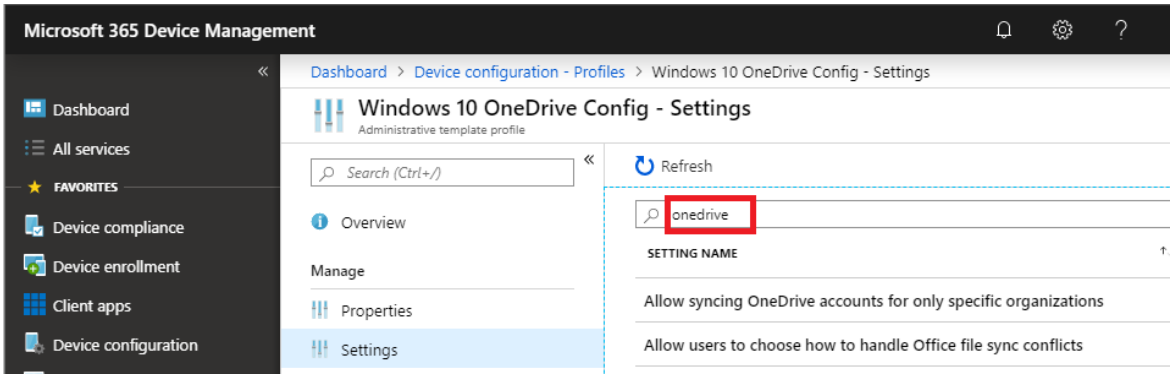


Return to Intune, go to **Device configuration > Profiles**. Pick **Create Profile**.



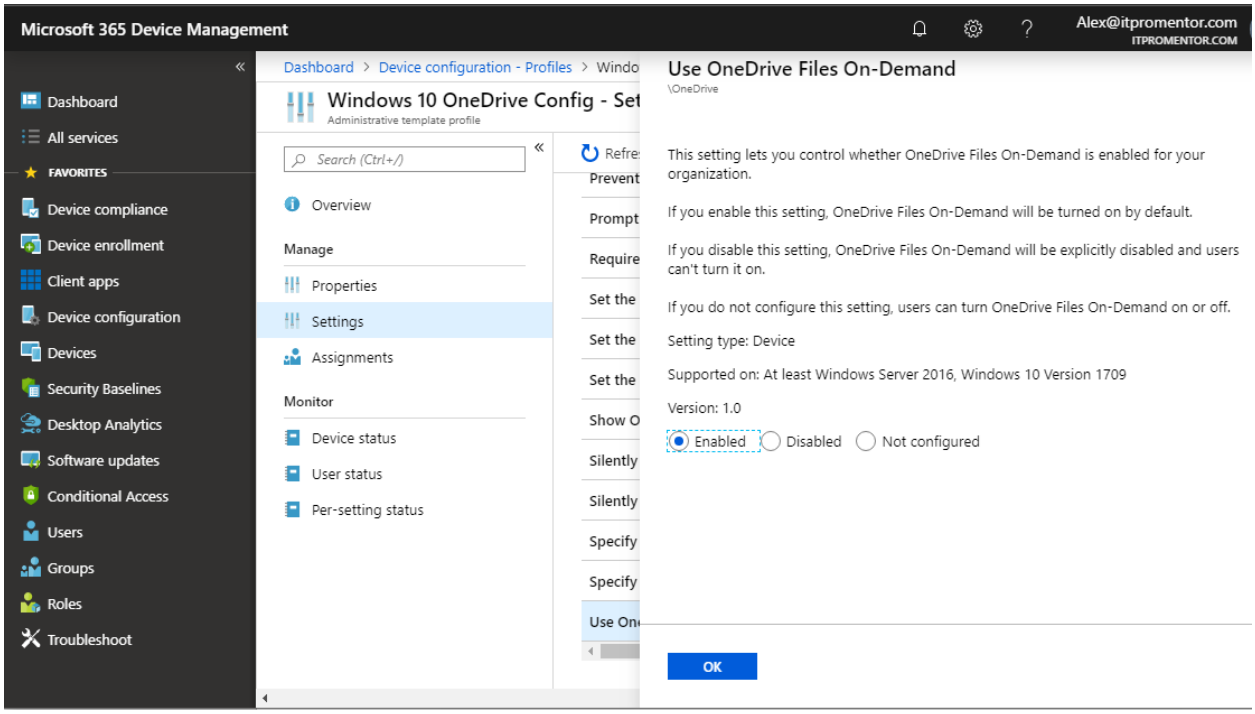
First, give this a descriptive name like **Windows 10 OneDrive Config**, and a description like the one pictured. Pick **Windows 10 and later** as the *Platform*, and **Administrative Templates** as the *Profile type*. Click **Create**.

Under **Settings**, type “onedrive” in the search field to filter your choices.

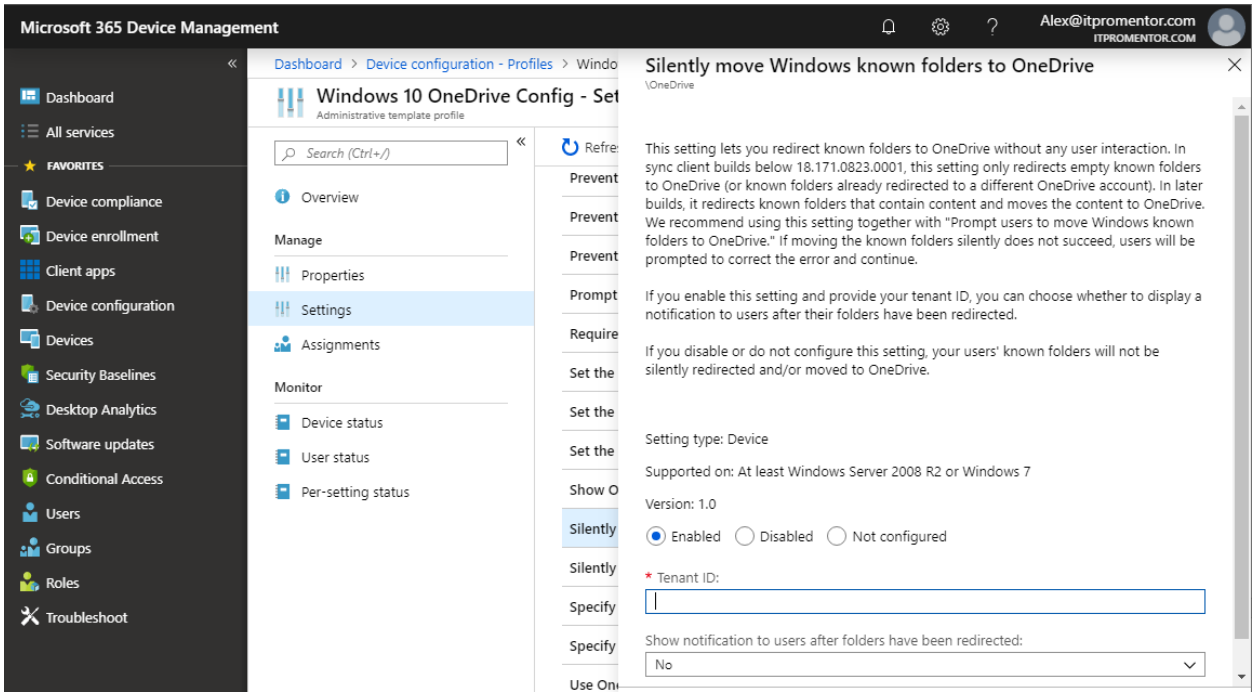


Scroll down to enable the following settings:

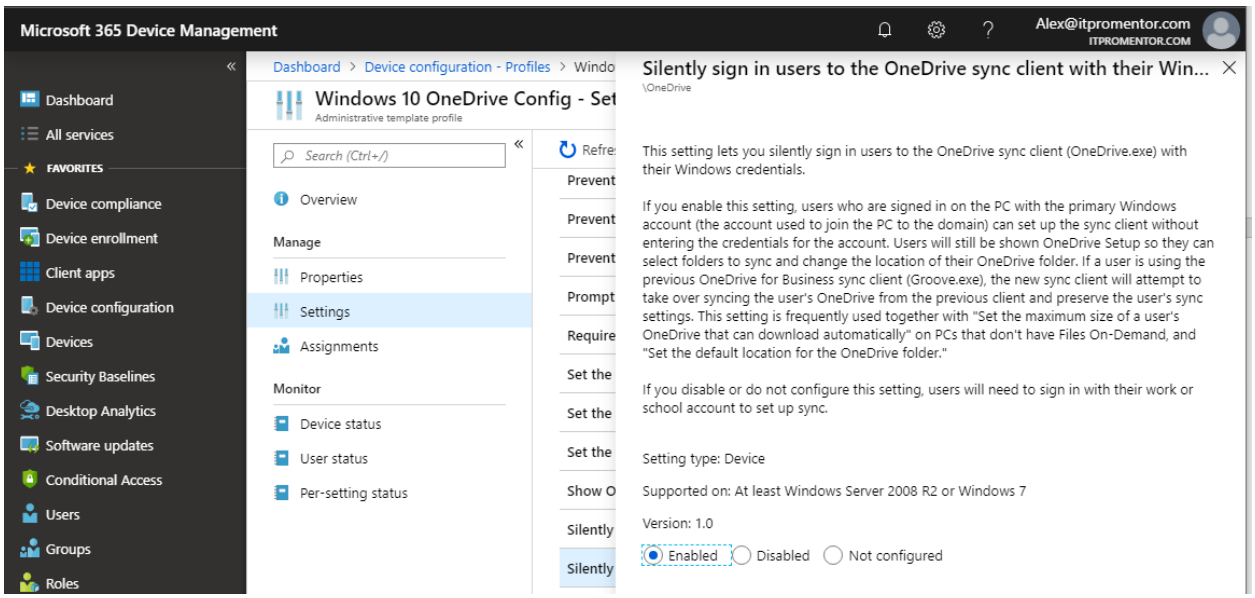
1. *Use OneDrive Files On-Demand*: Choose **Enabled**. **OK**.



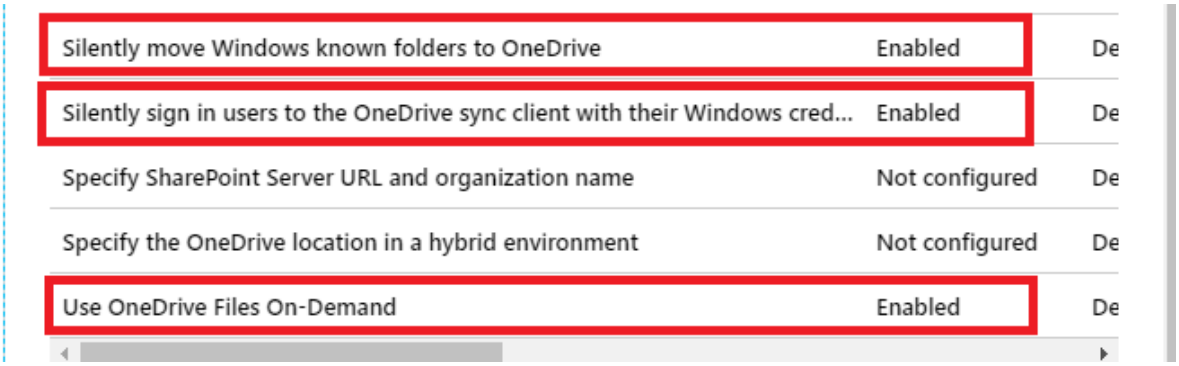
2. *Silently move Windows known folders to OneDrive*: Choose **Enabled**. Paste the Directory ID from Azure AD admin center into the **Tenant ID** field. **OK**.



3. *Silently sign in users to the OneDrive sync client with their Windows credentials*: **Enabled**.



You should end up with settings similar to this:

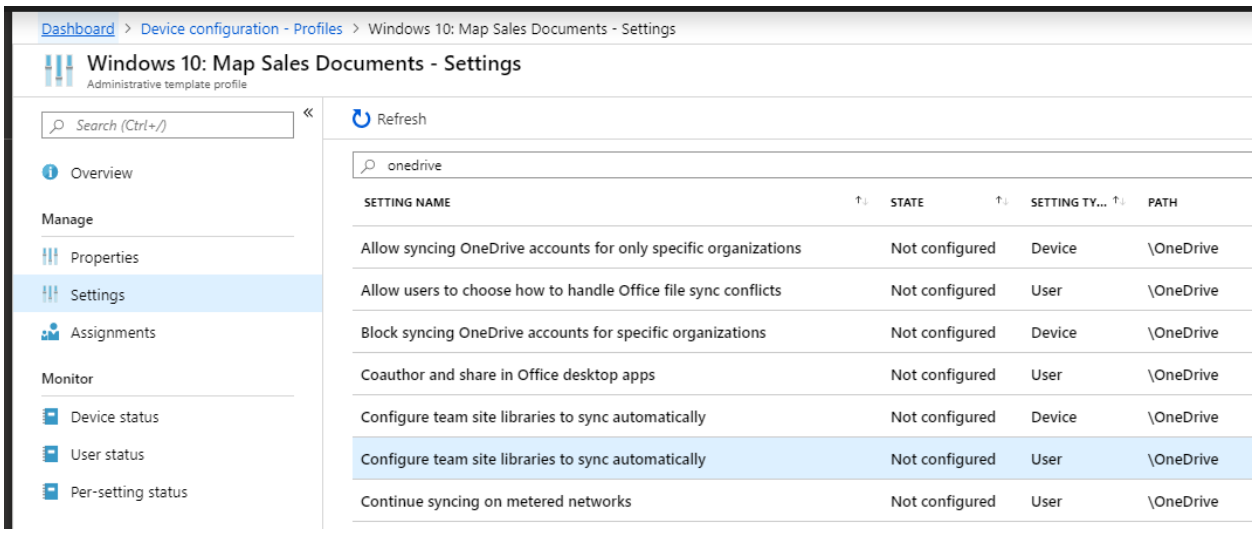


This policy can be assigned broadly, as most everyone should be using these settings.

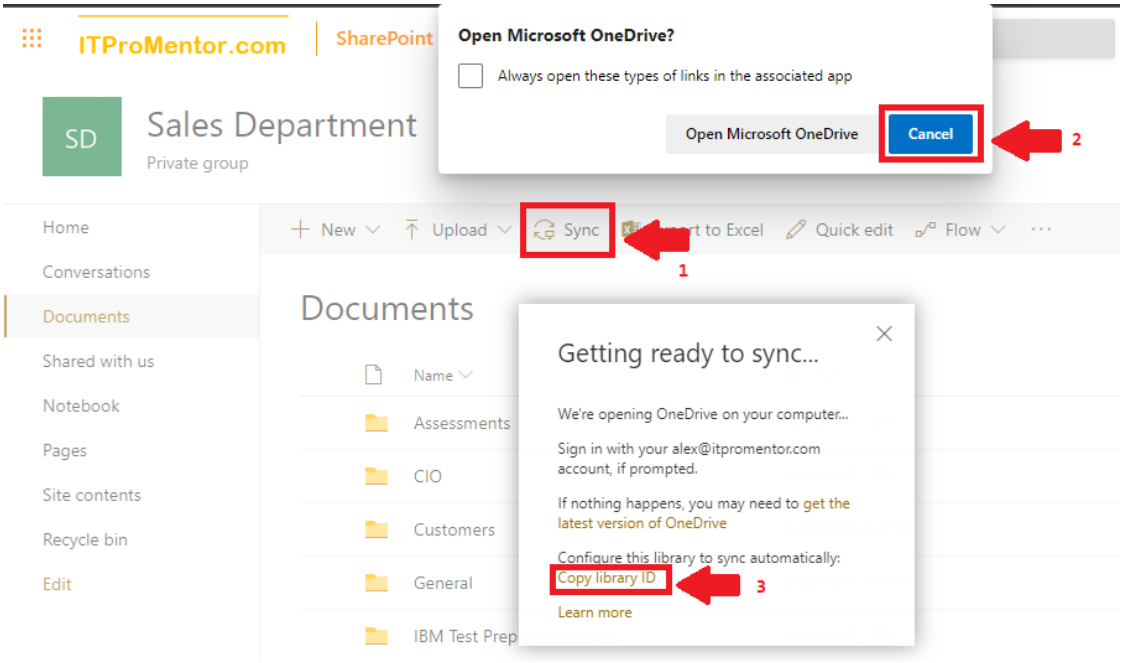
To automatically sync certain SharePoint document libraries to File Explorer in Windows, you would want to create a separate profile. Make as many of these as you need to—similar to mapped drives, these would only be assigned to the users who need access to those locations. For example, if you had a sales department with a Team site, their document library would be mapped using this mechanism (rather than mapped drives pointing to a file server).

Map Shared Document libraries automatically

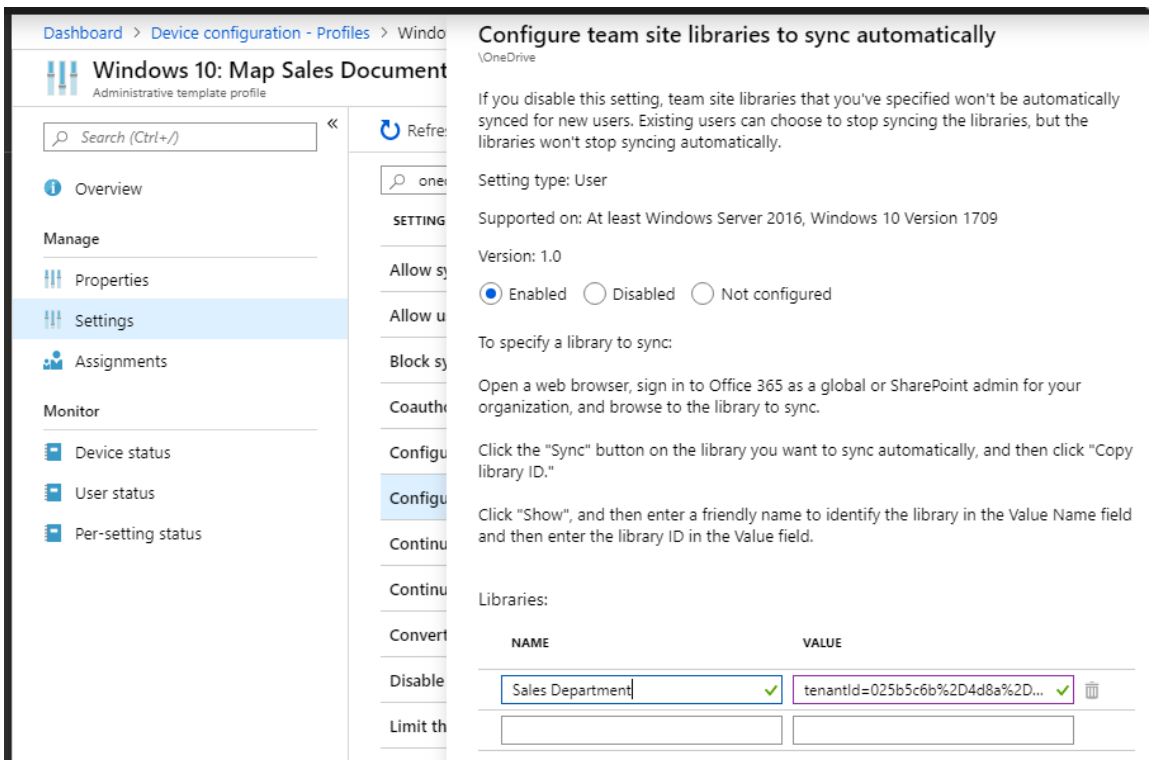
Repeat the process of creating a new profile, selecting **Windows 10 and later**, and **Administrative Templates** as the type. Choose the option **Configure team site libraries to sync automatically** (using the **User** Setting Type). Pick **Enabled**.



As you will see, to configure this setting, it is necessary to retrieve the **library ID** for each library you wish to sync. Navigate to the library in SharePoint Online. (1) Click **Sync** at the top, then (2) **Cancel** out of the prompt to Open Microsoft OneDrive, finally (3) **Copy library ID**.



In the configuration profile, paste the library ID into the field called “VALUE” and give it a friendly name.



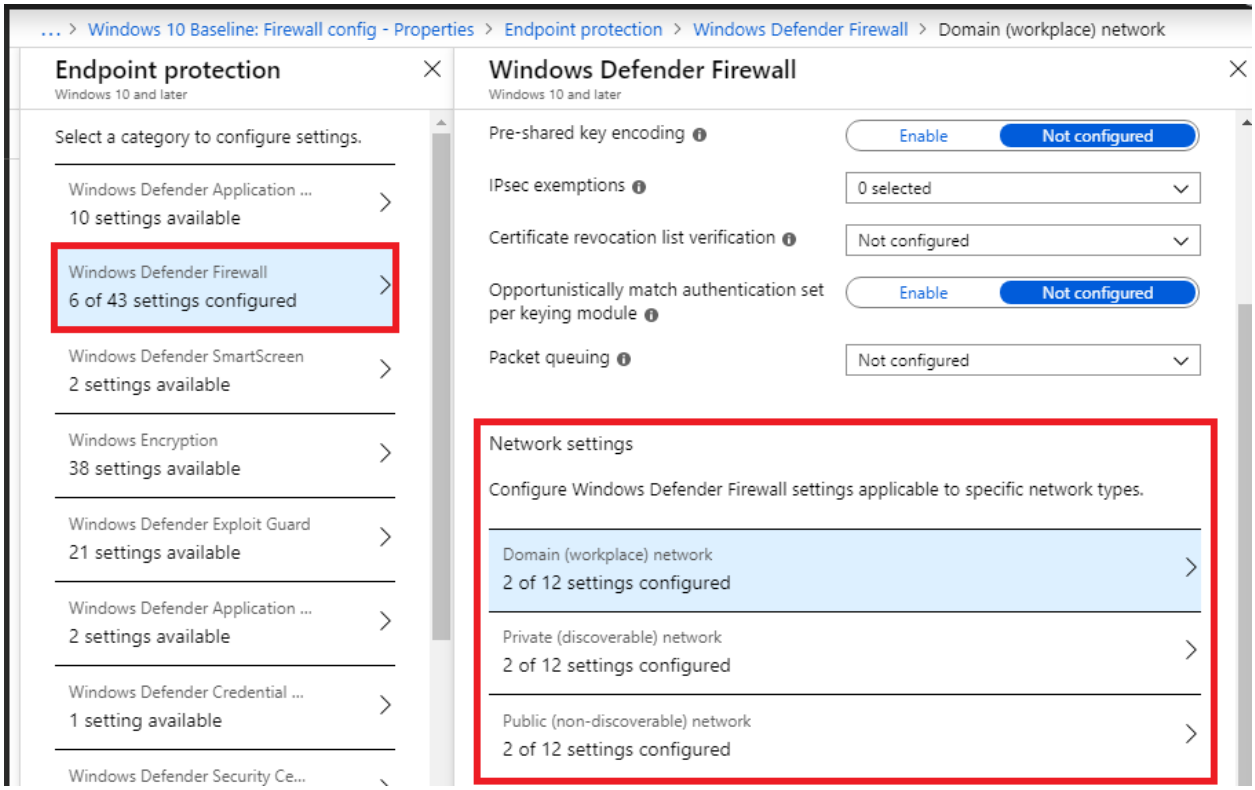
Repeat this process for each library you need to map. Under **Assignments**, you can scope these policies to the proper groups (e.g. use the same Office 365 Group that is associated with the Team site).

☐ Windows 10 Device Restrictions & Endpoint Protection settings

Windows 10 includes a lot of really great features for locking down and protecting endpoints, built-in to the OS. But beware, not all features are available to Windows 10 Pro / Business users—some specifically require Windows 10 Enterprise. Nowhere in the Intune portal does it indicate which are which. Also, these things tend to change over time (what features are supported on what versions), so refer to Microsoft's Windows 10 edition comparison. Enterprise editions generally support everything—only MDATP is specifically available in E5 or purchased separately as on add-on to E3.

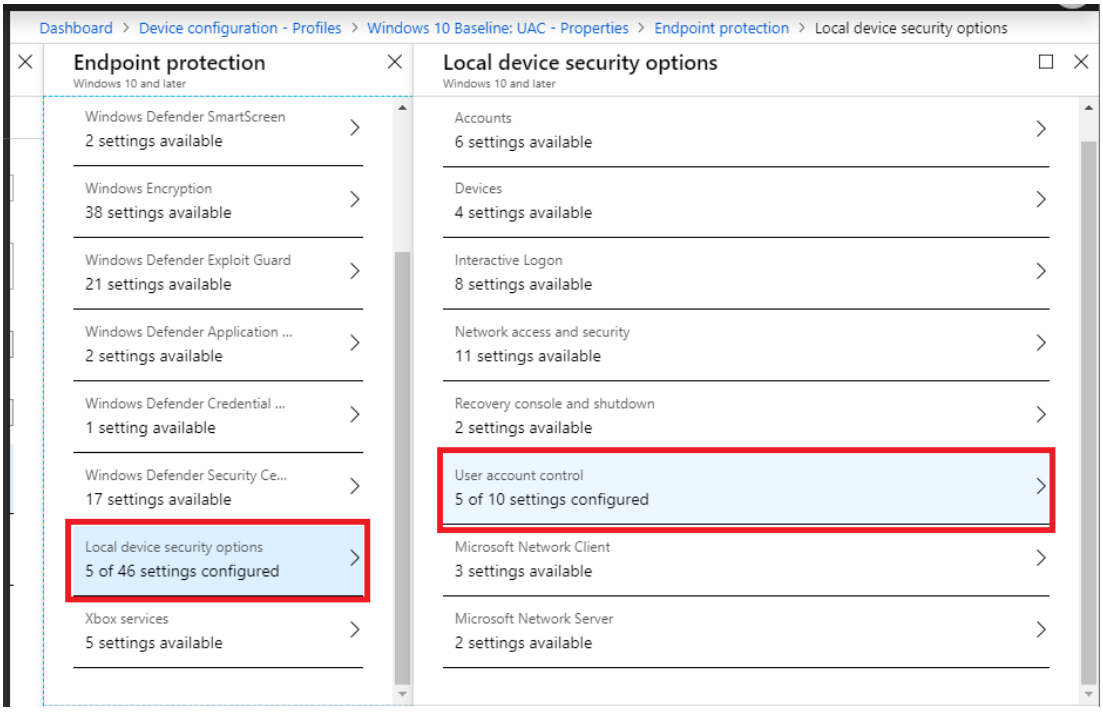
Windows Defender Firewall

To enable the firewall, build a profile for **Windows 10 and later**, with **Endpoint protection** as the type. Under Settings choose Windows Defender Firewall. **Enable** the firewall for each network type (Domain, Private and Public). Also recommended to block all incoming connections by default (note: may not be appropriate for every environment).

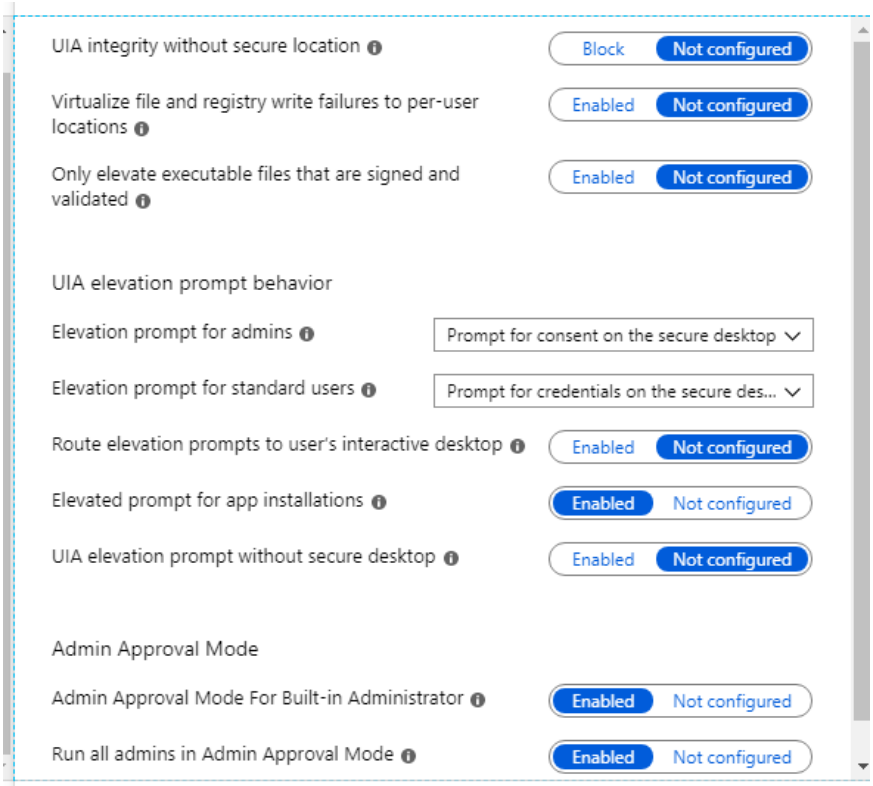


User Account Control

Profile type: **Endpoint protection**. UAC is not an optional setting. I don't understand people who think otherwise, especially when running as local admin (and so many do). This is equivalent to "Always notify" (the only correct option). Go to **Local device security options > User account control**.

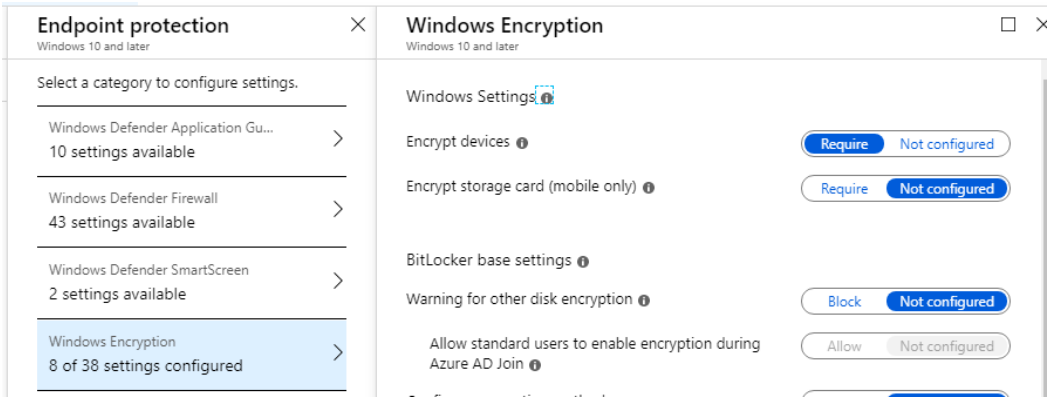


Make the following settings selections (as pictured):

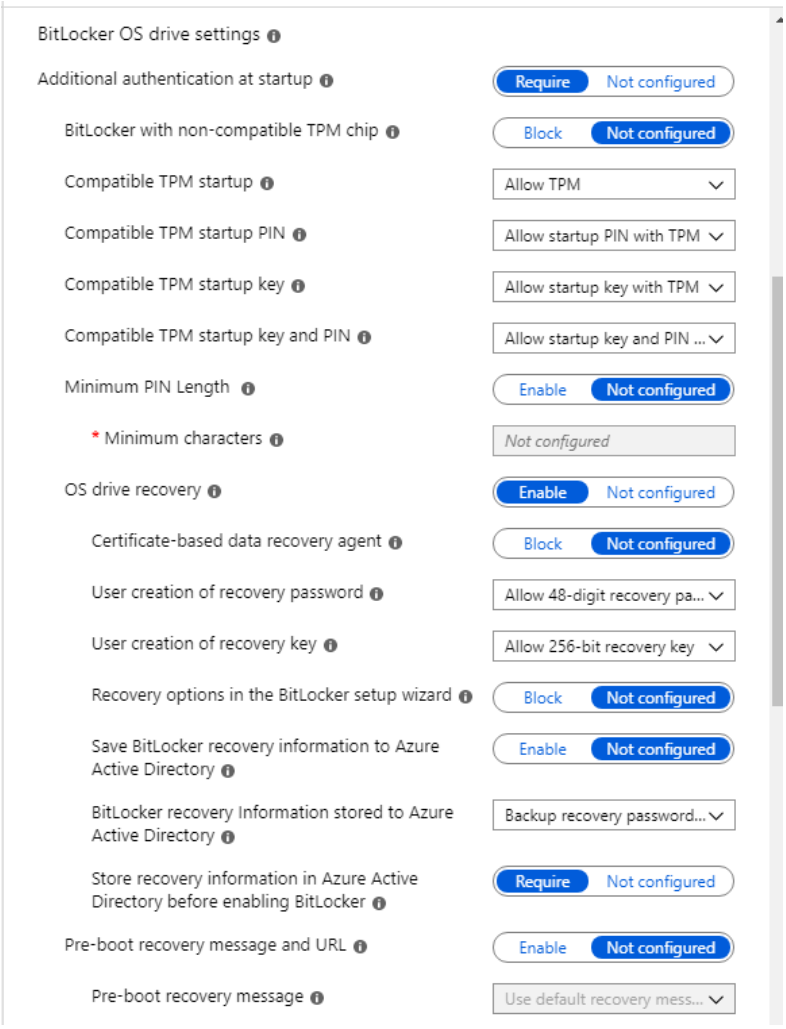


Windows Encryption (BitLocker)

Profile type: **Endpoint protection**. **Settings > Windows Encryption**. Pick **Require** for *Encrypt devices*.

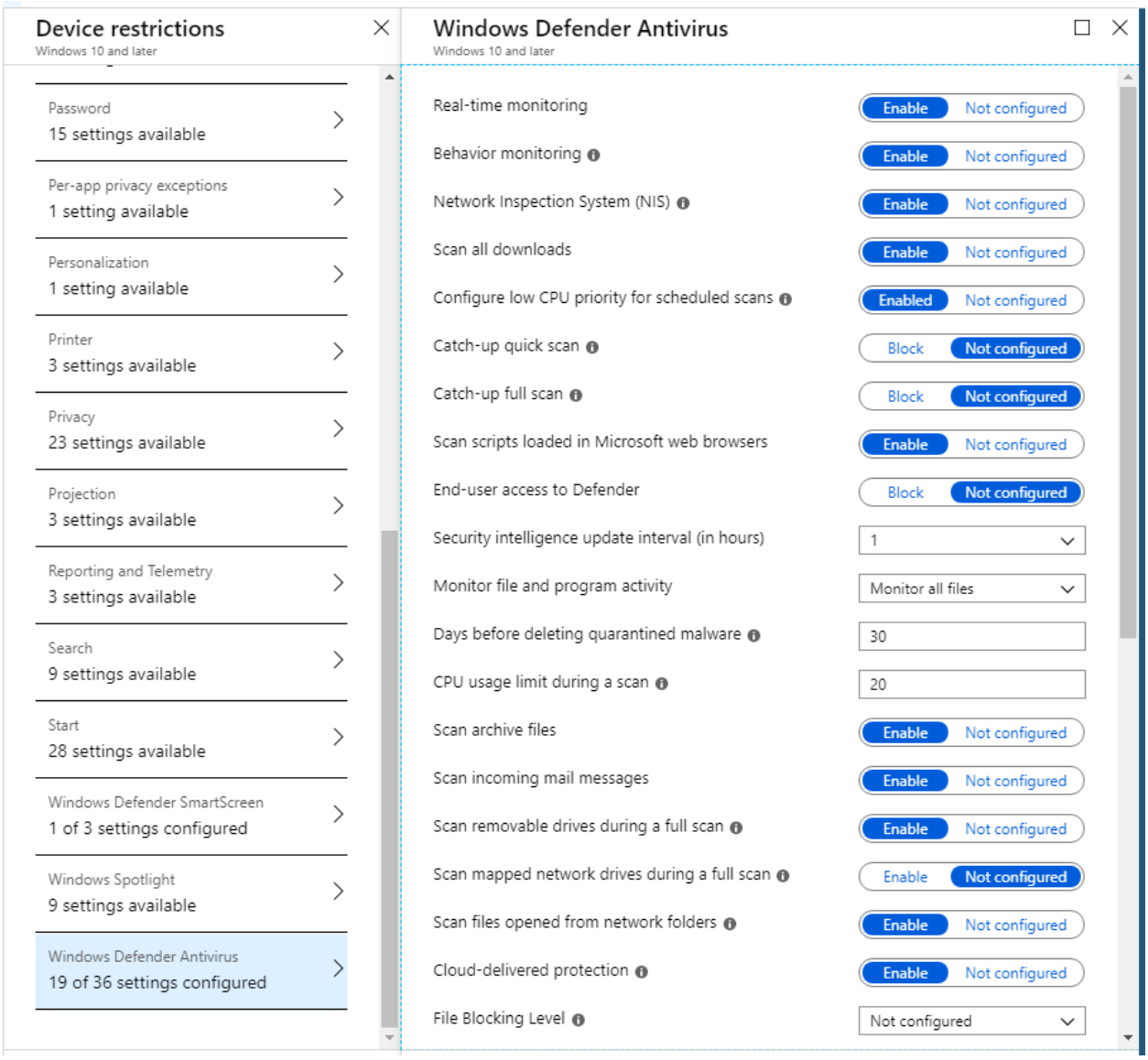


Configure at least the OS drive settings (removable, etc. optional/depends on the environment).

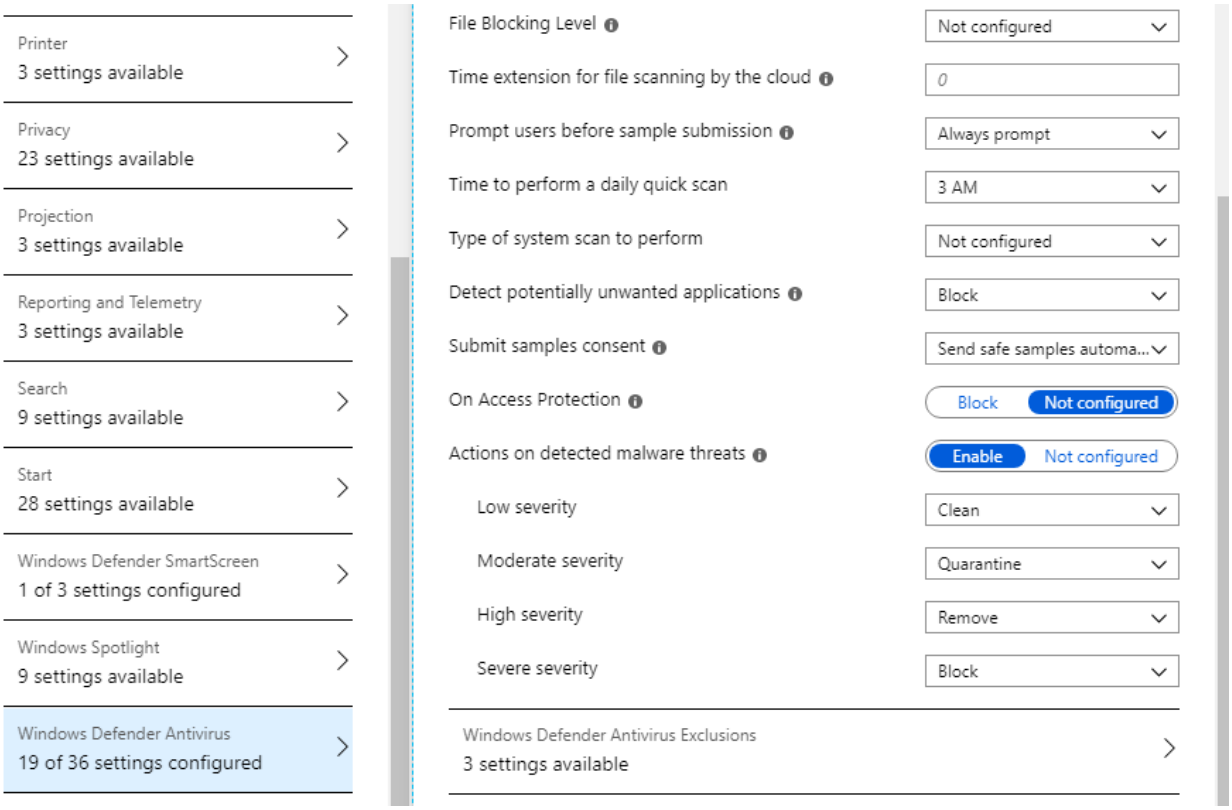


Windows Defender Antivirus

Profile type: **Device restrictions**. Pick **Settings > Windows Defender Antivirus**. Refer to baseline depicted below for guidance. Be more careful with your selections or forego this profile if using a third-party for Antivirus/Antimalware/Antispyware/etc.



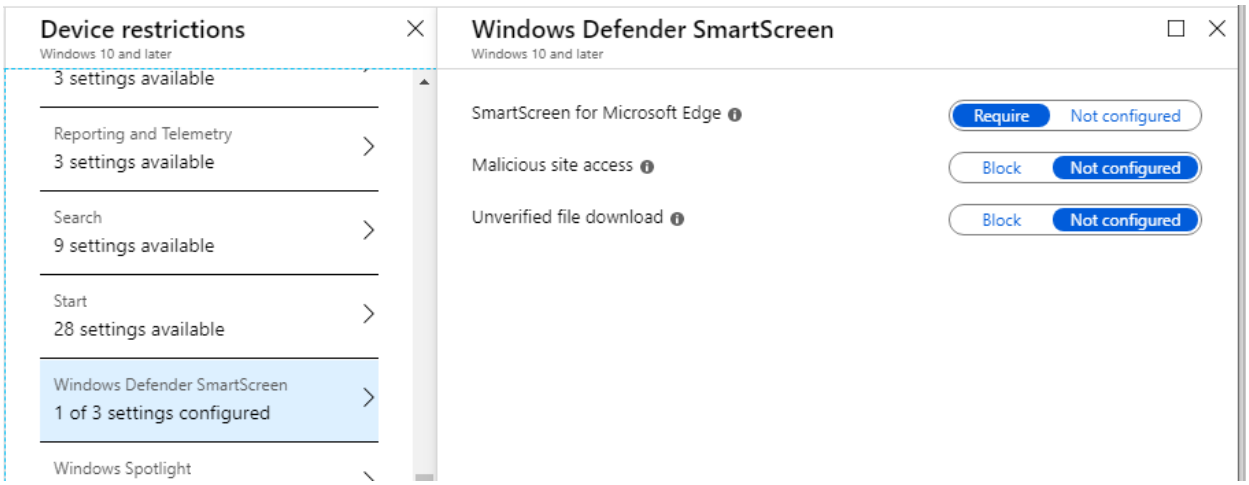
Continued...



As with everything, you are ultimately responsible for your own configuration here, and should know what exclusions you need to make in your environment, if any.

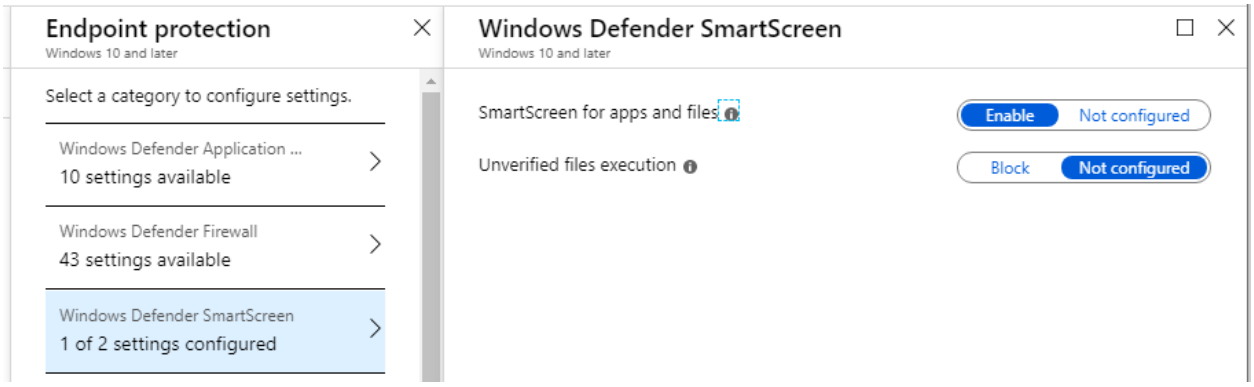
Windows Defender SmartScreen (Edge)

Profile type: **Device restrictions**. Pick **Windows Defender SmartScreen**. Note: This only protects browsing in Microsoft Edge (not Firefox, Chrome, etc.)



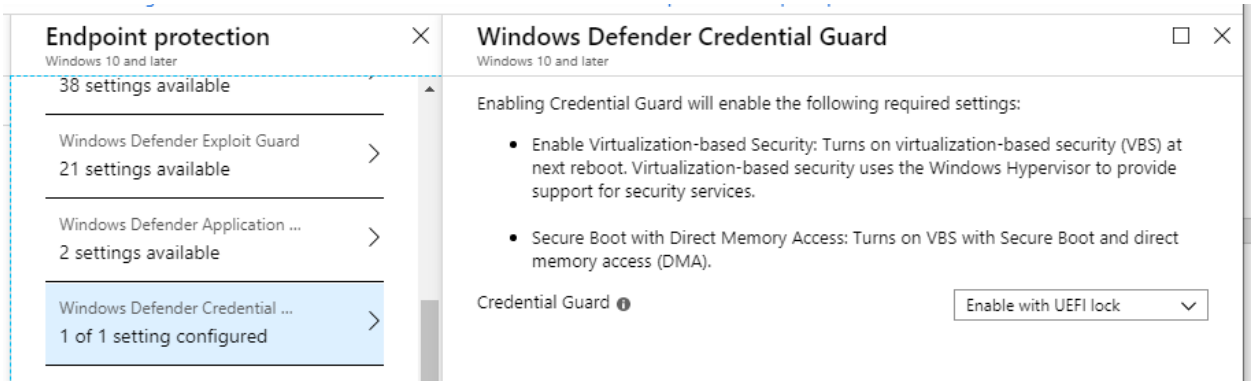
Windows Defender SmartScreen (Files & Apps)

Profile type: **Endpoint protection**. Pick **Windows Defender SmartScreen**.



Windows Defender Credential Guard

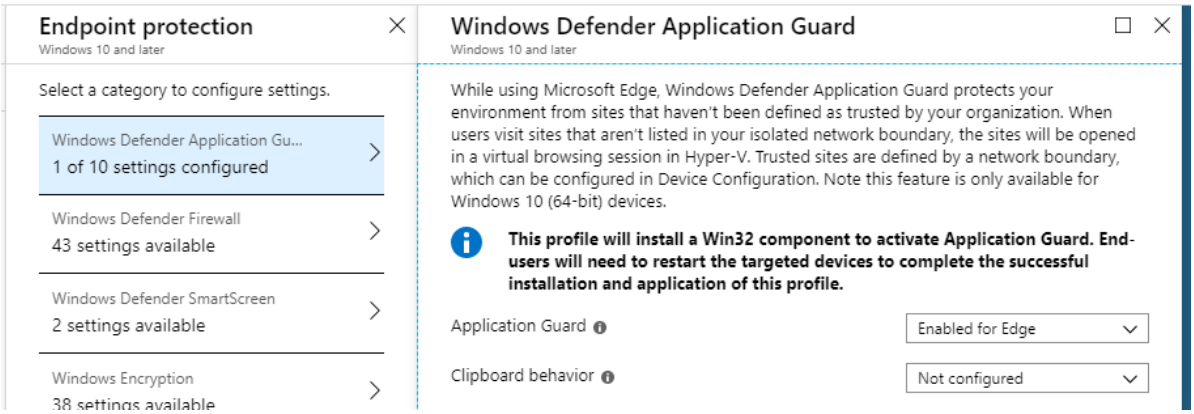
Highly recommended if your endpoints support this feature and virtualization-enabled security. Profile type: **Endpoint protection**. Pick **Windows Defender Credential Guard**.



Recommended setting: **Enable with UEFI lock**.

Windows Defender Application Guard

Profile type: **Endpoint protection**. Pick **Windows Defender Application Guard > Enable**. Review supporting settings at your own discretion.

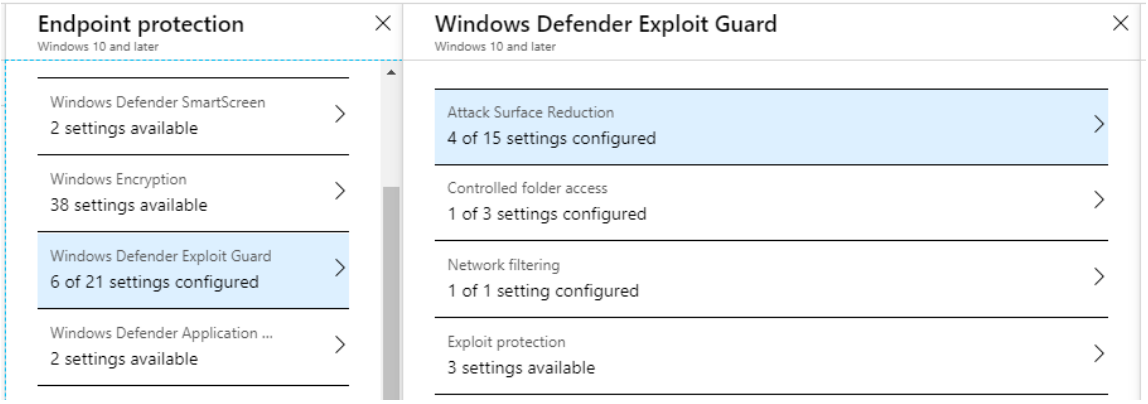


Note: Application Guard only protects browsing in Edge (not Chrome, Firefox, etc.). Will cause workstations to reboot in order to configure the virtualization.

Windows Defender Exploit Guard

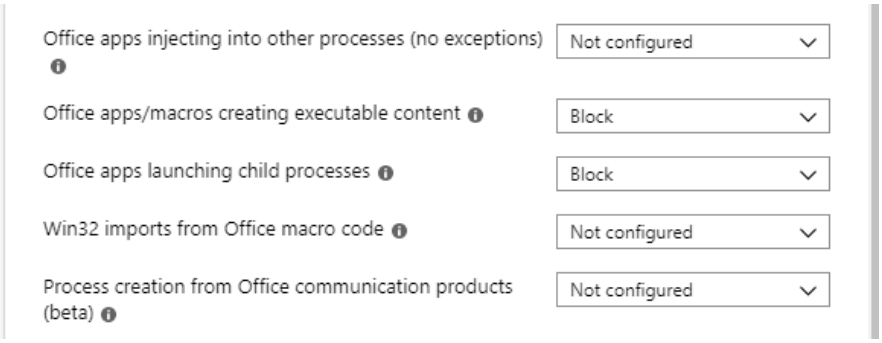
Profile type: **Endpoint protection**. Pick **Windows Defender Exploit Guard**. Here again, pay attention to which features are supported (and not supported) for your version of Windows.

Note: Windows Defender Antivirus must be enabled in order for these features to work.

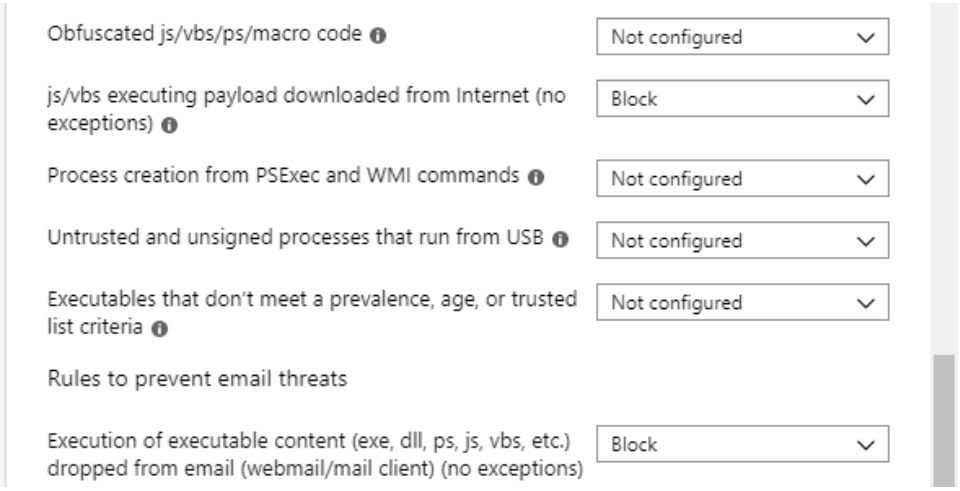


Attack Surface Reduction

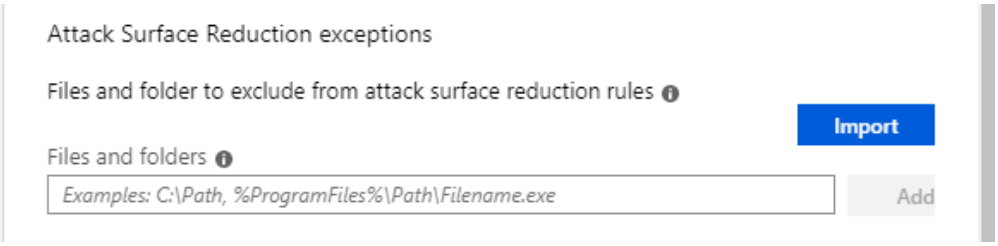
Contains a few gems that you should consider as a baseline/starting point, for example **Rules to prevent Office Macro threats**:



And **Rules to prevent script threats**:

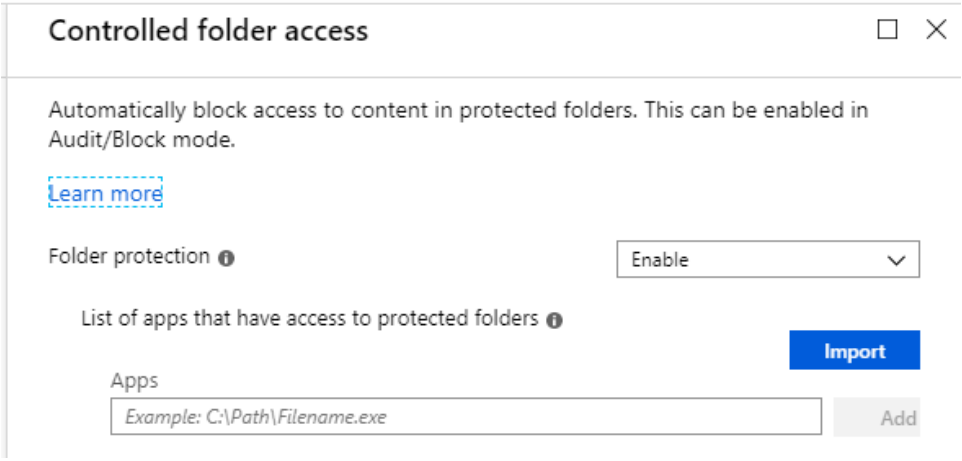


You can also define **exceptions** to enable certain content in specified files/folders:

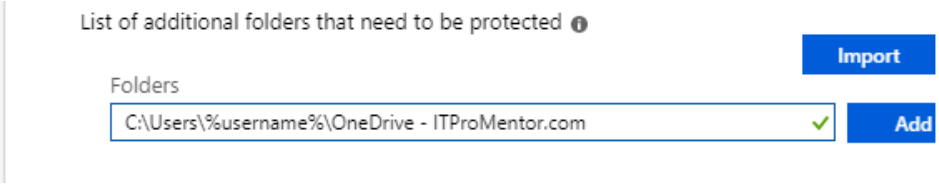


Controlled folder access

Prevents potentially malicious software from making changes to protected folders. This can have end-user impacts as some apps need to make changes. Allow apps as needed.

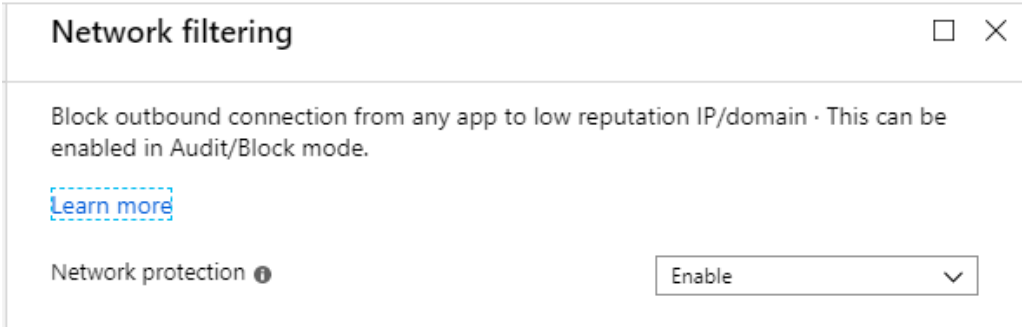


You can also choose to protect other folders, like OneDrive.



Network filtering

Highly recommended. Also protects browsing in third-party web browsers.



Exploit protection

Not recommended for typical baseline configuration.