

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

Guide to The Intune Best Practices Checklist	1
<input type="checkbox"/> Create security groups for Intune deployment rings.....	2
<input type="checkbox"/> Configure Windows 10 Software Update Rings.....	3
<input type="checkbox"/> Setup Office 365 app deployments for Windows 10.....	5
<input type="checkbox"/> Setup App protection policies (MAM)	8
<input type="checkbox"/> Create the Company terms and conditions	12
<input type="checkbox"/> Customize Company Portal Branding	13
<input type="checkbox"/> Configure Device cleanup rules	13
<input type="checkbox"/> Configure Device enrollment restrictions	15
<input type="checkbox"/> Configure Windows 10 automatic enrollment.....	16
<input type="checkbox"/> Configure Windows Hello for Business	17
<input type="checkbox"/> Configure Apple MDM push certificate	18
<input type="checkbox"/> Configure the default Compliance policy settings	19
<input type="checkbox"/> Configure Device Compliance policies	20
<input type="checkbox"/> Enroll devices	25
Windows 10 Enrollment options	26
<input type="checkbox"/> Verify compliance status of enrolled devices	29
<input type="checkbox"/> Enable Conditional access.....	31
<input type="checkbox"/> Setup Device Configuration profiles	32
Control the OneDrive for Business experience.....	32
Map shared document libraries automatically.....	36
Windows 10 Device restrictions & Endpoint protection settings.....	38

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.

The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a sidebar with various service icons like Dashboard, All services, Device compliance, Device enrollment, Client apps, Device configuration, Devices, Software updates, Conditional Access, Users, Groups, and Roles. The 'Groups' icon is highlighted. The main area is titled 'Groups - All groups' and shows a list of existing groups: Intune-Android-Pilot, Intune-iOS-Pilot, Intune-MacOS-Pilot, Intune-MAM-Pilot, Intune-MDM-Pilot, and Intune-Win10-Pilot. A 'New group' button is visible. In the center, there's a form to create a new group, with 'Name' set to 'Intune'. The 'GROUP TYPE' column for all groups listed is 'Security'.

NAME	GROUP TYPE
IN Intune-Android-Pilot	Security
IN Intune-iOS-Pilot	Security
IN Intune-MacOS-Pilot	Security
IN Intune-MAM-Pilot	Security
IN Intune-MDM-Pilot	Security
IN Intune-Win10-Pilot	Security

Configure Windows 10 Software Update Rings

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

The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a navigation sidebar with options like Dashboard, All services, Favorites (Device compliance, Device enrollment, Client apps, Device configuration, Devices, Software updates), Overview, Manage, and Monitor. The 'Software updates' option is highlighted. In the center, the title is 'Software updates - Windows 10 Update Rings'. Below it, there's a search bar, a 'Create' button, and filter options. A table is shown with columns for NAME, FEATURE DEFERRAL, and QL. A message says 'There are no Windows 10 Update Rings to show.'

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

The screenshot shows the 'Create Update Ring' dialog. On the left, there's a form with fields for Name (Win10-Pilot ring), Description (Enter a description...), Settings (Configure), and Scope (Tags) (0 scope(s) selected). On the right, there's a 'Settings' tab for Windows 10 and later. It includes sections for Update settings, Servicing channel (Semi-Annual Channel (Targeted)), and various policy options like Microsoft product updates (Allow/Block), Windows drivers (Allow/Block), Quality update deferral period (0 days), Feature update deferral period (0 days), and Set feature update uninstall period (10 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

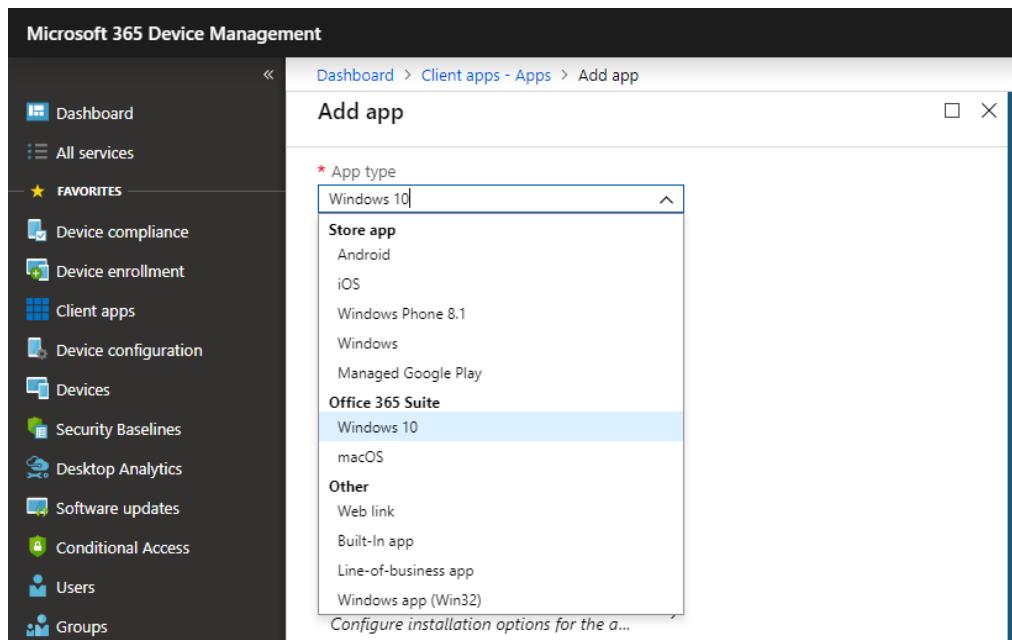
The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a sidebar with various navigation options like Dashboard, All services, Favorites, Device compliance, Device enrollment, Client apps, Device configuration, Devices, Software updates, and Conditional Access. Under 'Software updates', the 'Windows 10 Update Rings' option is selected. In the main content area, the title is 'Broad ring - Assignments'. Below it, there are tabs for Overview, Manage, Properties, and Assignments (which is highlighted with a red box). There are also buttons for Save, Discard, and Evaluate. A note says: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.' A 'Select groups to exclude' field contains 'Intune-Sensitive'.

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

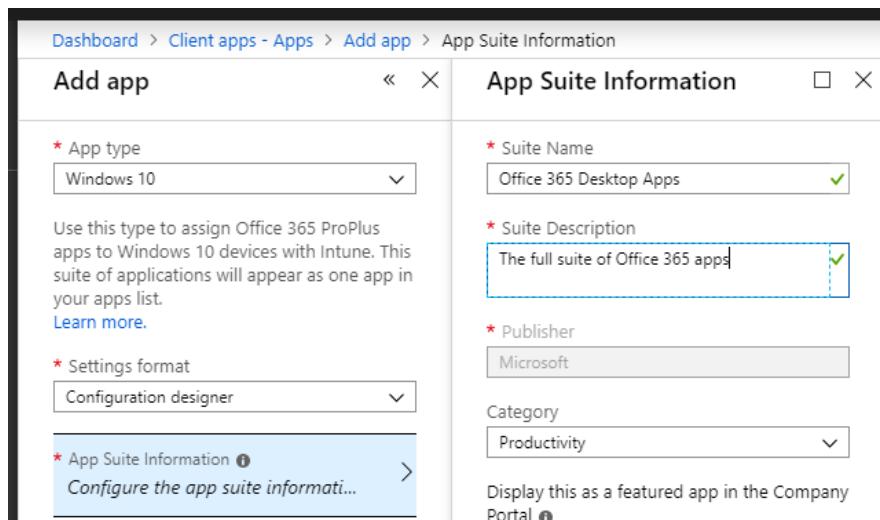
It is possible to push software packages to managed devices via Intune. Setup a policy that will automatically install the Office 365 desktop applications to newly enrolled devices.

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



The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a navigation sidebar with various options like Dashboard, All services, Favorites (Device compliance, Device enrollment, Client apps, etc.), Security Baselines, Desktop Analytics, Software updates, Conditional Access, Users, and Groups. The main area is titled 'Add app' and has a sub-header 'Dashboard > Client apps - Apps > Add app'. A dropdown menu for 'App type' is open, showing 'Windows 10' selected. Below it, other options include Store app, Android, iOS, Windows Phone 8.1, Windows, Managed Google Play, and 'Office 365 Suite'. Under 'Office 365 Suite', 'Windows 10' is also selected. Other categories listed are macOS and Other (Web link, Built-In app, Line-of-business app, Windows app (Win32)). At the bottom of the dropdown, there's a link 'Configure installation options for the a...'. The overall interface is clean and modern, typical of Microsoft's product design.

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



The screenshot shows the 'App Suite Information' blade of the 'Add app' process. On the left, under 'Add app', there's a 'Settings format' dropdown set to 'Configuration designer'. Below it, there's a link 'App Suite Information' with a note 'Configure the app suite informati...' and a right-pointing arrow. On the right, the 'App Suite Information' blade has several fields: 'Suite Name' (set to 'Office 365 Desktop Apps'), 'Suite Description' (set to 'The full suite of Office 365 apps'), 'Publisher' (set to 'Microsoft'), and 'Category' (set to 'Productivity'). There's also a note at the bottom right: 'Display this as a featured app in the Company Portal'. The interface is consistent with the previous screenshot, maintaining the same clean design and color scheme.

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 screenshot shows two blades side-by-side. The left blade is titled 'Add app' and includes sections for 'App type' (set to 'Windows 10'), 'Settings format' (set to 'Configuration designer'), 'App Suite Information' (with a note that it's being configured), 'Configure App Suite' (selected, showing a list of Office 365 apps to be assigned), and 'App Suite Settings' (with a note about configuring installation options). The right blade is titled 'Configure App Suite' and lists the following checked apps: Access, Excel, OneDrive Desktop, OneNote 2016, Outlook, PowerPoint, Publisher, Skype for Business, Teams, and Word. Below this is a section for 'Additional Office apps' with two unchecked options: Project Online Desktop Client and Visio Online Plan 2.

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

The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a sidebar with various service icons. The main area has a breadcrumb navigation path: Dashboard > Client apps - Apps > Add app > App Suite Settings. The central panel is titled "Add app" and shows a dropdown for "App type" set to "Windows 10". Below it, there's a note about assigning Office 365 ProPlus apps to Windows 10 devices via Intune. The right panel is titled "App Suite Settings" and contains several configuration options:

- Architecture:** Set to 64-bit.
- Update channel:** Set to Monthly.
- Specific version:** Set to Latest version.
- Remove other versions of Office (MSI) from end user devices:** Set to Yes.
- Automatically accept the app end user license agreement:** Set to Yes.
- Use shared computer activation:** Set to No.
- Languages:** An option to manage OS Languages.

 A note at the bottom of the right panel states: "Microsoft has changed the behavior for sending service and diagnostic data from Office. Review these changes to ensure the".

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**.

The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a sidebar with 'FAVORITES' containing 'Device enrollment', 'Device compliance', 'Device configuration', 'Devices', and 'Client apps'. The 'Client apps' item is highlighted with a red box. The main area is titled 'Client apps - App protection policies' and shows a table of policies:

POLICY	DEPLOY...	PLATFORM
Application policy for Android	Yes	Android
Application policy for iOS	Yes	iOS
Application policy for Windows 10	Yes	Windows 10

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

The screenshot shows the Microsoft 365 Admin center. On the left, the navigation menu has 'Devices' expanded, with 'Policies' selected and highlighted with a red box. The main area is titled 'Policies' and shows a list of policies:

Name	Policy type
Device policy for Windows 10	Windows 10 device configuration
Application policy for Android	Application management for Android
Application policy for iOS	Application management for iOS
Application policy for Windows 10	Application management on Windows 10

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.).

The screenshot shows the 'Create policy' interface. On the left, there's a form with fields for Name (set to 'Android app protection'), Platform (set to 'Android'), and Target to all app types (set to 'Yes'). Below these is a section labeled 'Apps' with a button 'Select required apps'. On the right, a list of apps is shown, each with a checkbox and a platform indicator (Android). Most apps have their checkboxes checked.

App	Platform
Microsoft Stream	Android
Microsoft Teams	Android
Microsoft To-Do	Android
Nine Work for Intune	Android
OneDrive	Android
OneNote	Android
Outlook	Android
PowerPoint	Android
PrinterOn for Microsoft	Android

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:

The screenshot shows the 'Data protection' settings page for an 'Android MAM Policy'. It includes sections for Data Transfer, Screen capture, and Google Assistant. Under Data Transfer, there are several settings with dropdown menus and buttons like 'Allow', 'Block', and 'Select'. For example, 'Backup Org data to Android backup services' has 'Block' selected. 'Send Org data to other apps' has 'Policy managed apps' selected with a 'Select' button. 'Receive data from other apps' also has 'Policy managed apps' selected. 'Save copies of Org data' has 'Block' selected. 'Restrict cut, copy and paste between other apps' has 'Policy managed apps with paste in' selected. 'Screen capture and Google Assistant' has 'Enable' selected.

Data protection > Encryption and Functionality settings:

Encryption		
Encrypt Org data ⓘ	Require	Not required
Encrypt Org data on enrolled devices ⓘ	Require	Not required
Functionality		
Sync app with native contacts app ⓘ	Enable	Disable
Printing Org data ⓘ	Enable	Disable
Restrict web content transfer with other apps ⓘ	Any app	▼

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

Access requirements		
Android MAM Policy		
<input type="checkbox"/> Save	<input type="checkbox"/> Discard	×
PIN for access ⓘ	Require	Not required
PIN type ⓘ	Numeric	Passcode
Simple PIN ⓘ	Allow	Block
Select minimum PIN length ⓘ	4	▼
Fingerprint instead of PIN for access (Android 6.0+) ⓘ	Allow	Block
Override fingerprint with PIN after timeout ⓘ	Require	Not required
Timeout (minutes of inactivity)		
PIN reset after number of days ⓘ	Yes	No
Number of days	0	
App PIN when device PIN is set ⓘ	Enable	Disable
Work or school account credentials for access ⓘ	Require	Not required
Recheck the access requirements after (minutes of inactivity) ⓘ	0	

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

The screenshot shows the 'Conditional launch' configuration page for an 'Android MAM Policy'. At the top, there are 'Save' and 'Discard' buttons. A note below explains how to set sign-in security requirements, mentioning 'Setting', 'Value', and 'Action'. The 'App conditions' section lists three entries:

SETTING	VALUE	ACTION	⋮
Max PIN attempts	10	Reset PIN	⋮
Offline grace period	720	Block access (minutes)	⋮
Offline grace period	90	Wipe data (days)	⋮

A dropdown menu at the bottom of this section says 'Select one'. Below this is a 'Device conditions' section with a single entry:

SETTING	VALUE	ACTION	⋮
Jailbroken/rooted devices		Block access	⋮

A dropdown menu at the bottom of this section says 'Select one'.

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

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**.

The screenshot shows the 'Create terms and conditions' page. At the top, there's a breadcrumb navigation: Dashboard > Device enrollment - Terms and conditions > Create terms and conditions. Below the breadcrumb, the title 'Create terms and conditions' is displayed. A horizontal navigation bar shows four steps: Basics (done), Terms (selected), Assignments, and Review + create. The 'Terms' step is highlighted with a blue underline and a green checkmark icon. The main content area has three sections:

- Title:** COMPANY Terms and Conditions (with a green checkmark icon)
- Terms and conditions:** By enrolling your device, you agree to COMPANY terms and conditions. (with a green checkmark icon)
- Summary of 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. (with a green checkmark icon)

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.

Customize Company Portal Branding

As I have mentioned in other places, they have 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.

Configure Device cleanup rules

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:

The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a navigation sidebar with various options like Dashboard, All services, Favorites, Device compliance, Device enrollment, Client apps, Device configuration, Devices, Software updates, Conditional Access, Users, Groups, Roles, and Troubleshoot. The 'Devices' option is selected. The main content area is titled 'Devices - Device cleanup rules' and includes a search bar, 'Save' and 'Discard' buttons, and a note about setting cleanup rules to delete inactive, stale, or unresponsive devices. It shows two configuration sections: 'Delete devices based on last check-in date' set to 'Yes' and 'Delete devices that haven't checked in for this many days' set to '90'. A warning message states that after saving, devices inactive for 90 days will be deleted, and reports may take up to 48 hours to refresh. There's also a link to 'View affected devices'.

- 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 Device enrollment restrictions

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

The screenshot shows the Microsoft Intune Device enrollment - Enrollment restrictions page. The left sidebar has a navigation menu with links for Overview, Quick start, Manage (Apple enrollment, Android enrollment, Windows enrollment, Terms and conditions, Enrollment restrictions, Device categories, Corporate device identifiers, Device enrollment managers), and Monitor. The main content area has two sections: 'Device Type Restrictions' and 'Device Limit Restrictions'. The 'Device Type Restrictions' section contains a table with one row: Priority: Default, Name: All Users, Assigned: Yes. The 'Device Limit Restrictions' section contains a table with one row: Priority: Default, Name: All Users, Device Limit: 5, Assigned: Yes.

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:

The screenshot shows a 'Select platforms' dialog box. It has a header 'Select platforms' and a note: 'You can allow enrollment of the following platforms. Only block platforms you will not support. Allowed platforms can be configured with additional enrollment restrictions.' Below is a list of platforms with 'Allow' and 'Block' buttons: Android (Allow is blue), Android work profile (Allow is blue), iOS (Allow is blue), macOS (Allow is blue), Windows (MDM) (Allow is blue), and Windows Mobile (Allow is blue). On the left, there's a form with fields for Name (All Users), Description (This is the default Device Type Restriction applied with lowest priority to all users regardless of group membership), and Restriction type (Device Type Restriction). At the bottom, it says 'Select platforms' and '4 platforms selected'.

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.

The screenshot shows the Microsoft Intune interface for Device enrollment - Windows enrollment. On the left, there's a sidebar with a search bar, 'Overview', 'Quick start', 'Manage' (selected), 'Apple enrollment', 'Android enrollment', 'Windows enrollment' (selected), and 'Terms and conditions'. The main content area has a heading 'Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. [Learn More.](#)' Below this is a 'General' section with two items: 'Automatic Enrollment' (with a gear icon) and 'Windows Hello for Business' (with a smiley face icon). Both items have descriptive text and links to learn more.

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

The screenshot shows the Microsoft 365 Device Management interface under 'Configure'. The left sidebar includes 'Dashboard', 'All services', 'FAVORITES' (with 'Device compliance' selected), 'Device enrollment' (selected), 'Client apps', 'Device configuration', 'Devices', 'Software updates', 'Conditional Access', and 'Users'. The main content area shows the 'Configure' page for Windows enrollment. It has sections for 'MDM user scope' (set to 'All'), 'MDM terms of use URL' (set to https://portal.manage.microsoft.com/TermsofUse.aspx), 'MDM discovery URL' (set to https://enrollment.manage.microsoft.com/enrollmentserver/disco...), 'MDM compliance URL' (set to https://portal.manage.microsoft.com/?portalAction=Compliance), 'Restore default MDM URLs', 'MAM User scope' (set to 'All'), and 'MAM Terms of use URL' (empty).

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:

The screenshot shows the Windows Hello configuration interface. On the left, there's a sidebar with a 'Settings' section where 'Enabled' is selected. The main area has a 'Save' and 'Discard' button at the top. It lists various configuration options for Windows Hello:

Setting	Value	Status
Configure Windows Hello for Business:	Enabled	Enabled
Use a Trusted Platform Module (TPM):	Required	Preferred
Minimum PIN length:	6	Valid
Maximum PIN length:	127	Valid
Lowercase letters in PIN:	Not allowed	Valid
Uppercase letters in PIN:	Not allowed	Valid
Special characters in PIN:	Not allowed	Valid
PIN expiration (days):	Never	Valid
Remember PIN history:	No	Valid
Allow biometric authentication:	Yes	Enabled
Use enhanced anti-spoofing, when available:	Yes	Valid
Allow phone sign-in:	Yes	Enabled
Use security keys for sign-in:	Not configured	Valid

Configure Apple MDM push certificate

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

The screenshot shows the Microsoft 365 Device Management portal. On the left sidebar, under 'FAVORITES', 'Device enrollment' is highlighted with a red box. In the main content area, 'Device enrollment - Apple enrollment' is selected. Under 'Manage', 'Apple enrollment' is highlighted with a red box. A red arrow points from the 'Apple MDM Push certificate' section in the 'Prerequisites' section to the 'Apple enrollment' link in the 'Manage' section. The 'Apple MDM Push certificate' section contains the text: 'Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. [Learn More.](#)'

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](#).

The screenshot shows the Apple Push Certificates Portal. At the top, there's a navigation bar with links for Store, Mac, iPod, iPhone, iPad, iTunes, Support, and a search icon. The main title is 'Apple Push Certificates Portal'. On the right, there's a sign-in message 'alex@itpromentor.com Sign out'. Below the title, a 'Confirmation' section shows a green checkmark icon. It says: 'You have successfully created a new push certificate with the following information:' followed by a table of details. To the right is a graphic of a globe with concentric circles around it, representing global reach. At the bottom, there are 'Manage Certificates' and 'Download' buttons.

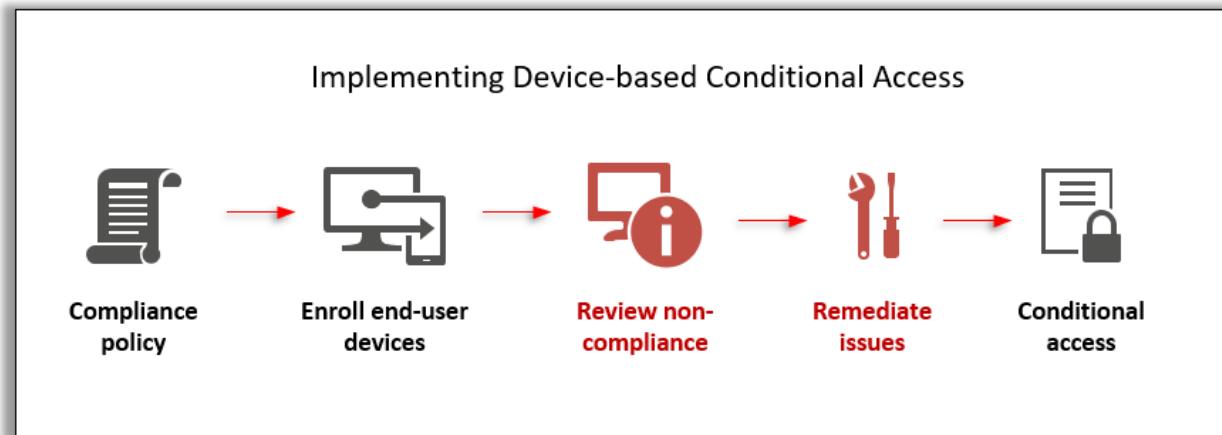
Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Aug 15, 2019

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 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:

The screenshot shows the 'Device compliance - Compliance policy settings' page in the Microsoft Intune portal. The left sidebar lists various compliance-related features: Windows health attestation r..., Threat agent status, Setup (selected), Compliance policy settings (highlighted in blue), Microsoft Defender ATP, Mobile Threat Defense, and Partner device management. The main content area displays configuration options for 'Compliance policy settings':

- Mark devices with no compliance policy assigned as:** A toggle switch is set to **Not Compliant**.
- Enhanced jailbreak detection:** A toggle switch is set to **Enabled**.
- Compliance status validity period (days):** A dropdown menu shows the value **15**.

- 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**.

The screenshot shows the Microsoft Intune interface for managing device compliance policies. On the left, there's a sidebar with 'Overview', 'Quick start', 'Manage' (which is expanded), 'Device enrollment', 'Device compliance' (which is selected and highlighted with a red box), 'Device configuration', and 'Devices'. The main content area is titled 'Device compliance - Policies'. It has a search bar, a 'Create Policy' button (also highlighted with a red box), and a 'Manage' section with tabs for 'Policies' (selected and highlighted with a red box), 'Notifications', and 'Locations'. Below the manage section is a 'Monitor' tab and a 'Device compliance' section.

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:

The screenshot shows the 'Windows 10 compliance policy' settings page. On the left, there's a sidebar with categories: 'Device Health' (3 settings available), 'Device Properties' (5 settings available), 'Configuration Manager Compliance' (1 setting available), 'System Security' (8 of 17 settings configured, selected and highlighted with a red box), and 'Microsoft Defender ATP' (1 setting available). The main content area is titled 'System Security' and contains several configuration items:

Setting	Value	Status
Require a password to unlock mobile devices	Not configured	Require (blue button)
Simple passwords	Not configured	Block (blue button)
Password type	Device default	(dropdown menu)
Minimum password length	4	(text input)
Maximum minutes of inactivity before password is required	5 Minutes	(dropdown menu)
Password expiration (days)	41	(text input)
Number of previous passwords to prevent reuse	5	(text input)
Require password when device returns from idle state (Mobile and Holographic)	Not configured	Require (blue button)

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

The screenshot shows the 'Windows 10 compliance policy' settings for 'System Security'. On the left, a sidebar lists categories: Device Health (3 settings available), Device Properties (5 settings available), Configuration Manager Compliance (1 setting available), System Security (4 of 17 settings configured, highlighted in blue), and Microsoft Defender ATP (1 setting available). The main pane displays 'Encryption' settings, which include 'Encryption of data storage on device' with a 'Require' status and a 'Not configured' link. Other sections like 'Device Security', 'Firewall', 'Trusted Platform Module (TPM)', 'Antivirus', 'Antispyware', and 'Defender' are also listed with their respective requirements.

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**

The screenshot shows the 'Mac compliance policy' settings for 'Device Health'. The sidebar shows 'Device Health' with 1 of 1 setting configured. The main pane displays a single setting: 'Require system integrity protection' with a 'Require' status and a 'Not configured' link.

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

System Security

macOS

Password

Require a password to unlock devices. ⓘ

Require Not configured

Simple passwords ⓘ

Block Not configured

Minimum password length ⓘ

Not configured ✓

Password type ⓘ

Device default ▾

Number of non-alphanumeric characters in password ⓘ

Not configured ▾

Maximum minutes of inactivity before password is required ⓘ

5 Minutes ▾

Password expiration (days) ⓘ

41

Number of previous passwords to prevent reuse ⓘ

5

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

Encryption

Encryption of data storage on device. ⓘ

Require Not configured

Device Security

Firewall ⓘ

Enable Not configured

Incoming connections ⓘ

Block Not configured

Stealth Mode ⓘ

Enable Not configured

Gatekeeper

Allow apps downloaded from these locations ⓘ

Not configured ▾

OK

iOS Compliance policy

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

The screenshot shows the 'iOS compliance policy' interface. On the left, under 'Device Health', there is a setting for 'Jailbroken devices' which is configured to 'Block'. The status bar at the top right indicates 'Block'.

iOS compliance policy		Device Health
ios		ios
Select a category to configure settings.		
Email	>	Jailbroken devices
1 setting available		<input checked="" type="button"/> Block <input type="button"/> Not configured
Device Health	>	Require the device to be at or under the Device Threat Level
1 of 2 settings configured		<input type="button"/> Not configured

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).

The screenshot shows the 'iOS compliance policy' interface. Under 'System Security', several settings are configured:

- 'Require a password to unlock mobile devices' is set to 'Require'.
- 'Simple passwords' is set to 'Block'.
- 'Minimum password length' is set to 4.
- 'Required password type' is set to 'Numeric'.
- 'Number of non-alphanumeric characters in password' is set to 'Not configured'.
- 'Maximum minutes after screen lock before password is required' is set to 'Immediately'.
- 'Maximum minutes of inactivity until screen locks' is set to 'Not configured'.
- 'Password expiration (days)' is set to 41.
- 'Number of previous passwords to prevent reuse' is set to 5.

iOS compliance policy		System Security
ios		ios
Select a category to configure settings.		
Email	>	Require a password to unlock mobile devices
1 setting available		<input checked="" type="button"/> Require <input type="button"/> Not configured
Device Health	>	Simple passwords
1 of 2 settings configured		<input checked="" type="button"/> Block <input type="button"/> Not configured
Device Properties	>	Minimum password length
4 settings available		4
System Security	>	Required password type
5 of 10 settings configured		Numeric
		Number of non-alphanumeric characters in password
		Not configured
		Maximum minutes after screen lock before password is required
		Immediately
		Maximum minutes of inactivity until screen locks
		Not configured
		Password expiration (days)
		41
		Number of previous passwords to prevent reuse
		5

[Android Compliance policy](#)

Recommended configuration settings:

The screenshot shows two tabs: 'Android compliance policy' and 'Device Health'. The 'Device Health' tab is active, displaying configuration options for rooted devices, Google Play Protect, and System Security.

Category	Setting	Action	Status
Device Health	Rooted devices	Block	Not configured
	Require the device to be at or under the Device Threat Level	Not configured	▼
	Google Play Protect	Require	Not configured
System Security	Up-to-date security provider	Require	Not configured
	Threat scan on apps	Require	Not configured
	SafetyNet device attestation	Not configured	▼

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**:

The screenshot shows the 'System Security' tab under the 'Android compliance policy' interface. It includes settings for password requirements, inactivity, password expiration, and previous password reuse.

Setting	Action	Status
Require a password to unlock mobile devices	Require	Not configured
Required password type	At least numeric	▼
Minimum password length	4	
Maximum minutes of inactivity before password is required	Not configured	▼
Number of days until password expires	Enter number of days (1-365)	
Number of previous passwords to prevent reuse	Enter a number (1-24)	

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

Encryption

Encryption of data storage on device. [i](#)

Require

Not configured

Device Security

Block apps from unknown sources [i](#)

Block

Not configured

Company Portal app runtime integrity [i](#)

Require

Not configured

Block USB debugging on device [i](#)

Block

Not configured

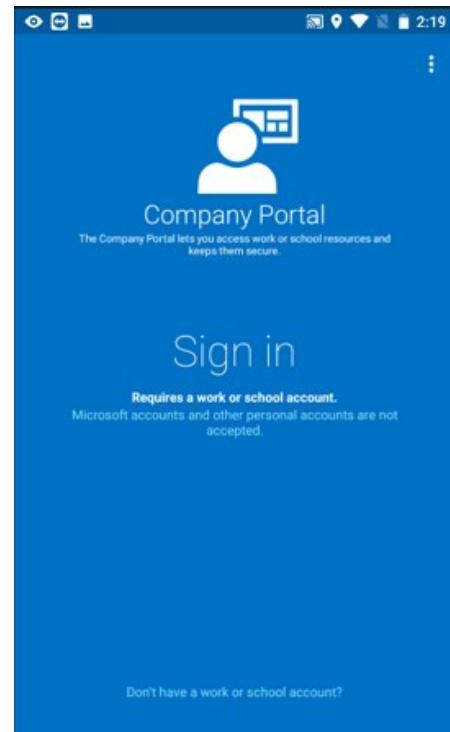
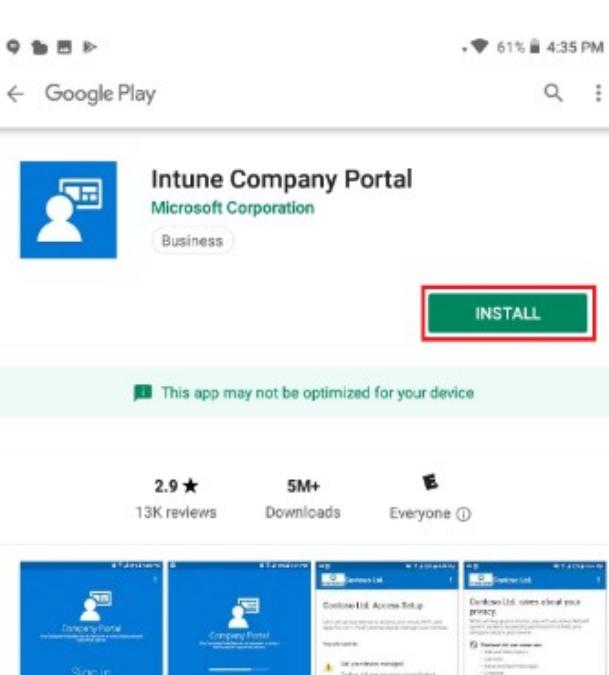
Minimum security patch level [i](#)

Not configured

Require for both Encryption and Company Portal app runtime integrity.

Enroll devices

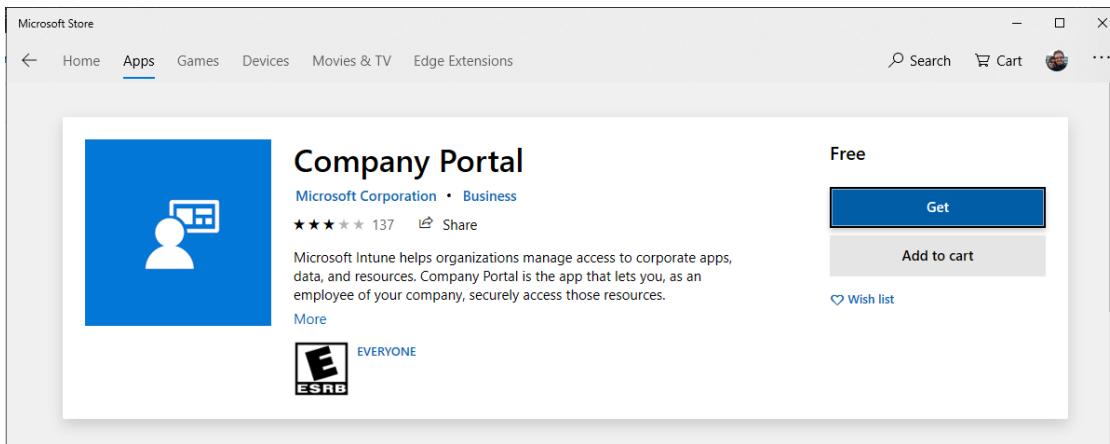
The most common method for enrolling devices (of all types) is the Company Portal app. Simply go the app store on your device of choice and search for Company Portal app. Once you have the app installed, sign into the app using your Microsoft/Office 365 credentials to complete enrollment steps.



I will not step 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.

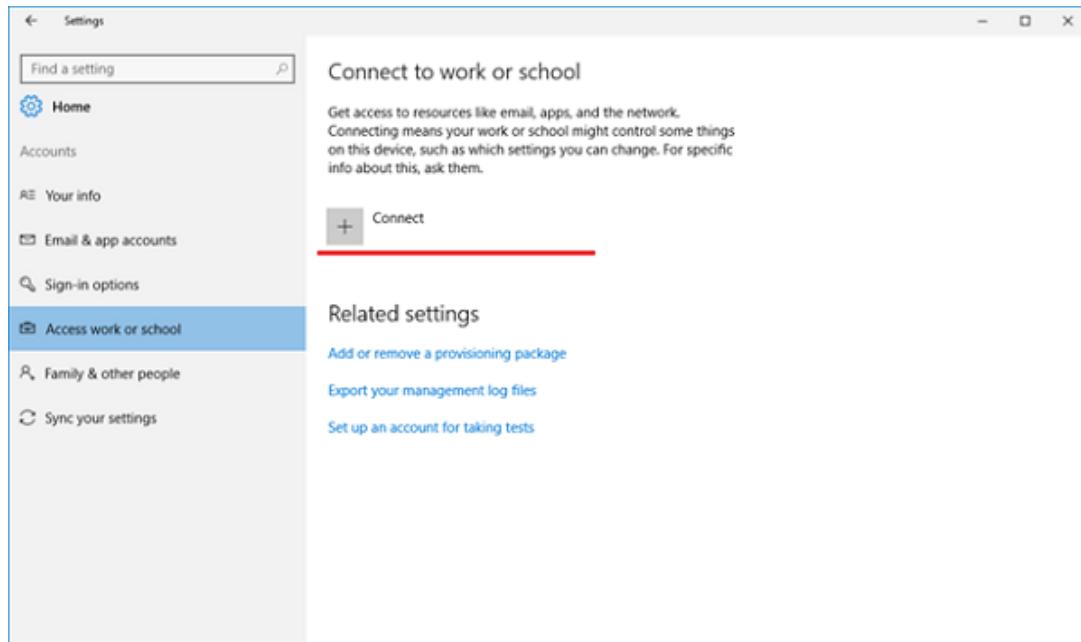
Windows 10 Enrollment options

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:

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Email address

Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

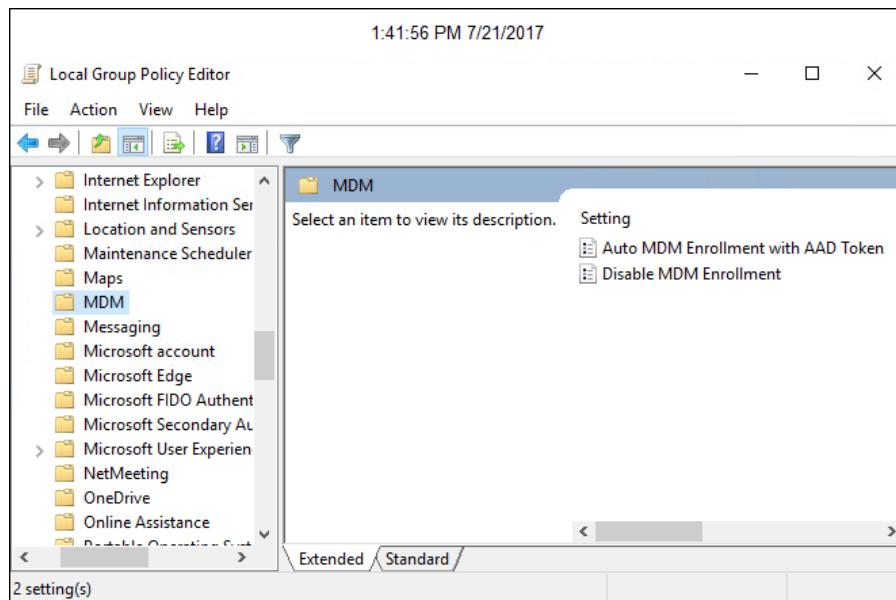
[Join this device to Azure Active Directory](#)

[Join this device to a local Active Directory domain](#)

Next

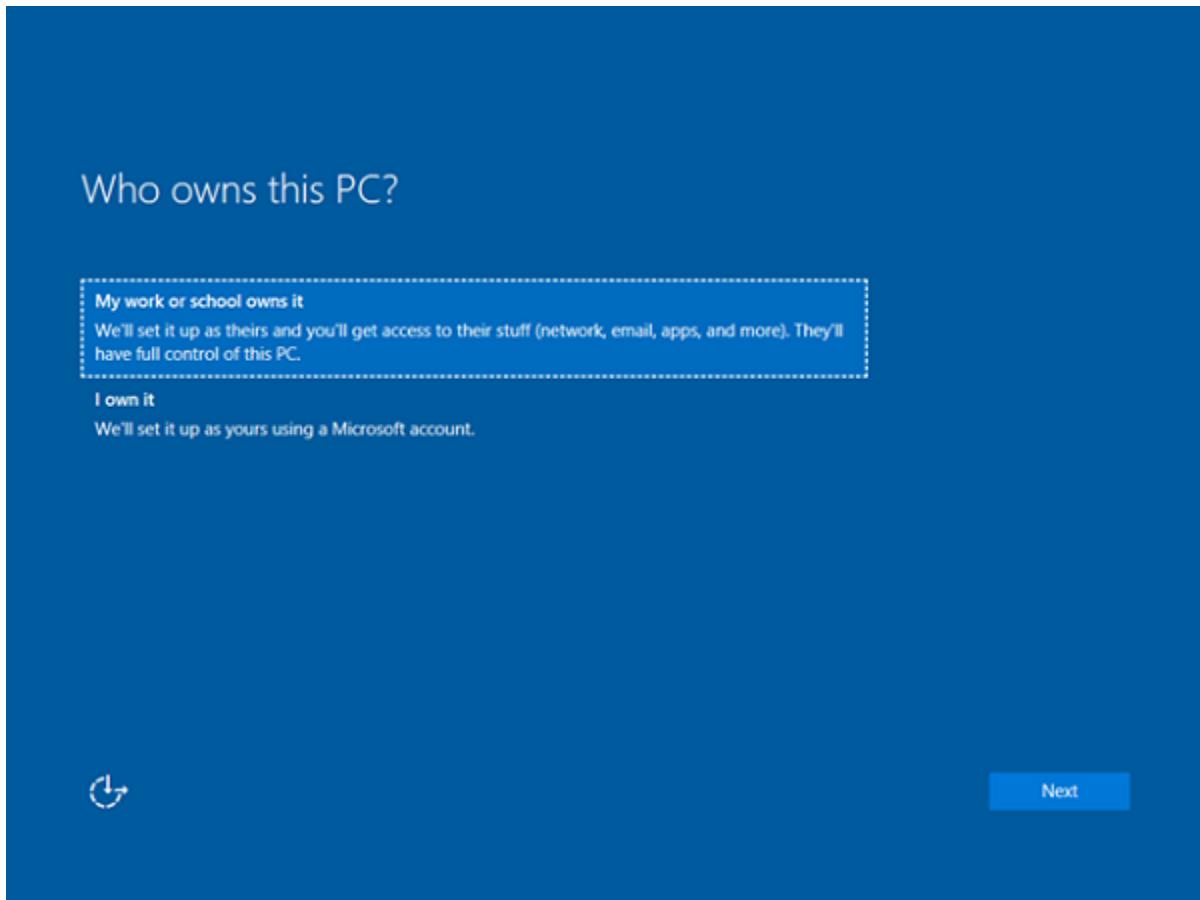
Group policy (hybrid)

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.



The only difference between the default OOBE option and Autopilot:

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

And that's about it.

Windows 10 Autopilot

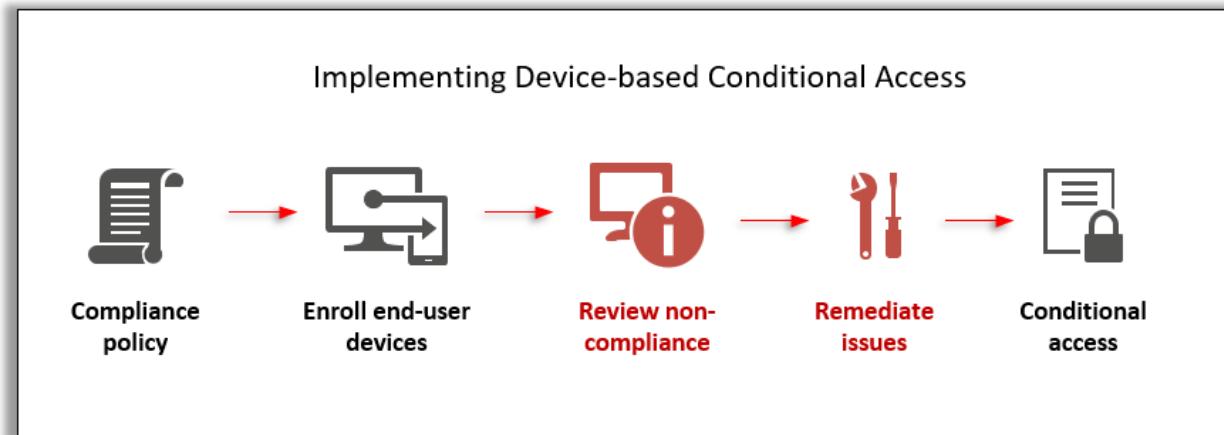
To configure Autopilot requires that you get unique device identifiers imported into Intune in advance. You'd want to get these from the OEM, but they can also be exported via PowerShell from the device. I honestly never do this, except in a lab.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with options like Home, Users, Devices, AutoPilot (which is selected), Policies, Manage, Groups, Roles, Resources, Billing, and Support. The main content area is titled "AutoPilot" and "Standard User". It includes a "Delete profile" button, a "Profile settings" section with a description, and two toggle switches labeled "On". Below that is a "Skip privacy settings" section with another "On" toggle. There's also a note about AutoPilot defaults and a link to a detailed explanation. At the bottom are "Save" and "Cancel" buttons.

You can basically create profiles, and then assign the imported devices (usually 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](#).

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**.

Microsoft 365 Device Management

Dashboard > Device compliance - Device compliance

Device compliance - Device compliance

Search (Ctrl+ /) Refresh Filter Columns Export Delete

Data in this view is live.

Filters applied: Managed by

0 Devices selected (100 max)

DEVICE NAME	USER PRINCIPAL NAME	MANAGED BY	COMPLIANCE
ALEX-LT01	Alex@itpromentor.com	MDM	Compliant
ALEX-D T01	Alex@itpromentor.com	MDM	Compliant
Elizabeth's MacBook	Elizabeth@itpromentor.com	MDM	Compliant
EV's iPhone	Elizabeth@itpromentor.com	MDM	Compliant

Device enrollment
All services
FAVORITES
Device compliance (highlighted)
Client apps
Device configuration
Devices
Software updates
Conditional Access
Users
Groups
Roles

Manage
Policies
Notifications
Locations
Monitor
Device compliance (highlighted)
Devices without compliance ...
Setting compliance
Policy compliance

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.

Microsoft 365 Device Management

... > Windows 10 Baseline Compliance policy > Device status > ALEX-LT01 - Device compliance > Windows 10 Baseline Compliance policy

Windows 10 Baseline Compliance policy

Policy settings
Export

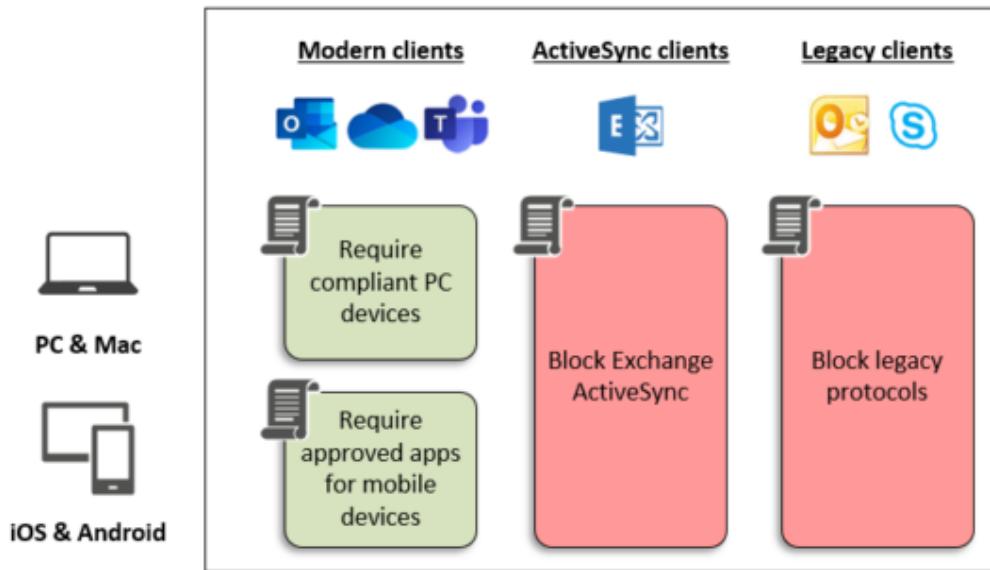
Filter by name

SETTING	STATE	STATE DETAILS
Antispyware	Compliant	
Antivirus	Compliant	
Firewall	Compliant	

Dashboard
All services
FAVORITES
Device enrollment
Device compliance
Client apps
Device configuration
Devices

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)	<ul style="list-style-type: none">o Users > All userso Cloud apps > All apps	<ul style="list-style-type: none">o Device platforms: Windows and MacOSo Client apps: Mobile apps & desktop clients and Modern authentication clients	<ul style="list-style-type: none">o Require device to be marked as complianto Require one of the selected controls
Require approved apps for mobile devices (MDM is optional)	<i>same as above</i>	<ul style="list-style-type: none">o Device platforms: Android and iOSo Client apps: <i>same selections as above</i>	<ul style="list-style-type: none">o Require approved client appo Require one of the selected controls
Block legacy protocols	<i>same as above</i>	<ul style="list-style-type: none">o Client apps > Mobile apps & desktop clients, Other clients	<ul style="list-style-type: none">o Block access
Block Exchange ActiveSync	<ul style="list-style-type: none">o Users > All userso Cloud apps > Office 365 Exchange Online	<ul style="list-style-type: none">o Client apps > Mobile apps & desktop clients, Exchange ActiveSync	<ul style="list-style-type: none">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.

The screenshot shows the Microsoft 365 Device Management interface. On the left sidebar, under the 'FAVORITES' section, the 'Device configuration' item is highlighted with a red box. The main content area is titled 'Device configuration - Profiles'. At the top right of this area, there is a 'Create profile' button with a red box around it. Below the title, there's a search bar and some navigation links like 'Overview' and 'Manage'. Under 'Manage', the 'Profiles' link is highlighted with a red box. The main pane displays a table with columns: PROFILE NAME, PLATFORM, PROFILE TYPE, and ASS. The table currently shows 'No device configuration profiles.'.

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**.

The screenshot shows the Azure Active Directory admin center interface. On the left sidebar, under 'FAVORITES', the 'Azure Active Directory' icon is selected and highlighted with a red box. Below it, the 'Properties' link is also highlighted with a red box. The main content area displays the 'itpromentor.com - Properties' page for Azure Active Directory. It includes fields for 'Name' (itpromentor.com), 'Country or region' (United States), 'Location' (United States datacenters), 'Notification language' (English), and a 'Directory ID' field containing a long GUID. A 'Save' button is visible at the top right.

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

The screenshot shows the Microsoft 365 Device Management interface. On the left sidebar, under 'FAVORITES', the 'Device configuration' icon is selected. The main content area shows the 'Create profile' screen. It has fields for 'Name' (Windows 10 OneDrive Config), 'Description' (Enable files on demand, silently configure known folder move), 'Platform' (Windows 10 and later), and 'Profile type' (Administrative Templates). The 'Name' field is highlighted with a purple border, and the 'Description' field has a green checkmark indicating validation status.

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.

The screenshot shows the Microsoft 365 Device Management interface. On the left, there's a navigation sidebar with various options like Dashboard, All services, Favorites (Device compliance, Device enrollment, Client apps, Device configuration), Devices, Security Baselines, Desktop Analytics, Software updates, Conditional Access, Users, Groups, Roles, and Troubleshoot. The main area is titled "Windows 10 OneDrive Config - Settings" and shows an "Administrative template profile". There's a search bar at the top with the placeholder "Search (Ctrl+/" and the word "onedrive" typed into it, which is highlighted with a red box. Below the search bar are tabs for Overview, Manage, Properties, and Settings (which is selected). The main content area displays two settings: "Allow syncing OneDrive accounts for only specific organizations" and "Allow users to choose how to handle Office file sync conflicts".

Scroll down to enable the following settings:

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

The screenshot shows the Microsoft 365 Device Management interface with a different set of navigation items on the left: Dashboard, All services, Favorites (Device compliance, Device enrollment, Client apps, Device configuration, Devices, Security Baselines, Desktop Analytics, Software updates, Conditional Access, Users, Groups, Roles, Troubleshoot). The main area is titled "Windows 10 OneDrive Config - Set" and shows the "Use OneDrive Files On-Demand" setting. A context menu is open over this setting, listing options: Refresh, Prevent, Prompt, Require, Set the, Set the, Show O, Silently, Specify, Specify, Use On..., and Use On... (with a dropdown arrow). The "Enabled" radio button is selected and highlighted with a blue dashed border. Other options are "Disabled" and "Not configured". At the bottom right of the dialog is a blue "OK" button.

2. *Silently move Windows known folders to OneDrive*: Choose **Enabled**. Paste the Directory ID from Azure AD admin center into the **Tenant ID** field. Do not show notifications (**No**). **OK**.

Microsoft 365 Device Management

Silently move Windows known folders to OneDrive

This setting lets you redirect known folders to OneDrive without any user interaction. In sync client builds below 18.171.0823.0001, this setting only redirects empty known folders to OneDrive (or known folders already redirected to a different OneDrive account). In later builds, it redirects known folders that contain content and moves the content to OneDrive. We recommend using this setting together with "Prompt users to move Windows known folders to OneDrive." If moving the known folders silently does not succeed, users will be prompted to correct the error and continue.

If you enable this setting and provide your tenant ID, you can choose whether to display a notification to users after their folders have been redirected.

If you disable or do not configure this setting, your users' known folders will not be silently redirected and/or moved to OneDrive.

Setting type: Device
Supported on: At least Windows Server 2008 R2 or Windows 7
Version: 1.0

Enabled Disabled Not configured

* Tenant ID:

Show notification to users after folders have been redirected: No

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

Microsoft 365 Device Management

Silently sign in users to the OneDrive sync client with their Win...

This setting lets you silently sign in users to the OneDrive sync client (OneDrive.exe) with their Windows credentials.

If you enable this setting, users who are signed in on the PC with the primary Windows account (the account used to join the PC to the domain) can set up the sync client without entering the credentials for the account. Users will still be shown OneDrive Setup so they can select folders to sync and change the location of their OneDrive folder. If a user is using the previous OneDrive for Business sync client (Groove.exe), the new sync client will attempt to take over syncing the user's OneDrive from the previous client and preserve the user's sync settings. This setting is frequently used together with "Set the maximum size of a user's OneDrive that can download automatically" on PCs that don't have Files On-Demand, and "Set the default location for the OneDrive folder."

If you disable or do not configure this setting, users will need to sign in with their work or school account to set up sync.

Setting type: Device
Supported on: At least Windows Server 2008 R2 or Windows 7
Version: 1.0

Enabled Disabled Not configured

You should end up with settings similar to this:

Silently move Windows known folders to OneDrive	Enabled	De
Silently sign in users to the OneDrive sync client with their Windows cred...	Enabled	De
Specify SharePoint Server URL and organization name	Not configured	De
Specify the OneDrive location in a hybrid environment	Not configured	De
Use OneDrive Files On-Demand	Enabled	De

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

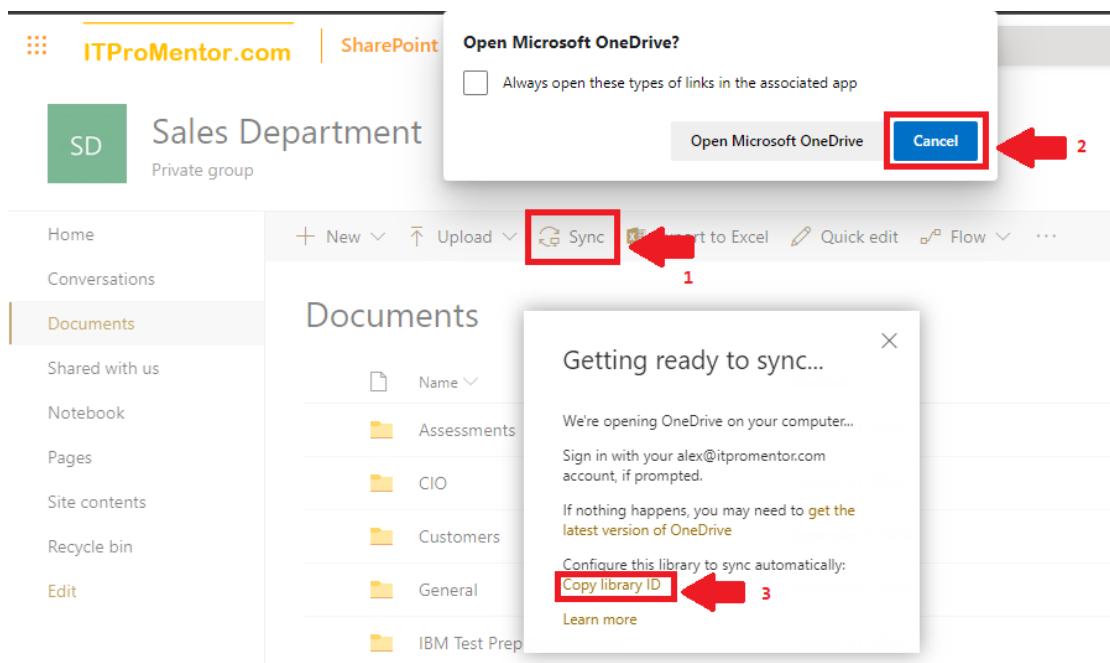
To automatically sync certain SharePoint document libraries to File Explorer in Windows, you would want to create a separate profile. Make as many of these as you need to—similar to mapped drives, these would only be assigned to the users who need access to those locations. For example, if you had a 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**.

SETTING NAME	STATE	SETTING TY...	PATH
Allow syncing OneDrive accounts for only specific organizations	Not configured	Device	\OneDrive
Allow users to choose how to handle Office file sync conflicts	Not configured	User	\OneDrive
Block syncing OneDrive accounts for specific organizations	Not configured	Device	\OneDrive
Coauthor and share in Office desktop apps	Not configured	User	\OneDrive
Configure team site libraries to sync automatically	Not configured	Device	\OneDrive
Configure team site libraries to sync automatically	Not configured	User	\OneDrive
Continue syncing on metered networks	Not configured	User	\OneDrive

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.

NAME	VALUE
Sales Department	tenantId=025b5c6b%2D4d8a%2D...

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 an 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).

The screenshot shows the Microsoft Intune portal interface for configuring Windows 10 Baseline: Firewall config - Properties. On the left, under 'Endpoint protection', there are several sections: Windows Defender Application (10 settings available), Windows Defender Firewall (6 of 43 settings configured, highlighted with a red box), Windows Defender SmartScreen (2 settings available), Windows Encryption (38 settings available), Windows Defender Exploit Guard (21 settings available), Windows Defender Application (2 settings available), Windows Defender Credential Guard (1 setting available), and Windows Defender Security Center. On the right, under 'Windows Defender Firewall', there are five tabs: Pre-shared key encoding (Enable, Not configured), IPsec exemptions (0 selected), Certificate revocation list verification (Not configured), Opportunistically match authentication set per keying module (Enable, Not configured), and Packet queuing (Not configured). Below these tabs is a 'Network settings' section with three items: Domain (workplace) network (2 of 12 settings configured), Private (discoverable) network (2 of 12 settings configured), and Public (non-discoverable) network (2 of 12 settings configured). A large red box surrounds the 'Windows Defender Firewall' tab and its network settings section.

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**.

The screenshot shows the Microsoft Endpoint Manager Admin Center interface. The left pane displays the navigation path: Dashboard > Device configuration - Profiles > Windows 10 Baseline: UAC - Properties > Endpoint protection > Local device security options. The right pane is titled "Local device security options" and lists several categories: Accounts (6 settings available), Devices (4 settings available), Interactive Logon (8 settings available), Network access and security (11 settings available), Recovery console and shutdown (2 settings available), User account control (5 of 10 settings configured), Microsoft Network Client (3 settings available), and Microsoft Network Server (2 settings available). The "User account control" section is highlighted with a red box.

Make the following settings selections (as pictured):

The screenshot shows the "User account control" settings configuration page. It includes the following sections and configurations:

- UIA integrity without secure location**: Block (Enabled) / Not configured (Not configured)
- Virtualize file and registry write failures to per-user locations**: Enabled (Enabled) / Not configured (Not configured)
- Only elevate executable files that are signed and validated**: Enabled (Enabled) / Not configured (Not configured)
- UIA elevation prompt behavior**:
 - Elevation prompt for admins**: Prompt for consent on the secure desktop (Prompt for consent on the secure desktop)
 - Elevation prompt for standard users**: Prompt for credentials on the secure des... (Prompt for credentials on the secure des...)
 - Route elevation prompts to user's interactive desktop**: Enabled (Enabled) / Not configured (Not configured)
 - Elevated prompt for app installations**: Enabled (Enabled) / Not configured (Not configured)
 - UIA elevation prompt without secure desktop**: Enabled (Enabled) / Not configured (Not configured)
- Admin Approval Mode**:
 - Admin Approval Mode For Built-in Administrator**: Enabled (Enabled) / Not configured (Not configured)
 - Run all admins in Admin Approval Mode**: Enabled (Enabled) / Not configured (Not configured)

Windows Encryption (BitLocker)

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

The screenshot shows two adjacent windows. The left window is titled "Endpoint protection" and lists categories like "Windows Defender Application Gu...", "Windows Defender Firewall", "Windows Defender SmartScreen", and "Windows Encryption". The right window is titled "Windows Encryption" and contains settings for "Encrypt devices", "Encrypt storage card (mobile only)", "BitLocker base settings", and "Warning for other disk encryption". Each setting has a "Require" or "Block" button next to a "Not configured" status indicator.

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

This screenshot shows the "BitLocker OS drive settings" configuration page. It includes options for "Additional authentication at startup", "BitLocker with non-compatible TPM chip", "Compatible TPM startup", "Compatible TPM startup PIN", "Compatible TPM startup key", "Compatible TPM startup key and PIN", "Minimum PIN Length", "Minimum characters", "OS drive recovery", "Certificate-based data recovery agent", "User creation of recovery password", "User creation of recovery key", "Recovery options in the BitLocker setup wizard", "Save BitLocker recovery information to Azure Active Directory", "BitLocker recovery Information stored to Azure Active Directory", "Store recovery information in Azure Active Directory before enabling BitLocker", "Pre-boot recovery message and URL", and "Pre-boot recovery message". Each setting has a configuration dropdown or button, with some showing "Not configured" and others showing "Allow" or "Block" options.

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.

The image shows two adjacent windows side-by-side. The left window is titled "Device restrictions" and lists various system components with their configuration status. The right window is titled "Windows Defender Antivirus" and lists various antivirus settings with their current state and configuration status.

Setting	Current State	Configuration Status
Real-time monitoring	Enable	Not configured
Behavior monitoring	Enable	Not configured
Network Inspection System (NIS)	Enable	Not configured
Scan all downloads	Enable	Not configured
Configure low CPU priority for scheduled scans	Enabled	Not configured
Catch-up quick scan	Block	Not configured
Catch-up full scan	Block	Not configured
Scan scripts loaded in Microsoft web browsers	Enable	Not configured
End-user access to Defender	Block	Not configured
Security intelligence update interval (in hours)	1	Not configured
Monitor file and program activity	Monitor all files	Not configured
Days before deleting quarantined malware	30	Not configured
CPU usage limit during a scan	20	Not configured
Scan archive files	Enable	Not configured
Scan incoming mail messages	Enable	Not configured
Scan removable drives during a full scan	Enable	Not configured
Scan mapped network drives during a full scan	Enable	Not configured
Scan files opened from network folders	Enable	Not configured
Cloud-delivered protection	Enable	Not configured
File Blocking Level	Not configured	Not configured

Continued...

File Blocking Level ⓘ Not configured

Time extension for file scanning by the cloud ⓘ 0

Prompt users before sample submission ⓘ Always prompt

Time to perform a daily quick scan 3 AM

Type of system scan to perform Not configured

Detect potentially unwanted applications ⓘ Block

Submit samples consent ⓘ Send safe samples automa...v

On Access Protection ⓘ Block Not configured

Actions on detected malware threats ⓘ Enable Not configured

Low severity	Clean
Moderate severity	Quarantine
High severity	Remove
Severe severity	Block

Windows Defender Antivirus Exclusions 3 settings available >

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.)

Device restrictions Windows 10 and later 3 settings available

Reporting and Telemetry 3 settings available >

Search 9 settings available >

Start 28 settings available >

Windows Defender SmartScreen 1 of 3 settings configured >

Windows Spotlight

Windows Defender SmartScreen Windows 10 and later

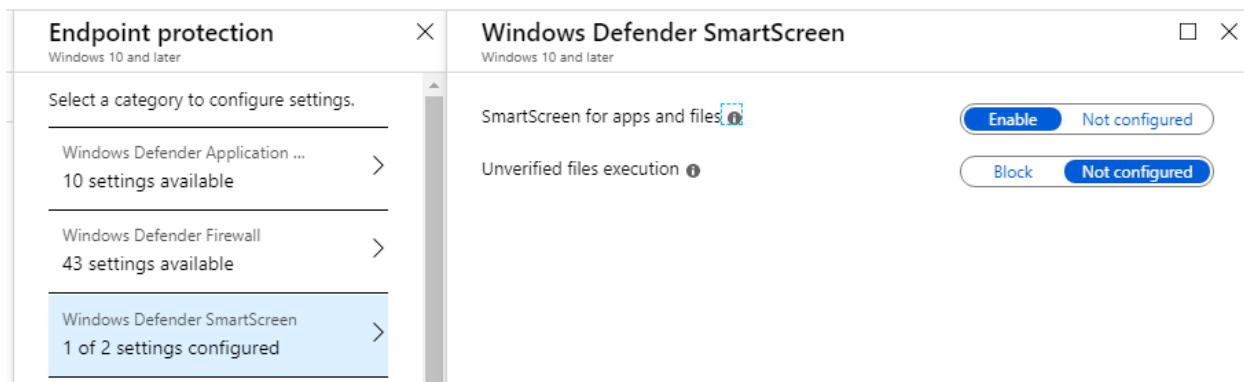
SmartScreen for Microsoft Edge ⓘ Require Not configured

Malicious site access ⓘ Block Not configured

Unverified file download ⓘ Block Not configured

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.

Endpoint protection (Windows 10 and later)

- Select a category to configure settings.
- Windows Defender Application Gu... 1 of 10 settings configured
- Windows Defender Firewall 43 settings available
- Windows Defender SmartScreen 2 settings available
- Windows Encryption 38 settings available

Windows Defender Application Guard (Windows 10 and later)

While using Microsoft Edge, Windows Defender Application Guard protects your environment from sites that haven't been defined as trusted by your organization. When users visit sites that aren't listed in your isolated network boundary, the sites will be opened in a virtual browsing session in Hyper-V. Trusted sites are defined by a network boundary, which can be configured in Device Configuration. Note this feature is only available for Windows 10 (64-bit) devices.

Application Guard ⓘ Enabled for Edge

Clipboard behavior ⓘ Not configured

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.*

Endpoint protection (Windows 10 and later)

- Windows Defender SmartScreen 2 settings available
- Windows Encryption 38 settings available
- Windows Defender Exploit Guard 6 of 21 settings configured
- Windows Defender Application ... 2 settings available

Windows Defender Exploit Guard (Windows 10 and later)

- Attack Surface Reduction 4 of 15 settings configured
- Controlled folder access 1 of 3 settings configured
- Network filtering 1 of 1 setting configured
- Exploit protection 3 settings available

Attack Surface Reduction

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

Office apps injecting into other processes (no exceptions) <small> ⓘ</small>	Not configured
Office apps/macros creating executable content <small> ⓘ</small>	Block
Office apps launching child processes <small> ⓘ</small>	Block
Win32 imports from Office macro code <small> ⓘ</small>	Not configured
Process creation from Office communication products (beta) <small> ⓘ</small>	Not configured

And Rules to prevent script threats:

Obfuscated js/vbs/ps/macro code <small> ⓘ</small>	Not configured
js/vbs executing payload downloaded from Internet (no exceptions) <small> ⓘ</small>	Block
Process creation from PSEXEC and WMI commands <small> ⓘ</small>	Not configured
Untrusted and unsigned processes that run from USB <small> ⓘ</small>	Not configured
Executables that don't meet a prevalence, age, or trusted list criteria <small> ⓘ</small>	Not configured
Rules to prevent email threats	
Execution of executable content (exe, dll, ps, js, vbs, etc.) dropped from email (webmail/mail client) (no exceptions)	Block

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

Attack Surface Reduction exceptions	
Files and folder to exclude from attack surface reduction rules <small> ⓘ</small>	Import
Files and folders <small> ⓘ</small>	Add
<i>Examples: C:\Path, %ProgramFiles%\Path\filename.exe</i>	

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.

Controlled folder access

Automatically block access to content in protected folders. This can be enabled in Audit/Block mode.

[Learn more](#)

Folder protection ⓘ

Enable

List of apps that have access to protected folders ⓘ

Import

Apps

Example: C:\Path\Filename.exe

Add

This screenshot shows the 'Controlled folder access' settings page. It includes a descriptive text about blocking access to protected folders, a 'Learn more' link, a dropdown menu for folder protection (set to 'Enable'), a list of apps with access, an 'Import' button, a text input for app paths, and an 'Add' button.

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

List of additional folders that need to be protected ⓘ

Import

Folders

C:\Users\%username%\OneDrive - ITProMentor.com

Add

This screenshot shows the 'List of additional folders that need to be protected' section. It displays a single folder path 'C:\Users\%username%\OneDrive - ITProMentor.com' with an 'Add' button next to it.

Network filtering

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

Network filtering

Block outbound connection from any app to low reputation IP/domain · This can be enabled in Audit/Block mode.

[Learn more](#)

Network protection ⓘ

Enable

This screenshot shows the 'Network filtering' settings page. It includes a descriptive text about blocking connections to low-reputation IPs/domains, a 'Learn more' link, a dropdown menu for network protection (set to 'Enable'), and a 'Network protection' section.

Exploit protection

Not recommended for typical baseline configuration.