

The Microsoft 365 Business Admin Guide:

Deploying, Securing & Managing Microsoft 365 Business

By Alex Fields, ITProMentor.com

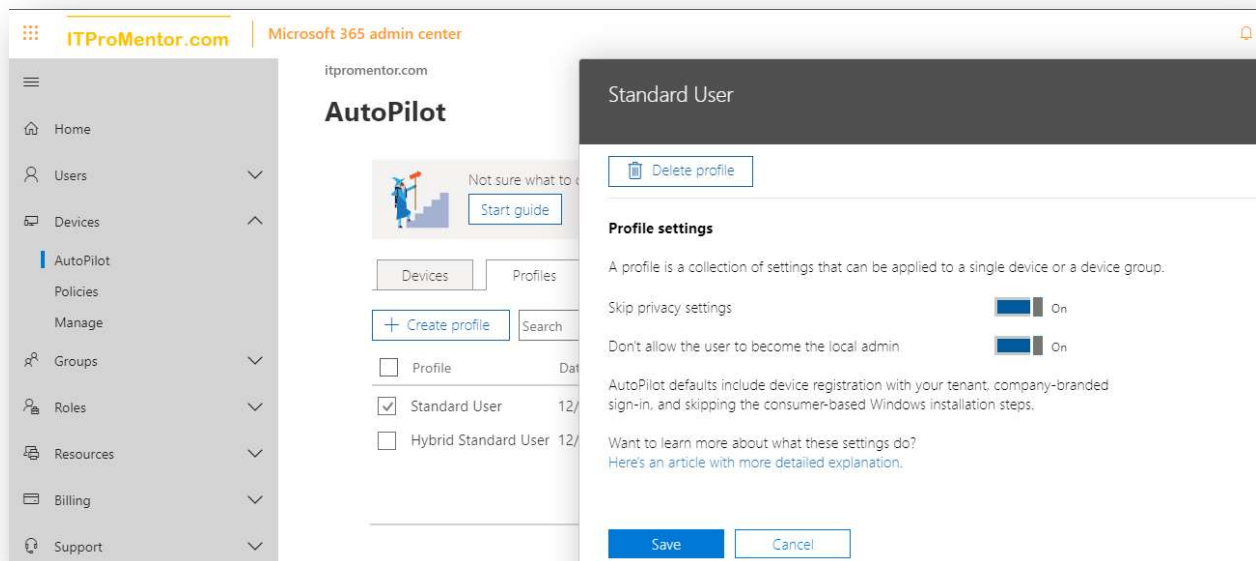


Table of Contents

Contents

| | |
|-----------------------------------------------------------------------|----|
| The Microsoft 365 Business Admin Guide:..... | |
| Deploying, Securing & Managing Microsoft 365 Business | |
| By Alex Fields, ITProMentor.com..... | |
| Table of Contents..... | i |
| Contents..... | i |
| Deploying, Securing & Managing Microsoft 365 (SMB)..... | 1 |
| Introduction: The problem of life after “the four walls” | 1 |
| Target audience | 2 |
| The structure of this guide..... | 3 |
| Getting Started with the Microsoft 365 Business subscription..... | 3 |
| Step 1. Personalize sign-in (add your vanity domain) | 4 |
| Step 2. Add Users..... | 6 |
| Step 3. Protect Data & Devices..... | 8 |
| Part 1. Identity Management..... | 13 |
| Introducing the Microsoft 365 Admin center | 14 |
| Managing user identities and assigning software licenses..... | 14 |
| Customize the theme | 16 |
| Enabling Multi-factor Authentication (MFA) | 17 |
| Configure the password policy in the Microsoft 365 admin center | 20 |
| Passwordless sign-in..... | 20 |
| Explore the Azure AD Admin Center..... | 21 |
| Managing Users in Azure AD | 22 |
| Password reset for cloud identities | 22 |
| User enrollment in MFA and SSPR | 26 |
| Activity Logs..... | 27 |
| Groups..... | 29 |
| Configure Company branding | 30 |
| Configure the Azure AD application portal..... | 31 |
| Configure SSO to third-party applications..... | 32 |
| Hybrid support in Microsoft 365 Business..... | 35 |
| Understanding User Sign-in options..... | 36 |

| | |
|-------------------------------------------------------------------------------------|-----|
| Prepare for Azure AD Connect..... | 38 |
| Installing Azure AD Connect..... | 40 |
| Deploy group policy for Seamless SSO..... | 49 |
| Understanding the Source of Authority and Hybrid management of Exchange Online..... | 51 |
| Hybrid SSPR with password write-back..... | 57 |
| Conditional Access for the SMB..... | 61 |
| Conditional Access | 61 |
| Part 2. Device Management..... | 63 |
| Windows 10 Management..... | 63 |
| Windows 10 device configuration policies..... | 63 |
| Device Settings and Enterprise State Roaming | 65 |
| Understanding the device’s relationship to Azure AD..... | 67 |
| Enabling Hybrid Join for Windows 10 devices..... | 73 |
| Windows 10 Deployment Options | 76 |
| Mobility Management via Intune: MDM vs. MAM | 88 |
| Configuring MAM for iOS and Android | 89 |
| Configure MDM for iOS and Android..... | 96 |
| Manage devices in the Microsoft 365 admin center | 114 |
| Part 3. App & Data Protections | 115 |
| Configure Azure Information Protection..... | 116 |
| Enabling email encryption (OME)..... | 116 |
| Azure Information Protection labels..... | 121 |
| Office 365 Sensitivity labels | 133 |
| Data Governance: Archive and retention | 149 |
| Enable the Archive mailbox..... | 151 |
| Configure retention policies | 154 |
| Creating custom retention labels..... | 158 |
| Configure Data Loss Prevention (DLP) | 163 |
| Example 1. GLBA: Auto-encrypt email content..... | 164 |
| Example 2. HIPAA: File an incident report..... | 171 |
| Enable Advanced Threat Protection (ATP) policies..... | 178 |
| Safe Links | 178 |
| Safe Attachments..... | 182 |

| | |
|----------------------------------------------------|-----|
| Anti-Phish..... | 185 |
| Microsoft 365 Business: Continued improvement..... | 192 |
| Alert Policies | 193 |
| Secure Score..... | 199 |
| Compliance Manager..... | 200 |
| Conclusion..... | 203 |

Deploying, Securing & Managing Microsoft 365 (SMB)

By Alex Fields, ITProMentor.com

Introduction: The problem of life after “the four walls”

Microsoft 365 Business is an end-to-end productivity, security, and device management solution designed to transition—and ultimately replace—traditional on-premises server infrastructures for small and mid-sized businesses. For those of you familiar with Microsoft’s Windows Server products for the small business, Microsoft 365 Business is simply the next evolution.

In this guide we will cover a complete setup, as well as provide walk-throughs for *all* the add-ons, so that you can maximize your leverage of this software bundle and extract the most value from your subscription dollars.

Not to be confused with *Office 365*, which is a suite of cloud-based productivity apps, *Microsoft 365* is a unique SKU that provides further extensions on the Office 365 platform—extensions which, at their core, present answers to a perplexing problem: how do you manage and secure a computing environment that is built on top of a public cloud?

In the olden days, you would have had your data and applications installed on a server in your office building. Therefore, the equipment would be *physically* protected by lock and key, an alarm system, video cameras, and so forth. Likewise, *logical* protections were provided by firewalls, passwords, security logs, antivirus programs, etc., creating digital barriers or “boundaries” which closely mimicked and followed the physical ones around.

| Tools | On-premises (four walls) | Microsoft 365 (cloud) |
|----------------------------------------|--------------------------------------------------------------|---------------------------------------------------------|
| Identity Management | Active Directory, username and password | Azure AD, multi-factor / passwordless authentication |
| Device Management | Group Policy, SCCM, third-party tools, MDM, etc. | Microsoft Intune |
| Application deployment | Group Policy, SCCM, third-party tools, etc. | Microsoft Intune |
| Patch management | WSUS, SCCM, third party | Microsoft Intune |
| Antivirus and Security software | Third-party AV, firewall appliances w/ subscriptions | Windows Defender, Office 365 ATP |
| Data Loss Prevention | BitLocker, EFS, third-party encryption + other tools | BitLocker, Azure Information Protection, Office 365 DLP |
| Email Archive/Retention | Exchange Server Enterprise + Enterprise CAL's or third-party | Exchange Online Archiving, Litigation hold |
| Remote Access | Virtual Private Network (VPN), Remote Desktop | Secure Socket Layer (SSL), browsers, mobile apps, etc. |
| Backup | Windows Backup, DPM or third-party software | Third-party software |

However, with the rise of Office 365 and other Software-as-a-Service (SaaS) products like it within the last decade, the traditional, server-based, “four walls” model was beginning to break down. After all, when users, devices and data become mobile, every bit and byte you deposit into the cloud is now accessible from any device, anywhere—so where are your boundaries now? We suddenly find that all the walls have evaporated! The old security mechanisms just weren’t built to work within a mobile-first, cloud-first framework. So, we needed something new: some other ways to manage end-user identities, devices and data—without relying on the concept of the four walls.

Microsoft 365 Business was therefore designed specifically to answer these concerns and provide a modern management platform to compliment the Office 365 productivity suite.

Building on the foundation of Office 365 Business Premium, the new bundle adds an amazing set of enterprise-class subscription-based software such as:

- **Microsoft Intune (Device Management)** – provides modern device-management capabilities (supports iOS, Android, macOS and Windows)
- **Azure Information Protection (AIP)** – Enforces encryption on individual messages and data files, wherever they may go
- **Data Loss Prevention (DLP)** – prevents data leakage and protects sensitive information
- **Exchange Online Archiving** – for managing storage and data retention policies
- **Office 365 Advanced Threat Protection (ATP)** – Machine-learning-assisted anti-malware and anti-phishing protections

Finally: **Windows 10 Business** licensing is also included with the subscription, and it grants upgrade rights from Windows 7/8/8.1 Pro (but not Home editions). All this falls under a single unified SKU at a very affordable price point.

Target audience

I have in mind a specific audience for this guide: people who in some way administer the IT functions for a small or mid-sized business. Therefore, you will find this material helpful if you meet one of these descriptions:

1. You are an “accidental” IT person for a single small or mid-sized business. IT is not your passion, but it may be one of many hats you wear. A fair warning: some of the material here may go a little deeper than you’re used to—but I will do my best to keep it accessible.
2. You are part of a very small IT admin shop in a small business setting—in fact you might be the only person in this role. You basically have the day-to-day down, but when it comes to looking at the big picture—planning for and making substantial changes—you need help.
3. You are an IT consultant for several small and mid-sized businesses. You are constantly busy with your workload, and don’t always have time to study up on the latest and greatest news coming out of Redmond or elsewhere in Silicon Valley. You just appreciate a little bit of guidance to make your job easier, especially when you’re working on migrations to these newer technology platforms.

Because I frequently encounter a lot of individuals who meet the above descriptions in my own work, I think of you all often. I say this because I do want everyone to recognize that we are talking about a wide range of skill-sets and interest levels here. Some of my readers are *really* into tech and enjoy understanding all the bits and bytes. Others of you just sort of end up in the IT role by default, and need some help.

There is no right answer, and it's all good. But I point this out so that we share an understanding—my overarching aim here is to keep this guide simple and accessible, yet thorough. Therefore, I will avoid delving into too much detail, and will avoid overly complex or convoluted subjects.

Therefore, I will pick content with the widest possible audience which still achieves the goal of leveraging all the major components from this subscription to achieve better security, and hopefully a better end-user experience.

The structure of this guide

While focusing on the core management tools which have crystalized over the years on the Microsoft 365 cloud platform, we will cover the Microsoft 365 Business bundle in three major parts:

To begin, I will describe **Identity Management** (think user sign-on and permissions via security groups), which is all built on **Azure Active Directory**.

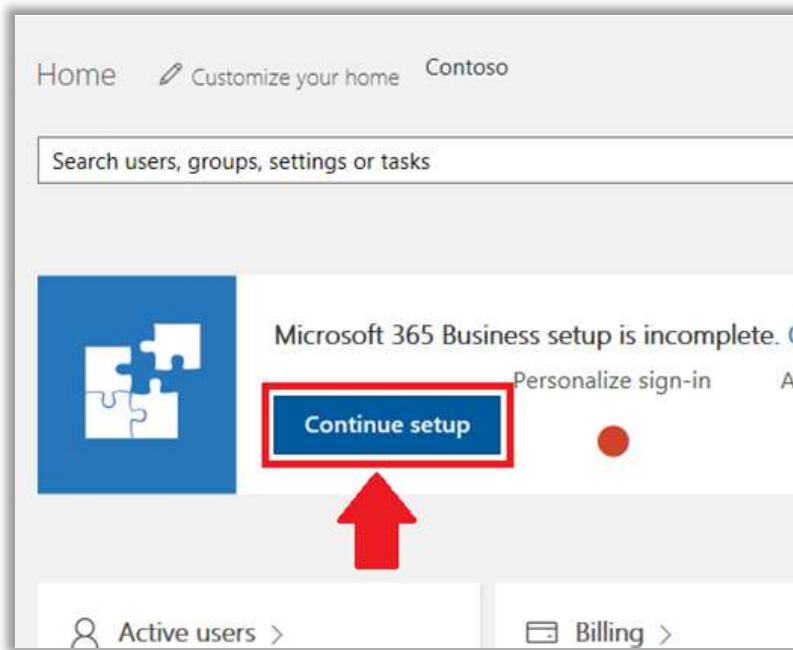
In the second part of the guide, I will cover **Device Management**, which is accomplished primarily through **Windows 10 Business** and **Microsoft Intune** (which also supports other platforms including iOS, Android, and macOS).

In the third and final part, we will cover **App and Data Protections**, enabled mostly via the **Security & Compliance Center** with support from various add-ons:

- **Azure Information Protection**
- **Exchange Online Archiving**
- **Office 365 Data Loss Prevention**
- **Office 365 Advanced Threat Protection**

Getting Started with the Microsoft 365 Business subscription

Before we leap into our first major section on identity management, we should cover some initial subscription configuration using the Microsoft 365 admin center. Hopefully you have already found where to purchase a new subscription, via CSP or direct from Microsoft Online Services.



Also see demos.microsoft.com to stand up quick tenants that you can use for testing.

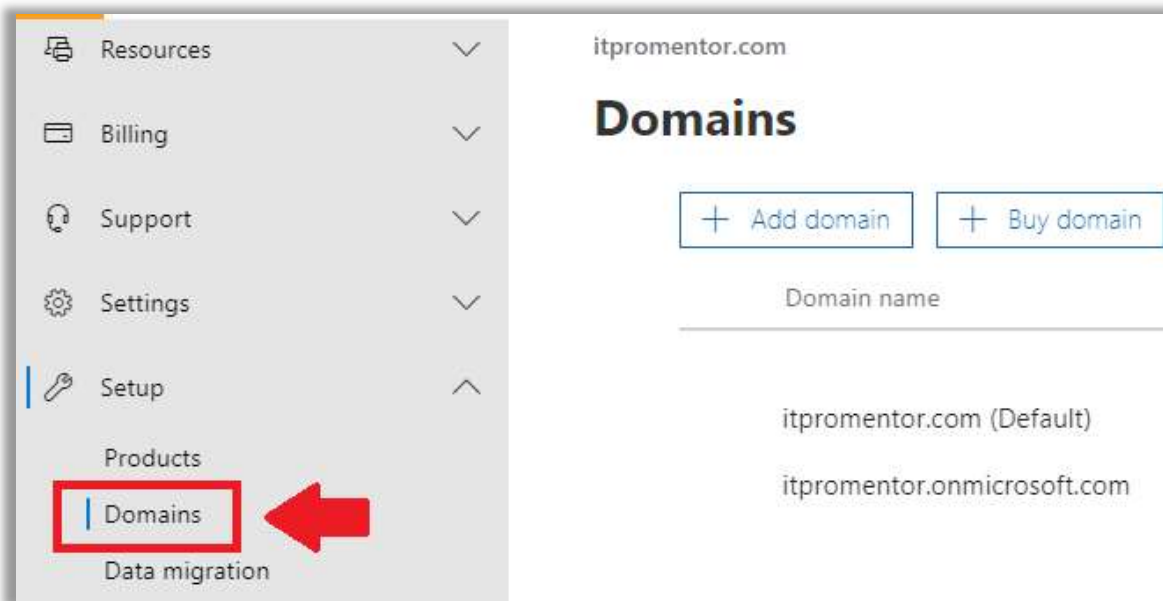
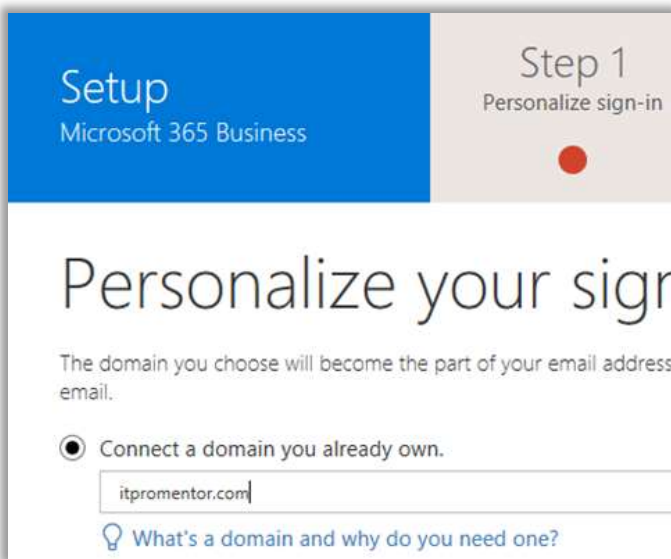
Sign-in to your [Microsoft 365 admin portal](#), find the banner with the button to **Continue setup**.

Note: some of the screens could look different by the time you read this; admin center updates in preview at the time of this writing.

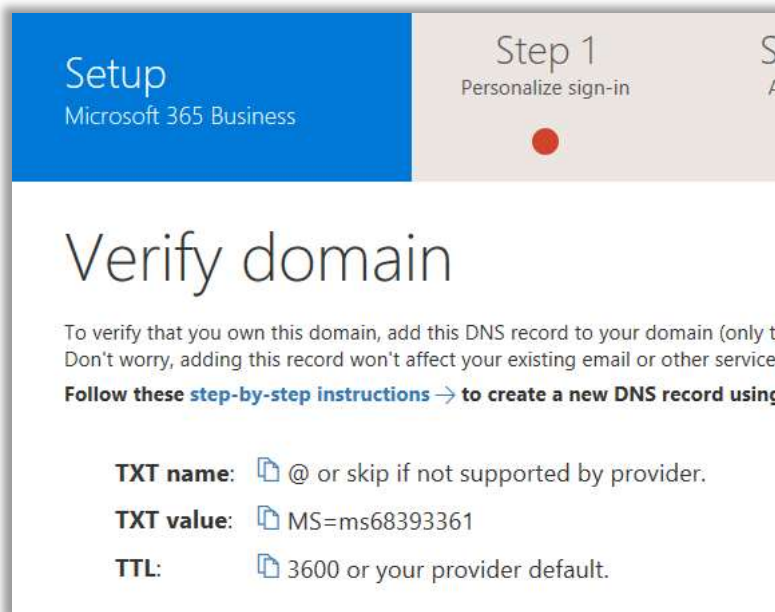
It is optional to complete this wizard, as it is also possible to configure these settings later, within the admin center portal. However, the wizard can save you time, and put a bit of scaffolding in place (in my opinion, it does not go nearly far enough—so only consider this a starting point).

Step 1. Personalize sign-in (add your vanity domain)

In the first step, we will simply add a custom domain name. Note that you can achieve this at any time from the admin center; just click **Show more** then find **Setup > Domains**.

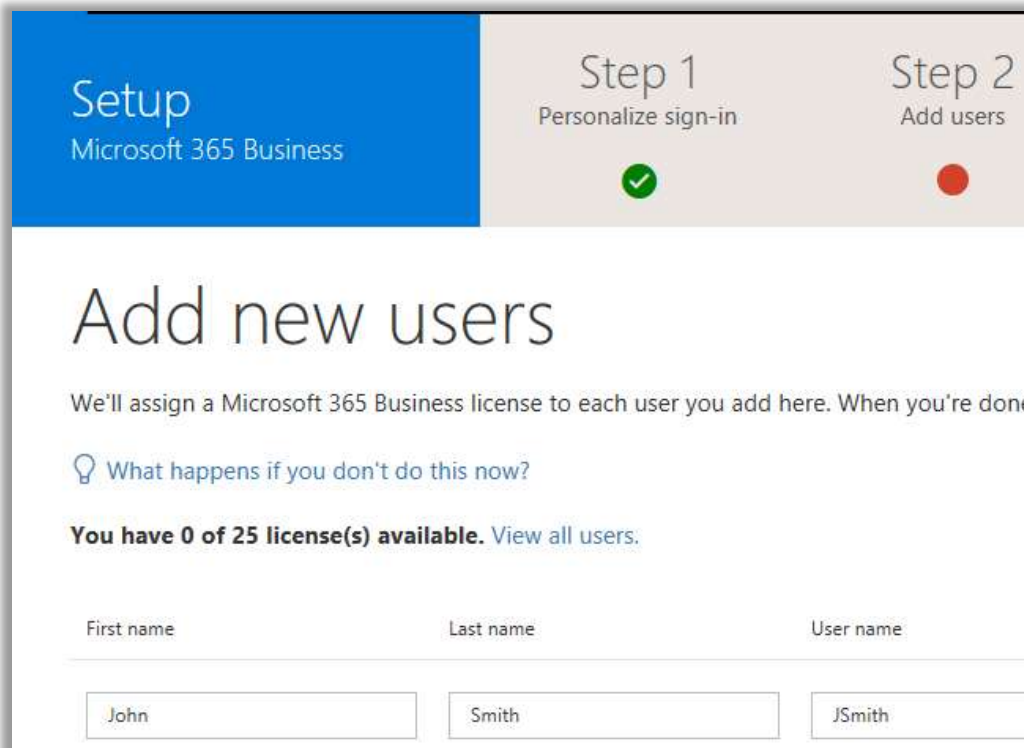


In order to verify the domain, it will be necessary to deposit a small TXT record at your DNS hosting provider. Microsoft will provide you with the necessary values here. Get this task done as early as possible, before you start configuring a lot of users in your tenant.

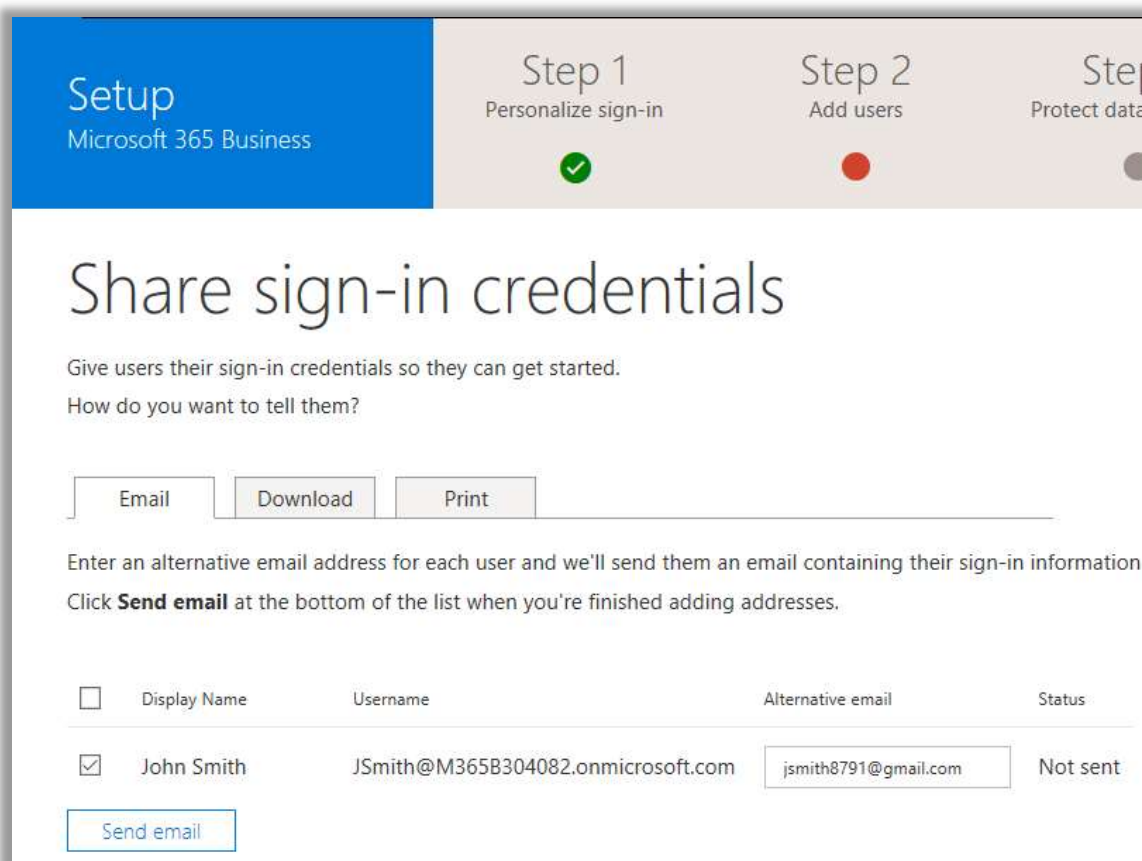


Step 2. Add Users

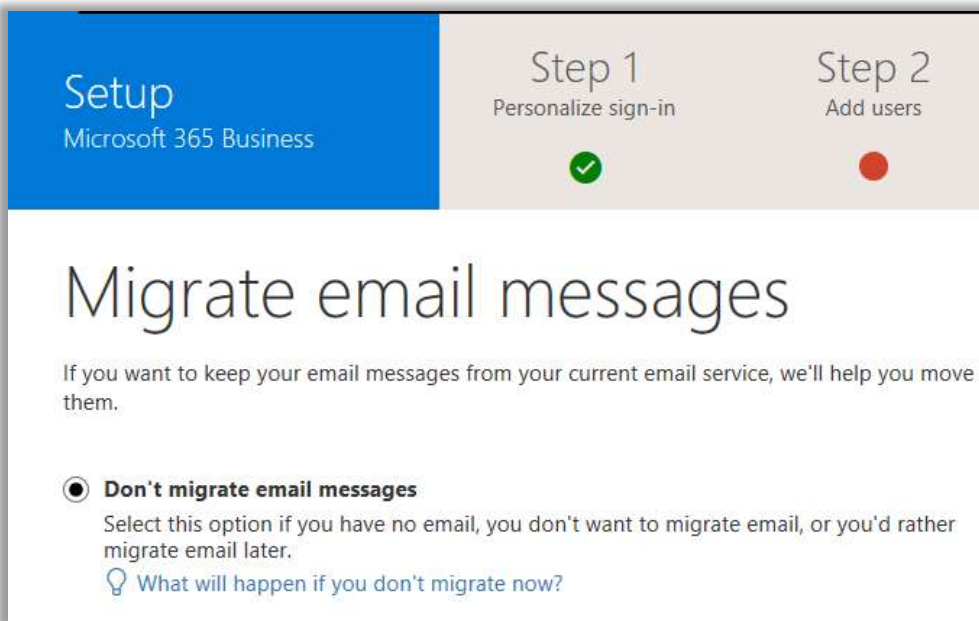
The next step just allows you to add users. If you are going to be importing users later from an on-premises Active Directory using the Azure AD Connect tool, you can skip this step for now.



If you do choose to add some new users at this time, Microsoft will present you with a few options to notify the user and get them started.



At this point in the wizard, you may be prompted to migrate email. I would recommend that you skip this step for now. If you were to opt-in for migration at this point, you will exit the setup wizard, and so would have to return to complete it later. ("SQUIRREL!" No. FOCUS!) Let's just finish stepping through the initial setup screens instead. My website contains good walk-throughs for completing hybrid (*remote move*) migrations to Exchange Online. But more on that later.



Step 3. Protect Data & Devices

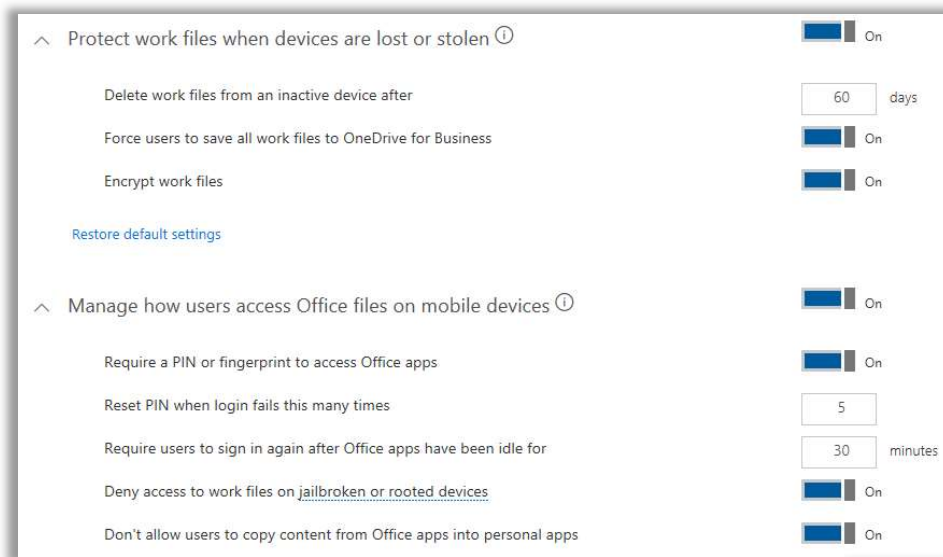
This is where it gets way more interesting, as we will be applying some advanced device and application management policies, through a very easy and intuitive UI. You will have a choice to enable or disable two options with a simple toggle switch:

- Protect work files when devices are lost or stolen
- Manage how users access Office files on mobile devices

These options correspond to Mobile Application Management (MAM) policies. Both of these options can be expanded further to see more granular controls within each.

In the device management chapter, I will cover the differences between Mobile Device Management (MDM) and Mobile Application Management (MAM). For now, just know that

MAM is most often used in Bring-Your-Own-Device or "BYOD" scenarios (which is most small businesses).

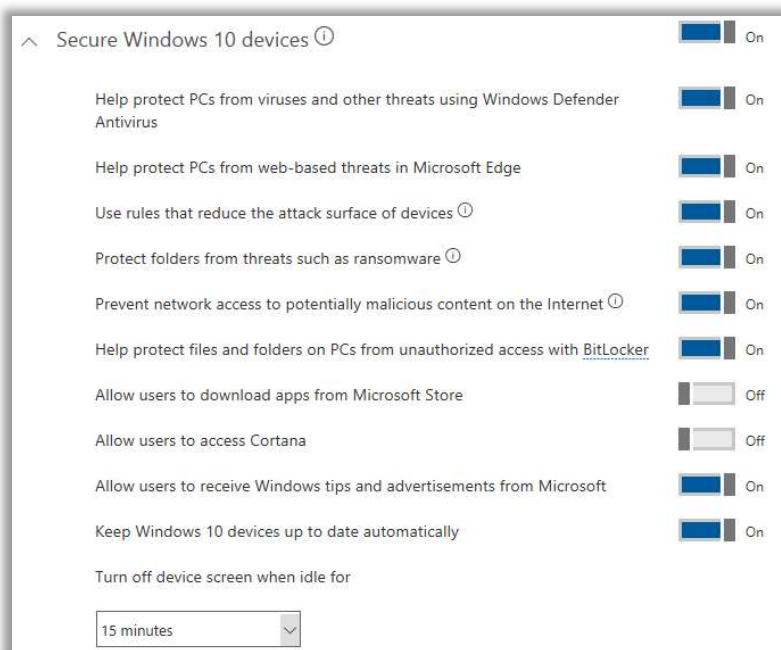


The next screen deals with Windows 10 device configuration policies. The toggles include:

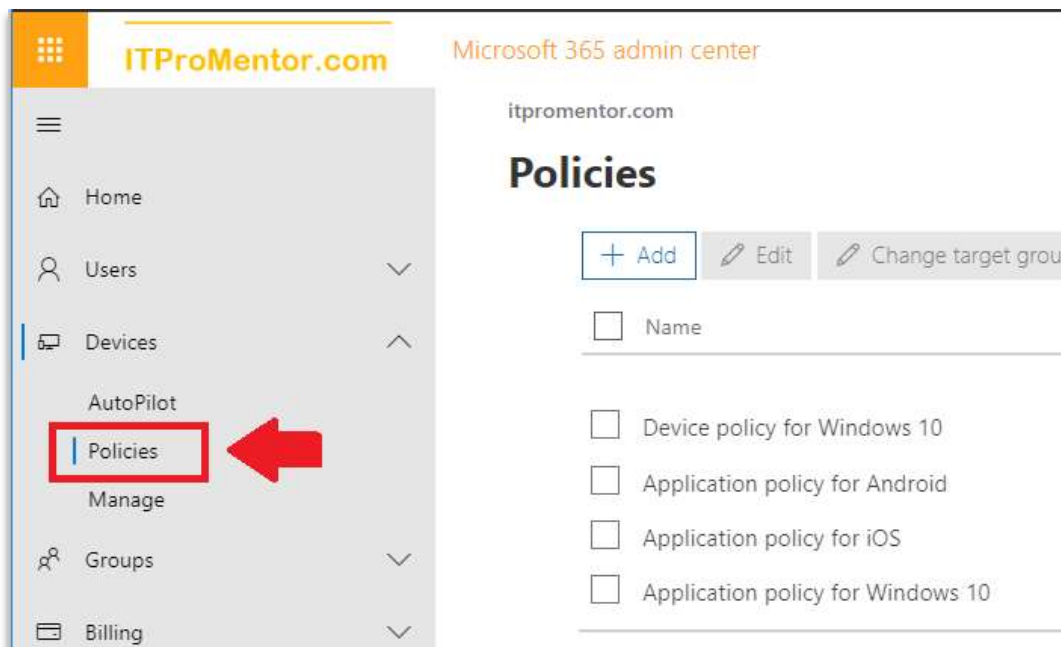
- Secure Windows 10 devices
- Install Office on Windows 10 devices



That first option, to **Secure Windows 10 devices**, can be expanded to reveal several more toggles, which you may also want to adjust. For example, perhaps you want to restrict access to the Microsoft Store.



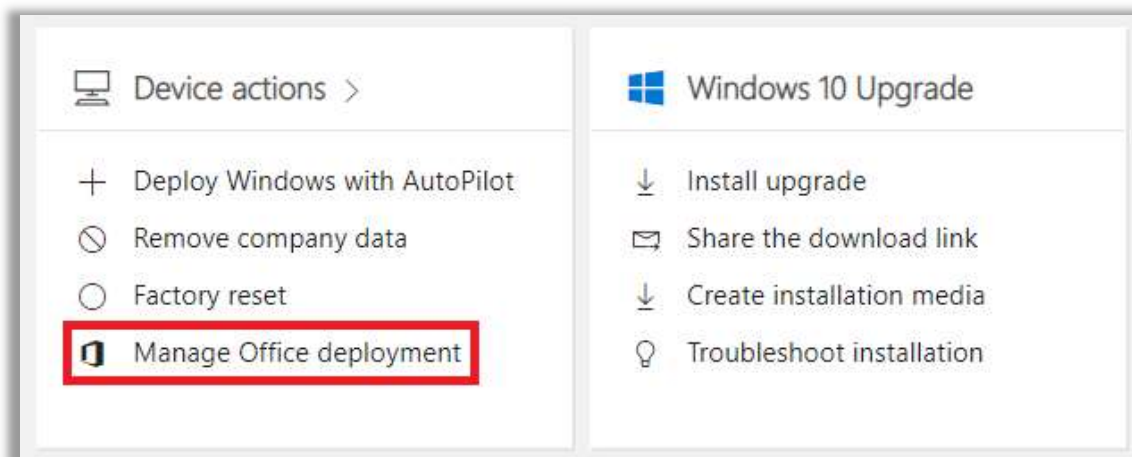
Let's pause for a moment. The policies we just configured correspond to those found in the Microsoft 365 admin center under **Devices > Policies**. You can always come here later and make changes, or, create additional policies and target different settings to various groups.



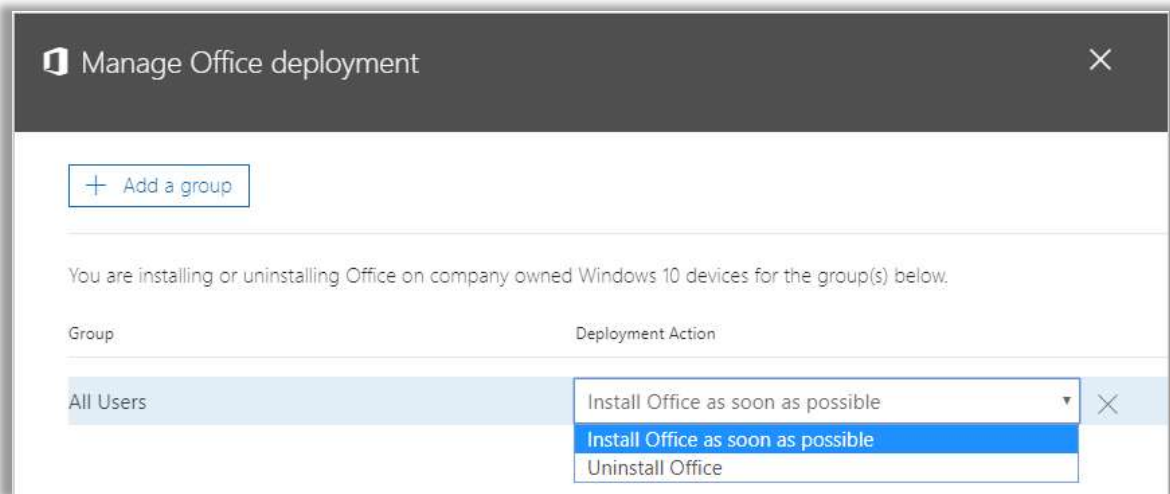
Now about that second option: **Install Office on Windows 10 devices**—automatic application deployment—it’s *really* cool. By default, if you choose to enable this policy, then new Windows 10 PCs which are joined up to Azure AD will have the Office 365 desktop apps (32-bit versions) installed automatically over the Internet.

Unfortunately, the default app deployment here will not remove previous versions or perform any in-place upgrades for you. Alternatively, if we wanted to enable a seamless upgrade experience, or install 64-bit instead of 32, or make any other adjustments to the deployment, then we can customize everything using the Intune/Device Management portal—I’ll have more on this subject in the Device Management section.

To manage the default app deployment policy later within the Microsoft 365 Business portal, find the **Device actions** card on the home screen, and click **Manage Office deployment** (note: this may appear slightly different with upcoming portal updates).



As you can see, we don’t get many toggles here (**Install** or **Uninstall** only), targeting specific groups of users; by default the setup wizard applies the settings to **All users**.



And that essentially concludes everything accomplished via the Setup wizard. As I mentioned, it is pretty slick for deploying org-wide policies quickly. However, it does not really go far enough in some cases, and you will almost certainly want to do further customization from here.

As we move through all of the sections on **Identity Management**, **Device Management** and **App and Data Management**, I will highlight what I think are the most important customizations for you to consider for your customers and/or end-users.

Part 1. Identity Management

Azure Active Directory is the mechanism used by Microsoft 365 to identify and manage users, groups, and devices. Similar to how Active Directory provided the common security boundary for users and computers in the past, you now have the ability to extend that same security boundary into the cloud, or to replace your legacy Active Directory altogether.

Azure AD comes in a few different subscription levels—Basic, Premium P1, and Premium P2. In the Enterprise subscriptions of Microsoft 365, E3 corresponds with Azure AD Premium P1, and the E5 subscription includes Azure AD Premium P2.

However, Microsoft 365 Business is a unique subscription in that it opens up a little bit more functionality than a typical Office 365 subscription, yet it does not quite have all the bells and whistles that you see in Azure AD Premium P1. It stands apart uniquely, as something in between.

| Identity management features | Office 365 Business Premium | Microsoft 365 Business | Azure AD Premium P1 |
|------------------------------------------|-----------------------------|------------------------|---------------------|
| Manage users and groups | Yes | Yes | Yes |
| 99.9% uptime SLA | Yes | Yes | Yes |
| Company branding for user sign-in | Yes | Yes | Yes |
| Basic security logs | Yes | Yes | Yes |
| Cloud Self-service password reset (SSPR) | Yes | Yes | Yes |
| Conditional Access “baseline” policies | Yes | Yes | Yes |
| SSO for up to 10 gallery apps | No | Yes | Yes |
| Multifactor authentication (MFA) | No | Yes | Yes |
| Enterprise State Roaming | No | Yes | Yes |
| Hybrid SSPR (password write-back) | No | Yes | Yes |
| Custom Conditional Access policies | No | Yes | Yes |
| SSO for unlimited apps, + custom apps | No | No | Yes |
| Administrative units | No | No | Yes |
| Two-way device sync (device write-back) | No | No | Yes |
| Detailed security reports including risk | No | No | Yes |

As of June 2019, Microsoft 365 Business subscriptions include custom conditional access policies. We are going to spend a lot of time on this topic, as it is one of the most important security controls available to you in the Microsoft 365 cloud.

Introducing the Microsoft 365 Admin center

Most common administrative tasks such as adding/deleting users, managing groups and assigning licenses can all be managed from within the Microsoft 365 Admin center:

<https://admin.microsoft.com>.

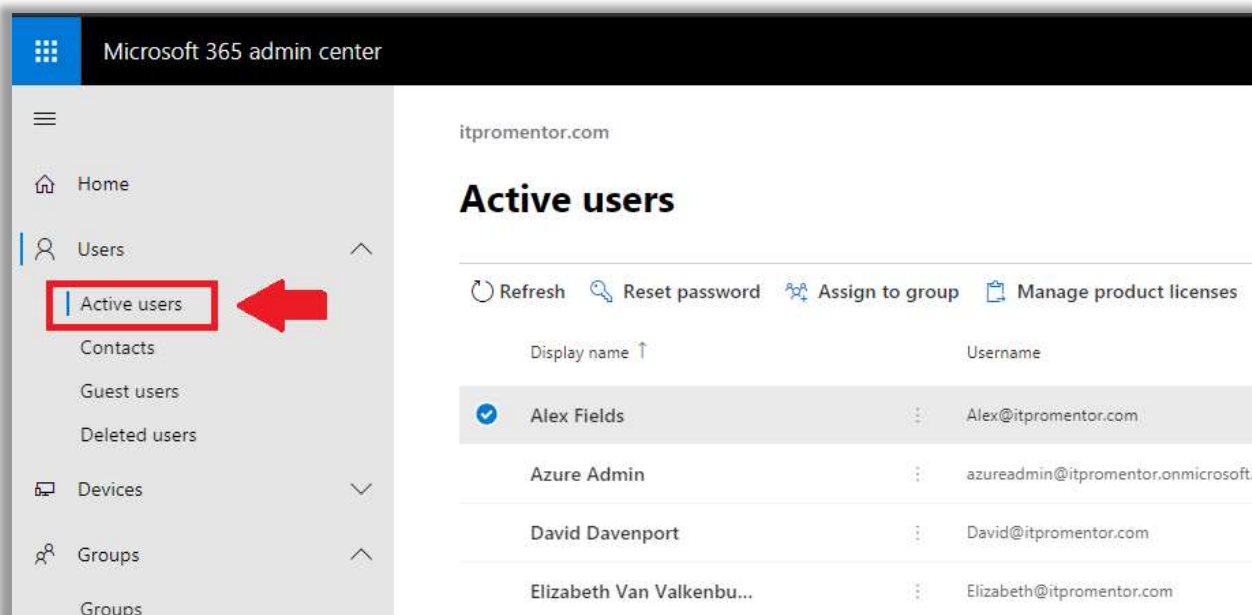
Nevertheless, it is important to remember that everything we see in this admin portal is being “rolled up” from other individual admin centers within our bundle of software such as Azure AD, Intune, SharePoint Online, and Exchange Online. That is why we sometimes find it necessary to go look behind the scenes and figure out what is really going on under the hood, since we only get “shorthand,” or an abbreviated view of options, presented to us through the primary admin interface. In some cases, we will even venture into PowerShell to see or manipulate certain values or settings. That usually provides the most complete view of options, anyway.

For now, let’s just get a feel for the basic Microsoft 365 Admin Center UI.

At the time of this writing, several updates to the portal are in preview, which should be made Generally Available (GA) soon and will probably be more akin to the experience most readers will encounter by the time they read this. But of course, things in the cloud change quickly—so don’t be surprised when some of the screens end up looking a little bit different in practice!

Managing user identities and assigning software licenses

Using the main admin portal, you can easily manage users and groups, and assign software licenses. Go to **Users > Active users**.



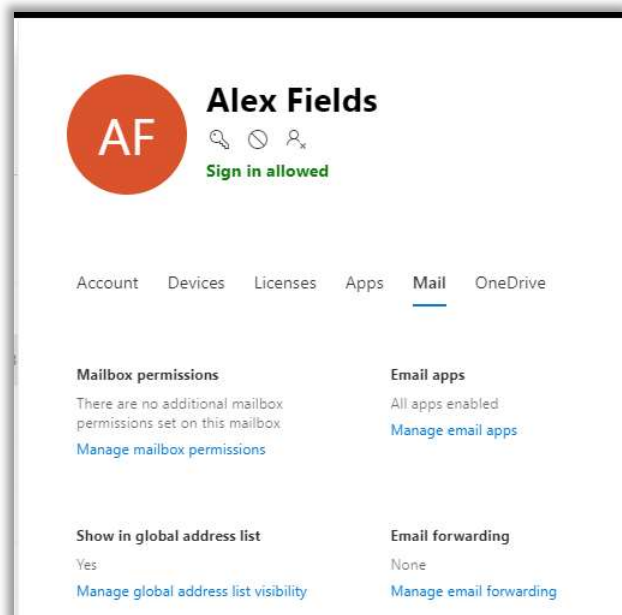
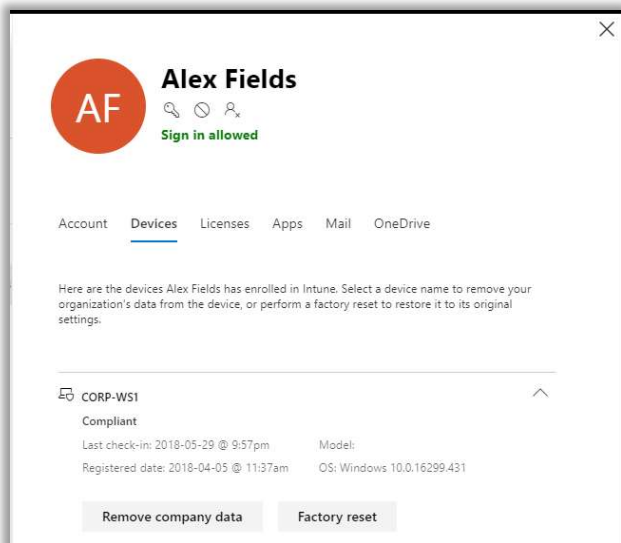
The new portal updates are fantastic. A lot of things which used to be found in disparate screens or portals are being pulled together under a single pane of glass here.

Right above the top row we have very common operations such as *Reset password*, *Assign to group*, *Manage product licenses*, etc. You can also select multiple users in order to make certain edits in bulk.

If you click the name of an individual user you will find several tabs that allow us to cover a lot of ground quickly, revealing almost anything tied to that user. For example, under **Devices**, we can quickly identify devices associated with that user via Intune. From there, you can *Remove company data* or perform *Factory reset*.

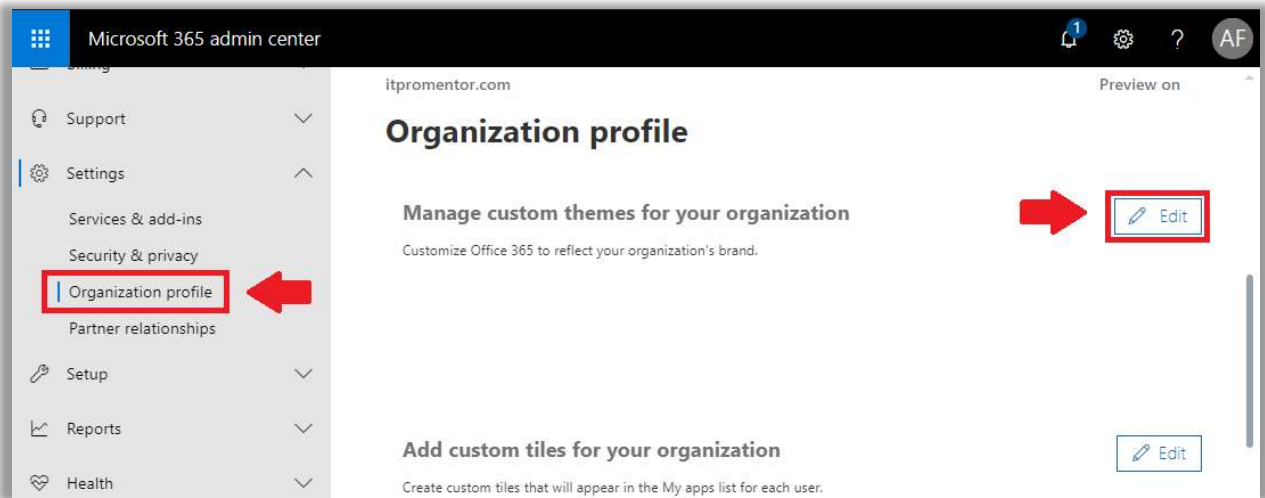
This is where you can edit application-specific settings also, such as those related to Exchange Online and OneDrive. Click on **Mail**, for instance; many options can be configured here without navigating to the Exchange Online admin center: aliases, delegation, forwarding, even Out-of-Office messages, and more!

Certain links will still take you out to the appropriate management UI in another browser tab, but overall this is a major improvement from the old Admin center, which was quite a bit clunkier. Feel free to explore all of the various options within the **Active users** area.

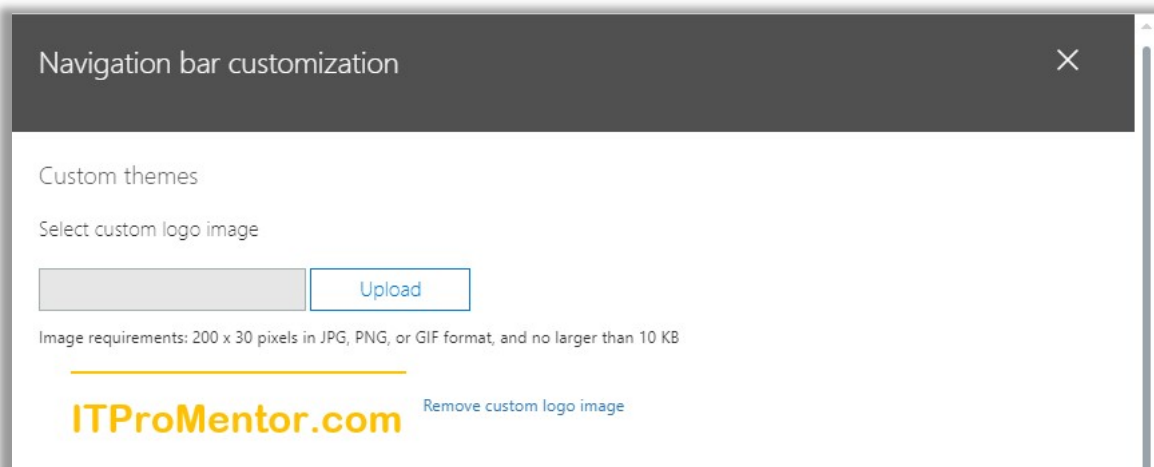
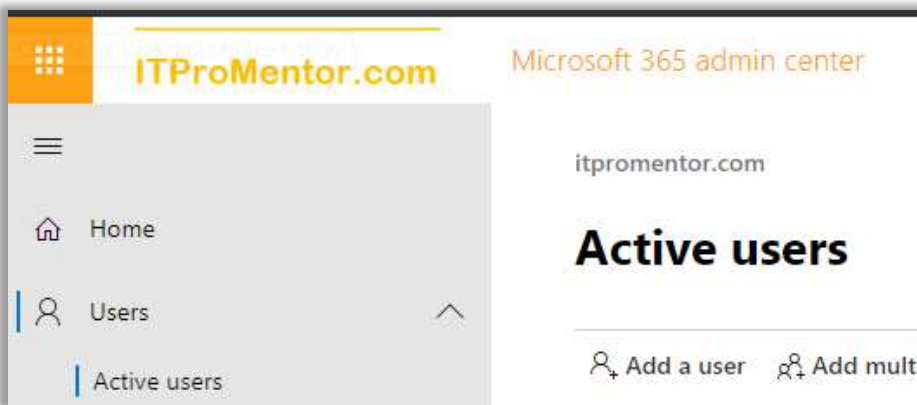


Customize the theme

From the Microsoft 365 admin center's left menu, click **Show more**, then scroll down to find **Settings > Organization profile**. Locate *Manage custom themes for your organization* and click **Edit** on the right.



From there you can upload your logo and further customize the theme. After you save changes, you will see the new branding reflected whenever you sign in to 365 services, including the Microsoft 365 admin center!



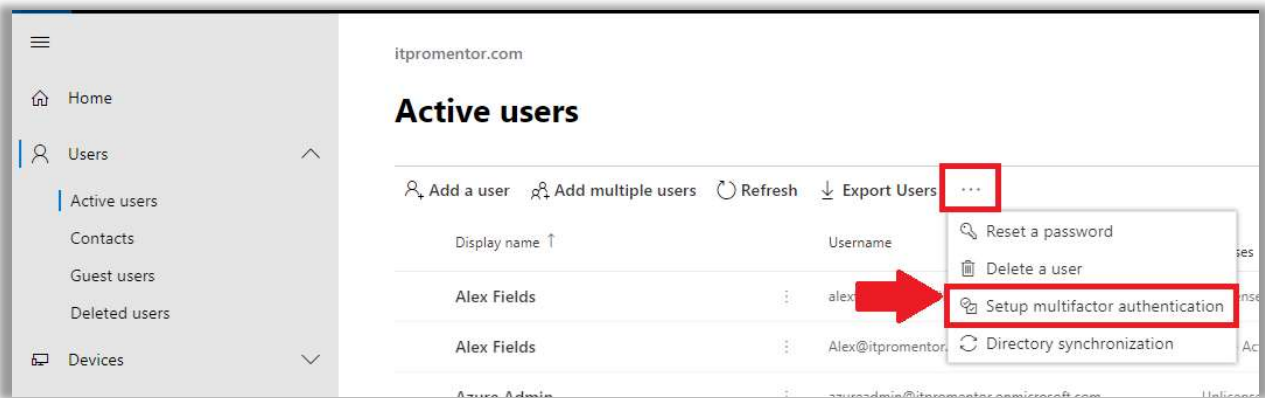
Enabling Multi-factor Authentication (MFA)

Multi-factor authentication (MFA) is any combination of two or more authentication mechanisms:

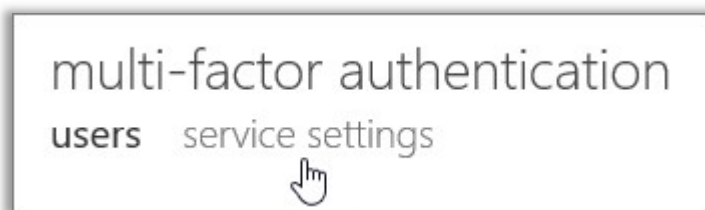
- Something you **know** (e.g. PIN, password)
- Something you **have** (e.g. physical security key, device or token)
- Something you **are** (e.g. biometric such as fingerprint or facial recognition)

MFA is now considered non-negotiable by many researchers and security experts, and it is one of the best security features available with your Microsoft 365 Business subscription, so you should definitely take advantage of it. The problem is, passwords just aren't that secure. And our attempts to make them more secure by imposing complexity requirements—remembered history and so on—have actually made matters worse. Therefore, the [new wisdom](#) says to implement MFA.

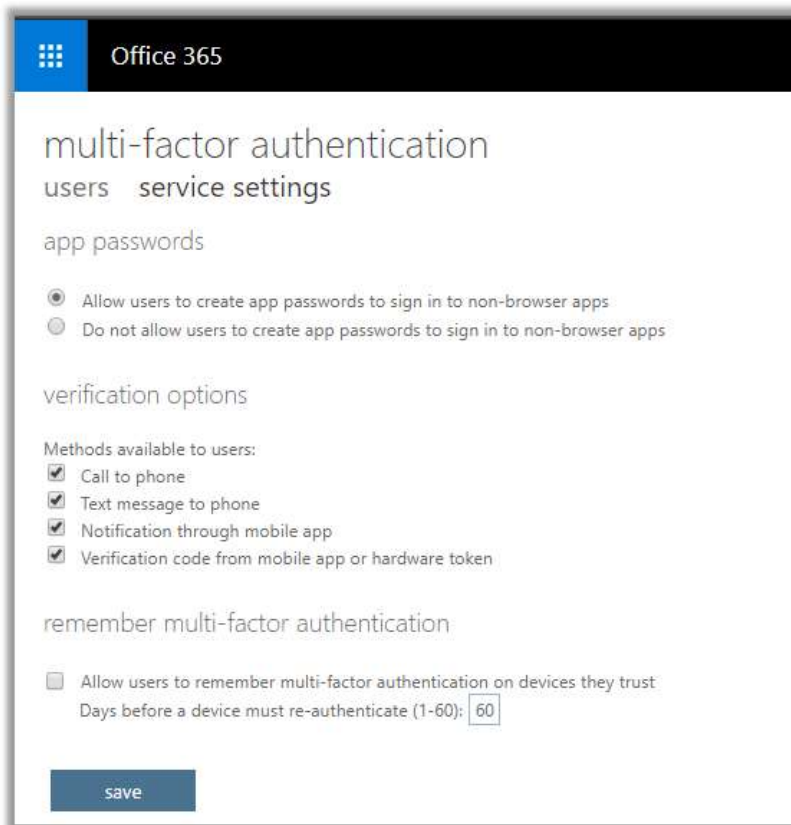
From the **Active users** area within the Microsoft 365 Admin center, and without selecting any users, click the **ellipses** at the top and then pick **Setup multifactor authentication**.



You can see your users listed here, but before you enable MFA for anyone in particular, check out the **service settings** area.



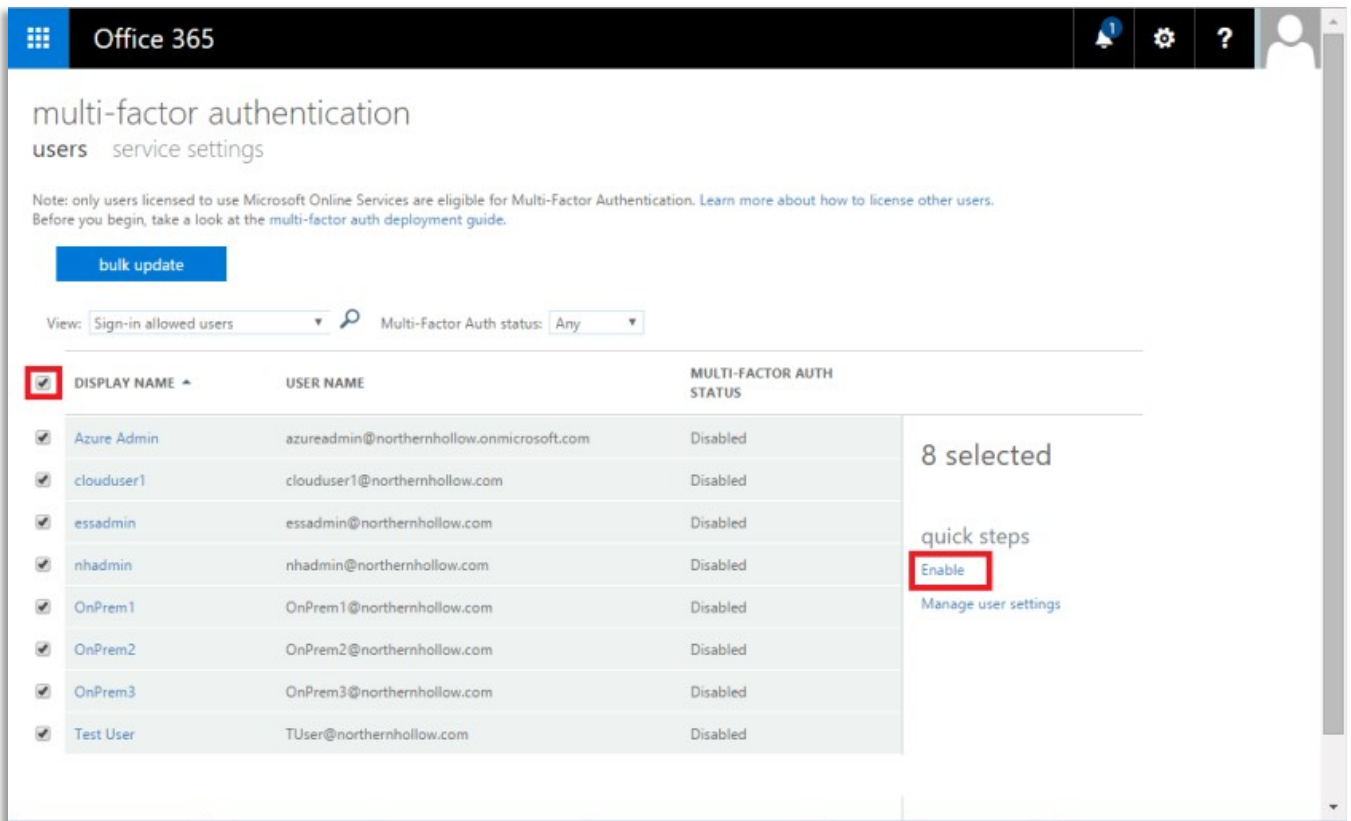
Here you can select various options surrounding the use of MFA, such as allowing certain types of MFA challenges like phone calls, SMS, mobile app notifications, or hardware tokens. It is also where you allow or disallow users to generate app passwords (for applications that do not support a second factor prompt—e.g. older versions of Office apps, Apple Mail, etc.).



Notes:

- **App passwords**—these are on their way out the door; your users should be getting the latest applications and using Microsoft mobile apps such as Outlook for iOS and Android, so you should not need to worry about this too much. I won't cover it here, but you can find information about this online, if needed.
- **Verification options**—I find that the *Notification* and *Verification code...* options via the mobile app usually provide the best end-user experience. They are also considered a bit more secure than a phone call or text message by some security researchers.
- **Remember multi-factor authentication**—For what it's worth, allowing remembered devices also presents risk of compromises in the event of loss/theft. Therefore, I usually recommend against it.
- **Trusted IP's** would be available here for Azure AD Premium users. This feature allows users to bypass MFA from known/trusted IP addresses such as corporate offices.

Once you are all set, you can enable your accounts back on the **Users** page.



Simply select as many of the users as you like and choose **Enable** on the right. You also have the option to use the **bulk update** button at the top of this page, providing a CSV file which is formatted as follows:

| | A | B |
|---|-------------------|------------|
| 1 | Username | MFA Status |
| 2 | chris@contoso.com | Enabled |
| 3 | ben@contoso.com | Disabled |
| 4 | kyle@contoso.com | Disabled |
| 5 | kenny@contoso.com | Enabled |
| 6 | eric@contoso.com | Enabled |

Notice that when you choose one or more of the users from this area, you also have an option to **Manage user settings**. These are self-explanatory:

- Require selected users to provide contact methods again
- Delete all existing app passwords generated by the selected users
- Restore multi-factor authentication on all remembered devices

It is recommended to provide users some instructional links in advance, so they know what to expect. For example:

[Setup 2-step verification for Office 365](#) (describes the classic MFA registration experience)

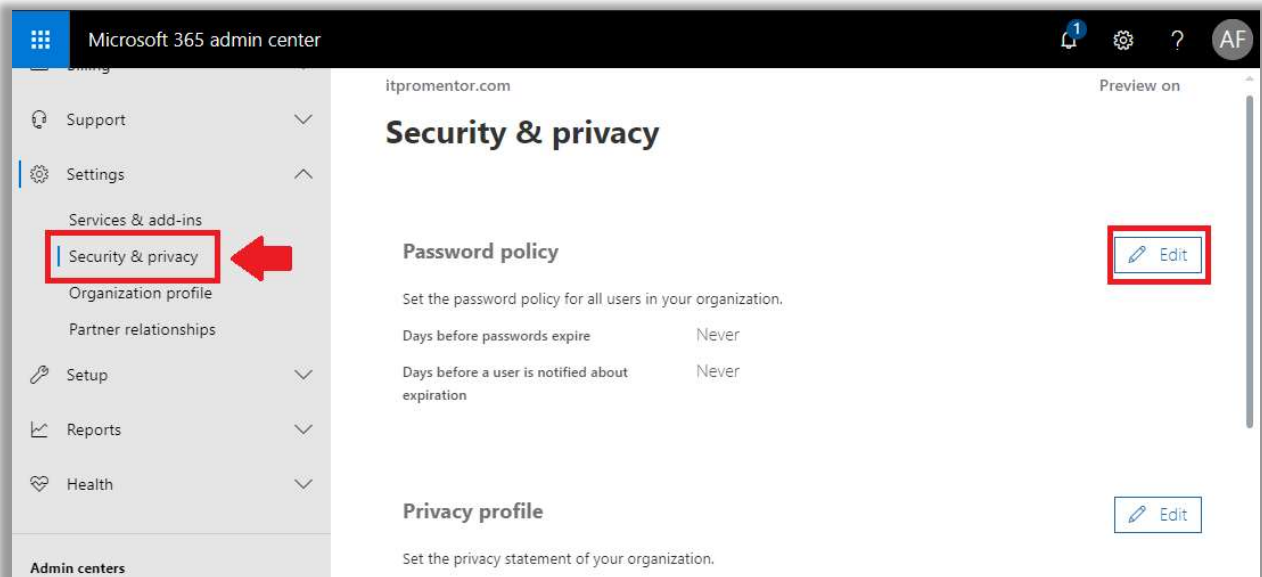
<https://aka.ms/authappstart> (configure the Microsoft Authenticator app)

They should be prompted to setup MFA authentication mechanisms upon next login, but it is also possible to visit the appropriate setup page manually with this link:

<https://aka.ms/mfasetup> (this is the classic MFA registration link)

Configure the password policy in the Microsoft 365 admin center

If you are successfully using MFA across the entire organization, then you should update your password policy. Navigate to **Settings > Security & Privacy** from the left menu of the Microsoft 365 admin center. In case it isn't already, you can set this policy to never expire passwords by clicking the **Edit** button. This is per Microsoft's new password guidance. If at any point you have reason to believe an account is at risk, then you can perform a password reset. More on this later.

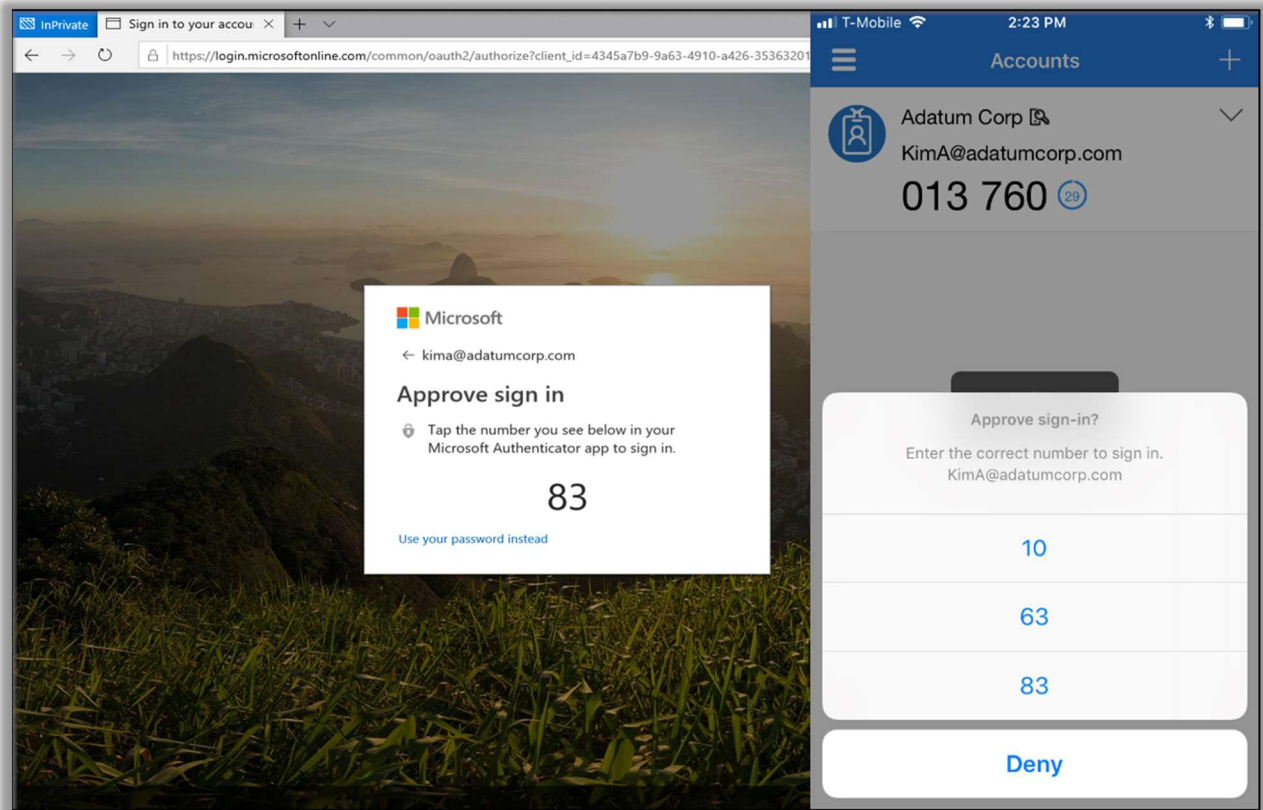


Passwordless sign-in

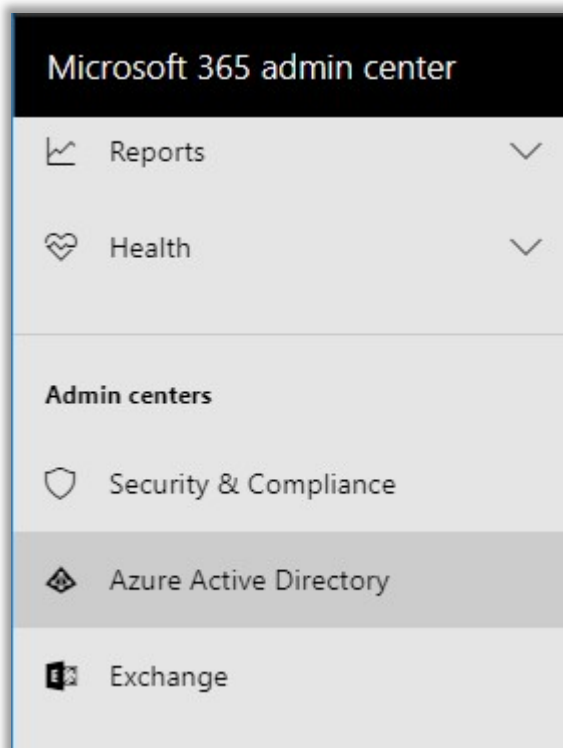
Another new feature that is in preview at the time of this writing is *Passwordless sign-in*. Building on the foundation of Multi-factor Authentication, Microsoft is hard at work to eliminate passwords altogether. Passwordless sign-in makes it possible to use MFA mechanisms in place of passwords, rather than in addition to them.

Right now, this method is only supported with the Microsoft Authenticator app for iOS and Android. Soon, however, Microsoft will add support for FIDO2 hardware devices and Windows Hello. This is already available with [Microsoft accounts](#) for the consumer (e.g Live ID's, non-Work or School accounts).

I wouldn't recommend jumping on board this bandwagon just yet. Give it time. For more information on configuring this feature in a lab, visit [Microsoft's documentation site](#).



Explore the Azure AD Admin Center



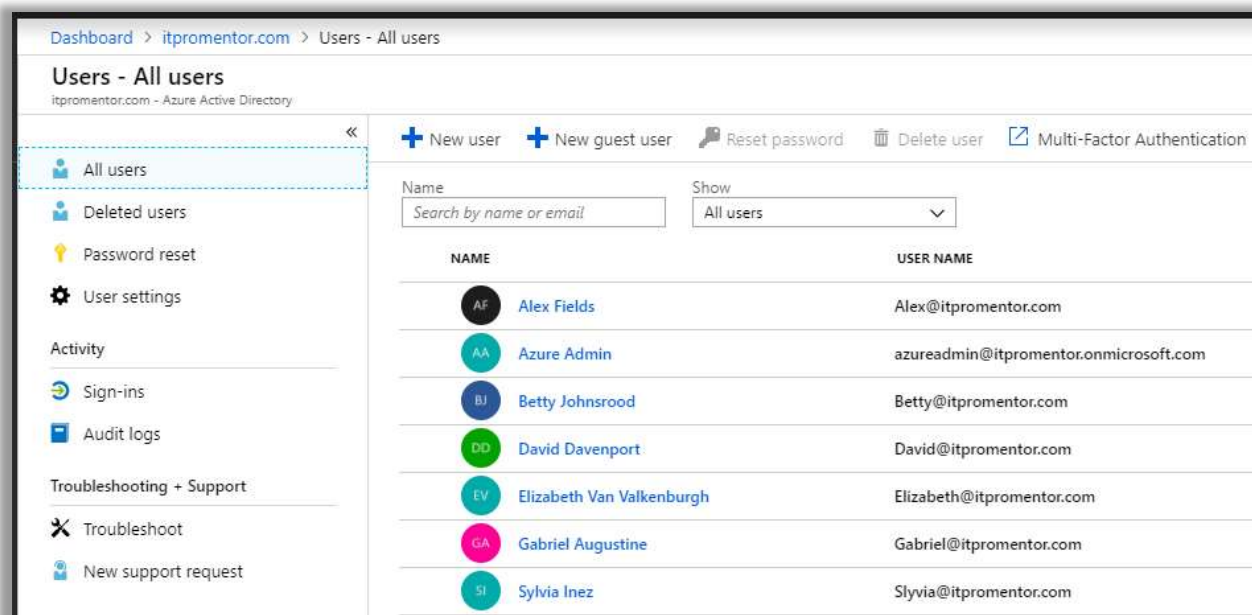
Even though most of us will probably be managing users and groups through the Microsoft 365 admin portal (<https://admin.microsoft.com>), I will actually ask you to poke around in the Azure Active Directory admin center. There is much of importance to see here—and we won't even be able to cover it all in this guide, but I do want to highlight a *few* things.

In the Microsoft 365 admin portal, from the left navigation, you may have to click on **Show more...** then scroll down to find **Admin centers** > **Azure Active Directory**.

It is also possible to navigate to Azure AD from the Azure portal itself: <https://portal.azure.com>.

Either way, you will be able to click on Azure Active Directory, to see the various options that are available to you. The first one we will look at is the **Users** > **All users** blade.

Managing Users in Azure AD



From the **All users** blade, you can find a listing of all the users in your tenant, and it will also indicate in one of the columns the *source* of the identity.

These are the possible identity sources:

Azure Active Directory - Users natively created in the Microsoft 365 or Azure AD admin center for your individual tenant. You create these in Azure AD by clicking **+ New User**.

Windows Server AD - Users who are synchronized from a traditional Windows Server-based Active Directory environment. Create new users of this type from the on-premises AD.

External Azure Active Directory - Users from other organizations that have Azure Active Directory and have been invited to share resources with your organization in some way (e.g. as an external user / guest participating in a Team or SharePoint library).

Microsoft account - External users *without* an Azure AD identity, but who nevertheless use another external identity such as a Gmail or a Microsoft Live ID to sign-in.

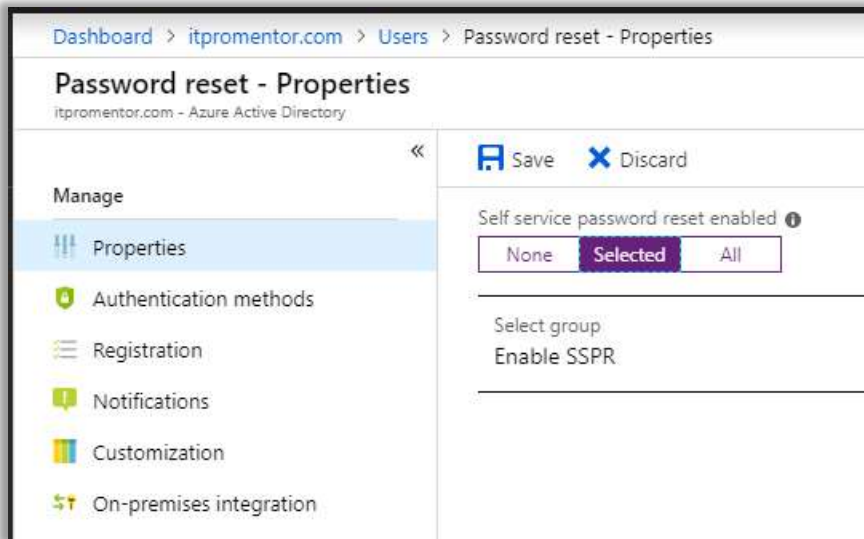
Invited User – External users to whom invitations have already been sent, but the user has not yet accepted the invitation. You can invite them using **+ New guest user** or from within apps such as Teams.

From the **All users** blade we can also find and restore **Deleted users accounts**, configure **Password reset** as well as edit **User settings**. For the purposes of this guide, we will cover *Password reset* in some detail, but I leave the other areas to your own exploration.

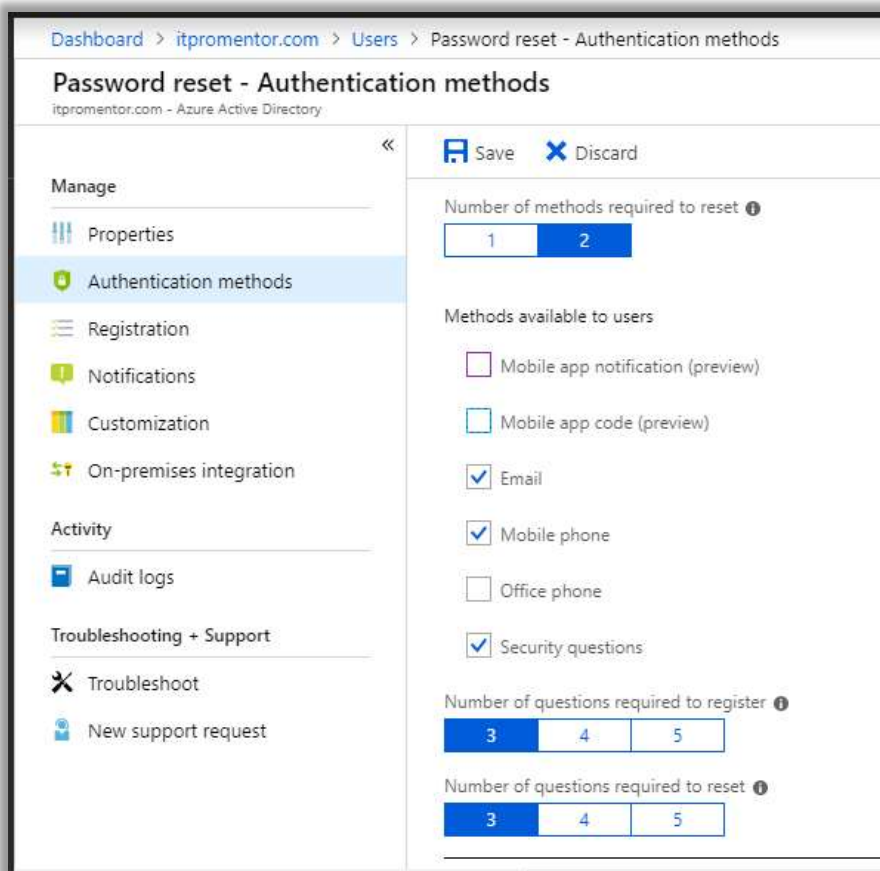
Password reset for cloud identities

Self-Service Password Reset (SSPR) is the ability for end-users to reset their own passwords in the cloud, without help from IT, by proving their identity using another factor of authentication.

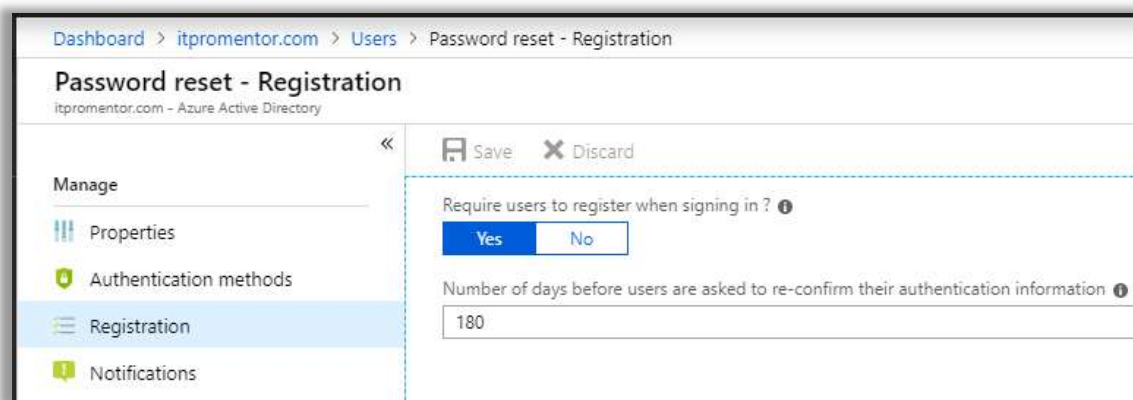
A very important point here is that SSPR is only supported using “cloud” identities by default. SSPR for *hybrid* identities would not be possible without the Azure AD Premium P1 add-on.



From the Azure AD Admin center, click on **Password reset**. The **Properties** blade is where you enable or disable the ability for users to self-service reset. Most small businesses will want this set to **All** so that every user can self-service reset. However, it is also possible to filter this using a Security group.

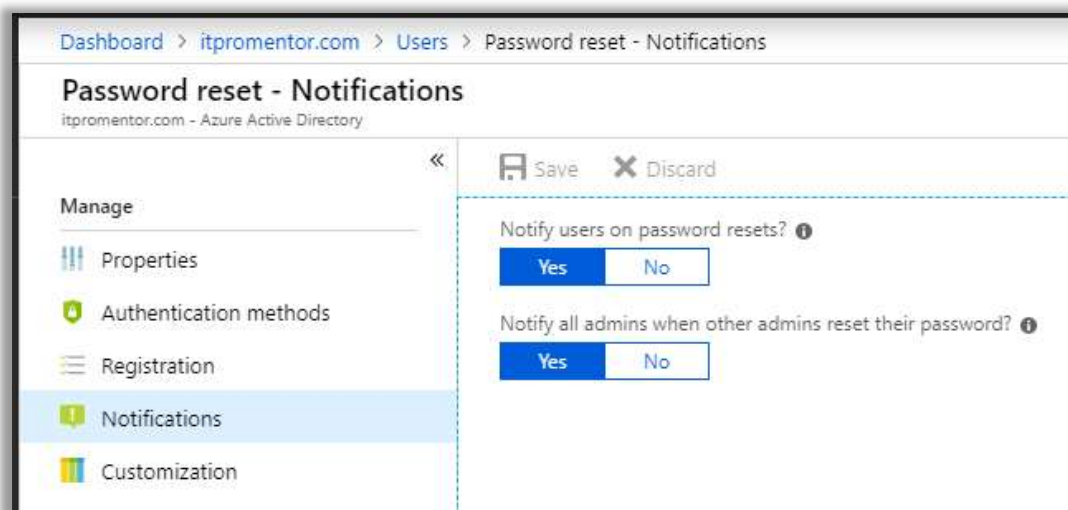


You also need to configure **Authentication methods**. It is recommended that you select at least two methods for enhanced security, e.g. mobile phone or app code, plus security questions.

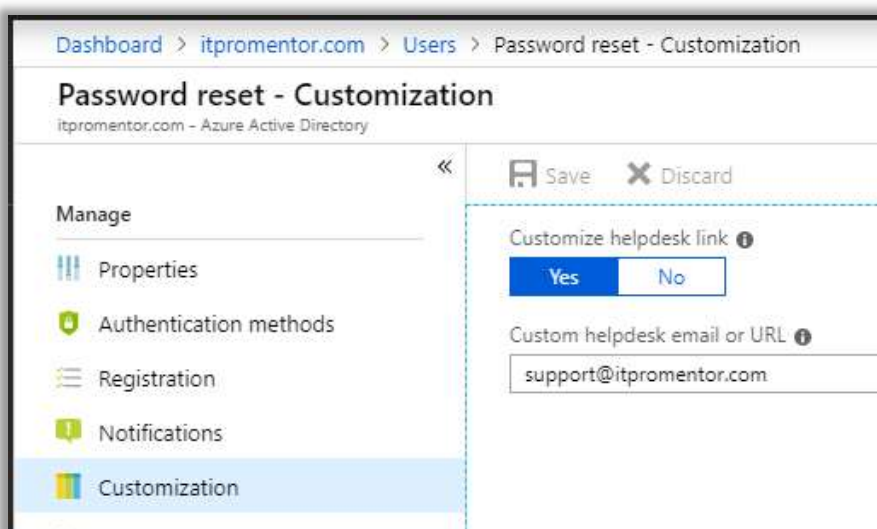


You can optionally force registration for self-service reset authentication on next logon from the **Registration** blade. If you did not choose this option it would be necessary to send users a link to the registration portal (<https://aka.ms/ssprsetup>) where they would register at their own leisure—which is often not at all—so I recommend that you just force the issue.

Next take a look at the **Notifications** blade. I recommend you turn both settings on, so that users and admins are notified when password changes happen in their accounts (and other admins get notified when any admin updates theirs). If the person in question did not initiate the change, then we know that we have a problem with that account.



Finally check out the **Customization** blade. Here you can insert your own custom helpdesk link so that in the event a user runs into an issue, a *Contact your administrator* link will lead them to your official support email address or web link.

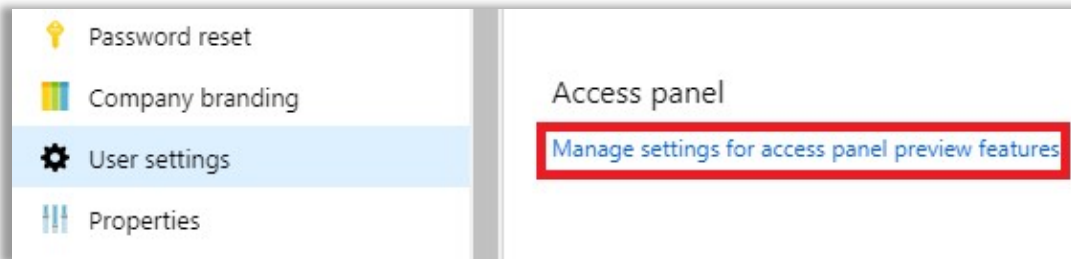


Later on in the hybrid section, I will also cover the **On-premises integration** blade, where we can enable password write-back to an on-premises AD environment. This requires Azure AD Connect and some custom permissions for the on-premises Active Directory.

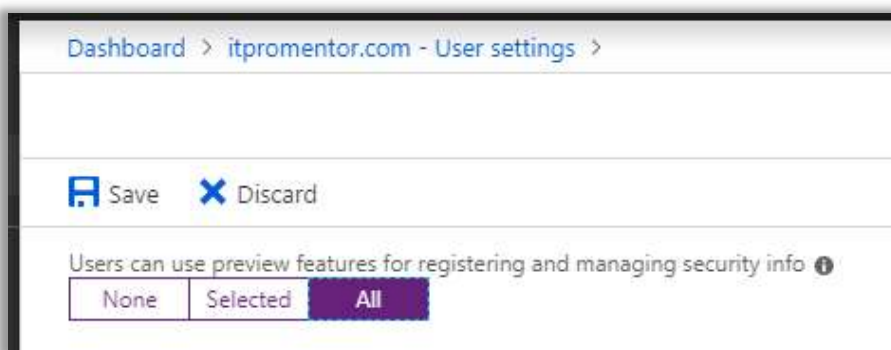
NOTE: at the time of this writing, there is a newer feature still in preview which allows us to offer a single experience for registration of self-service password reset and multi-factor authentication in one fell swoop. I'll cover that here, but the steps may change before it goes GA.

User enrollment in MFA and SSPR

Historically there have been two different registration experiences for multi-factor authentication and self-service password reset. Now you can have users register against both services at once.



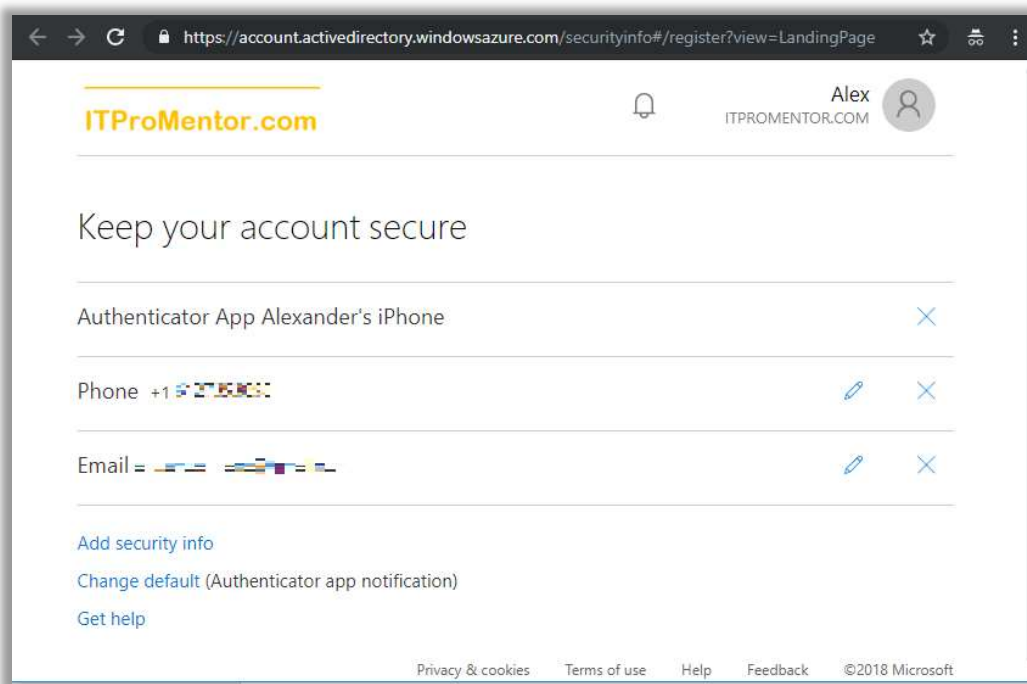
From Azure AD admin center scroll down to find **User settings > Access panel > Manage settings for access panel preview features**. You can enable for *All* or a *Selected* group of users.



If you enable this feature, and a user has previously setup MFA and SSPR separately, they do not need to register again. However, if they are required to update information for either, they may be prompted to update their security information.

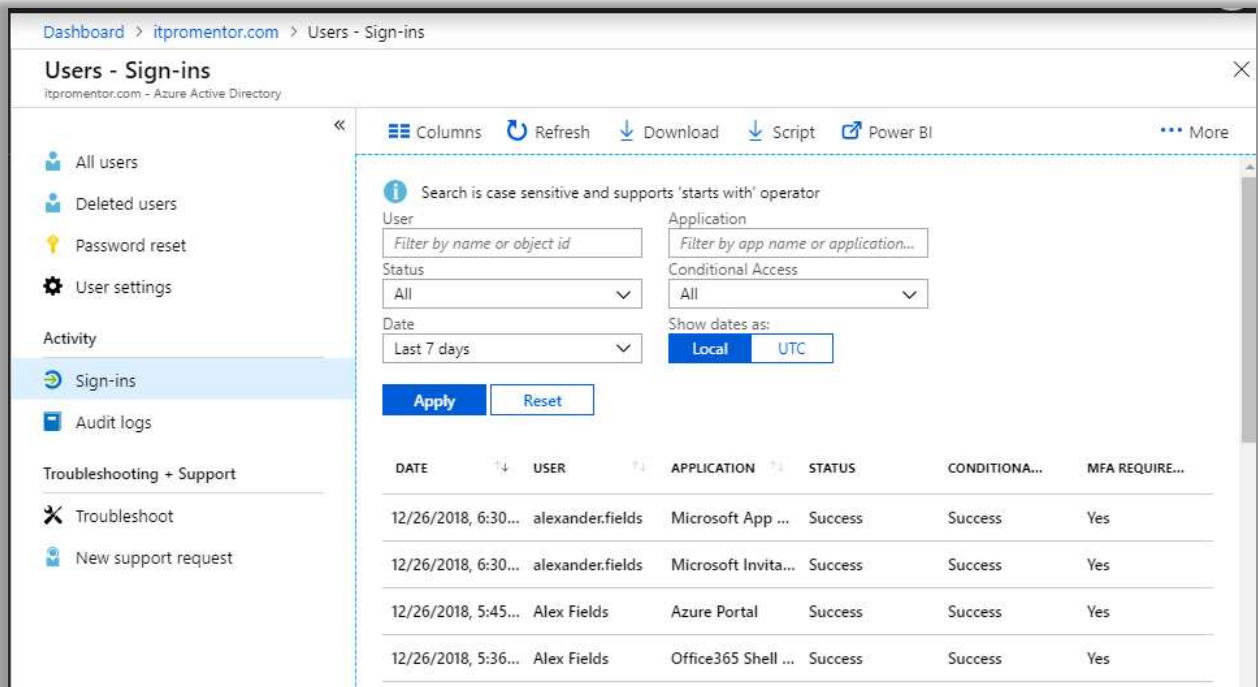
Alternately, you can send-users a link to self-register using the new method at this link:

<https://aka.ms/setupsecurityinfo>

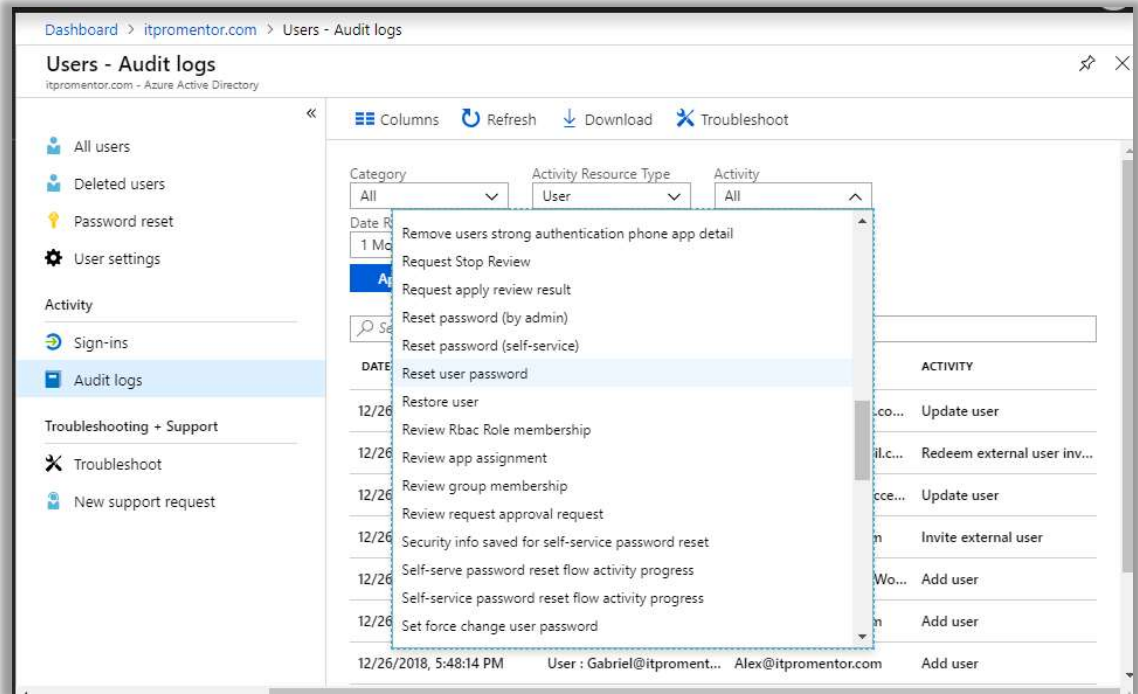


Activity Logs

Go back to **Users**, then under **Activity** > **Sign-ins** you will find a log of activities specifically having to do with authentication. It will tell you the user name, what application was accessed, whether the sign-in required MFA or fell under the scope of a conditional access policy, and of course whether the authentication attempt was successful or not.



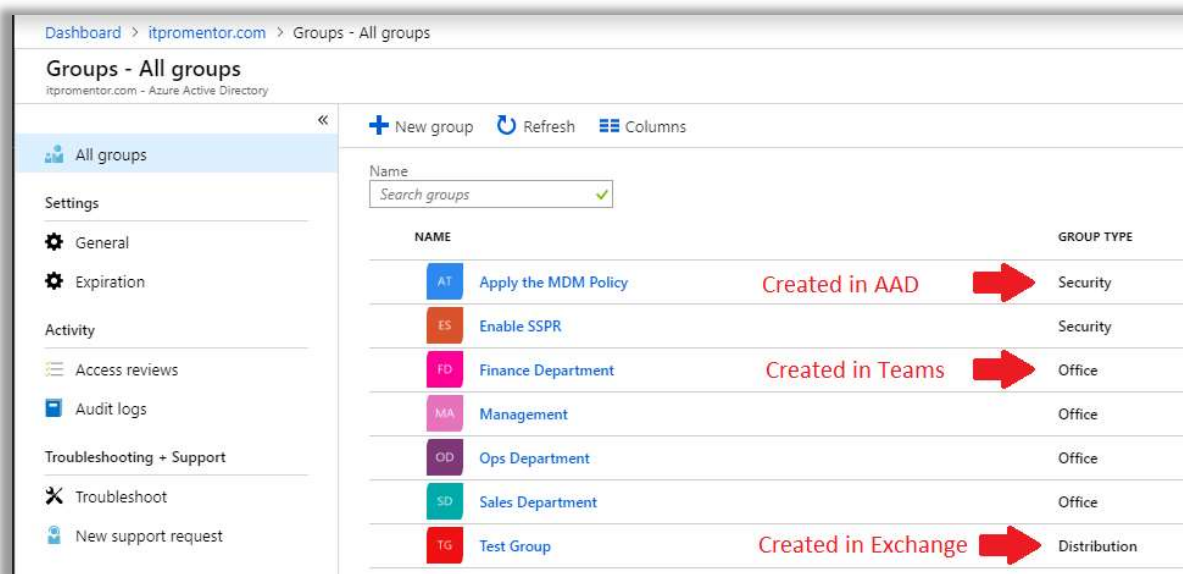
Audit logs are differentiated from Sign-ins. Audit logs contain information related to *any* changes going on within the tenant. Creation of new users, resetting of passwords, changing policies or settings—it's all in there. This is a very useful trove of data, as we will see later.



From the Security & Compliance Center, it is possible to setup “activity alerts” based on events in the audit log. But for now, just know that all types of events are logged and available here in Azure AD.

Groups

Go back to **Azure Active Directory** and click on **Groups > All Groups**. If you are synchronizing security and distribution group objects from your on-premises AD, then those will show in here as well.



In the image above, you can see there are various Group Types—*Security*, *Office* and *Distribution*.

From within the Azure AD Admin center, you can create either *Security* or *Office 365* groups. *Distribution* and *Mail enabled security* groups will also show up in here, although you cannot create them via the Azure AD admin center.

Office 365 Groups can be created from various places within Office 365 such as Microsoft Teams, and these groups are generally used to provide access to content in Office 365 apps.

Security Groups are typically generated by admins via the admin portal, or through synchronization with on-premises AD. Security Groups can be used to assign apps, or scope various policies such as device-based Intune policies, conditional access policies, or ATP policies.

Distribution Groups are used for email distribution, and can be created from the Exchange admin center, or the Microsoft 365 admin center.

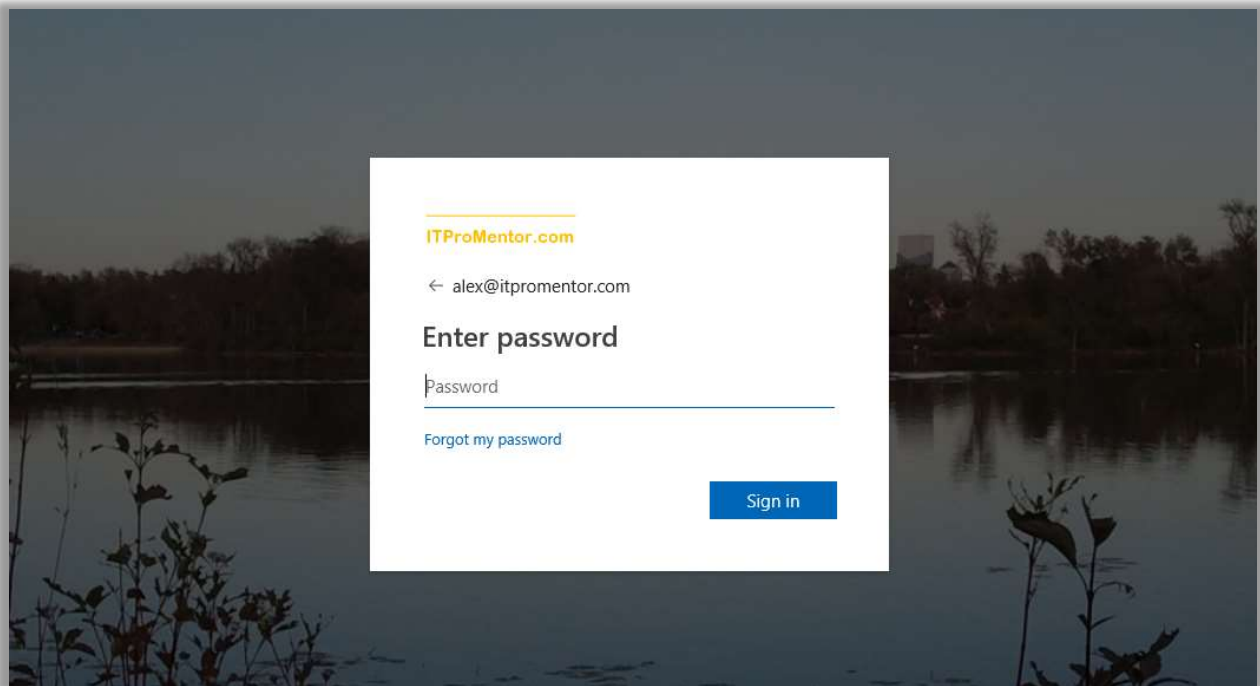
Mail enabled security groups are distribution lists that can also be used to grant access, like a security group. Usually these are synchronized Universal security groups from on-premises.

It is also worth noting that the **Membership Type** can show up as either *Assigned* (created in cloud) or *Synched* (from on-premises AD).

We will not cover the other **Settings** found under **All groups** at this time, but feel free to explore these options at your own leisure.

Configure Company branding

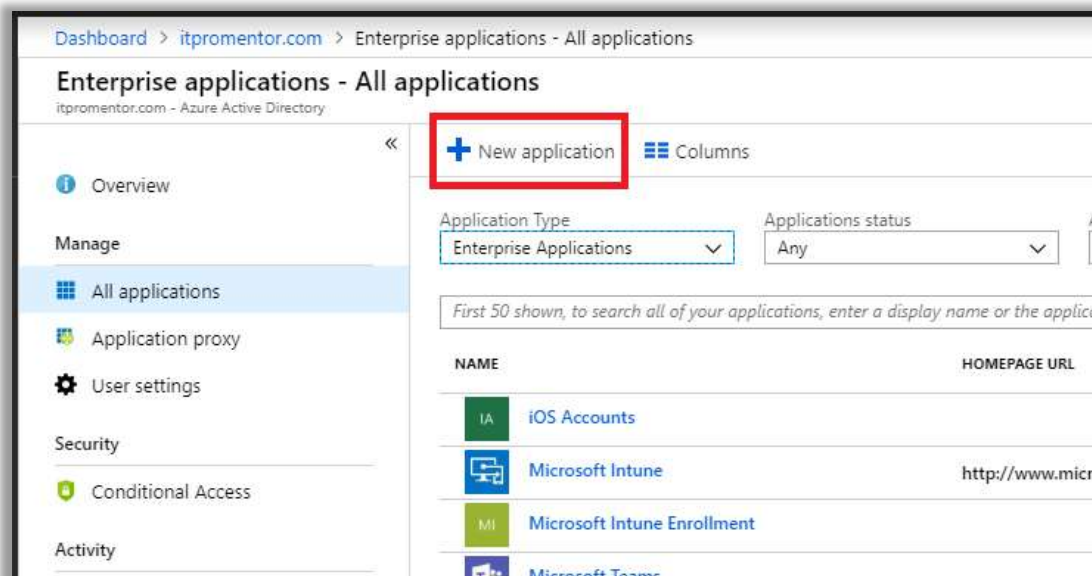
Go back to Azure Active Directory and scroll down to find the blade for **Company branding**. Click **Configure**. I won't go through all of the options here, but the first two are the most common: *background image* and *banner logo*. By way of example, in the image below, I have configured both. After making this change, the Azure AD sign-in page will feature the new branding.



The logo you upload here will flow through into some other areas (e.g. the access panel at myapps.microsoft.com), but it is *different* than the logo we uploaded previously to the Microsoft 365 admin center, and which is used on that top navigation bar as part of your “theme.” And neither of these logos will flow through to the branding for our encrypted emails—that is yet another *separate* configuration we will be detailing later on. I hope that Microsoft collapses these disparate areas into one single place someday.

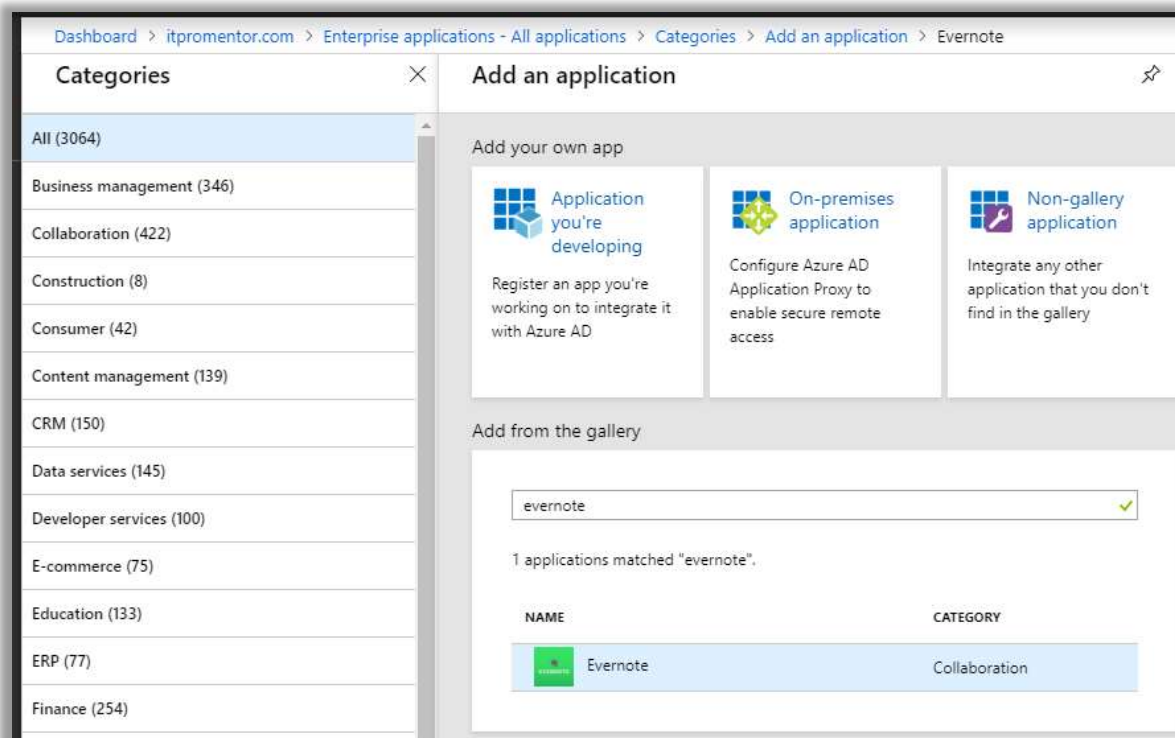
Configure the Azure AD application portal

Another feature of Azure Active Directory which nobody seems to talk about in the SMB space, is the ability to bring third-party SaaS applications under management, and assign them to end-users so that they can be accessed via an application portal (myapps.microsoft.com).

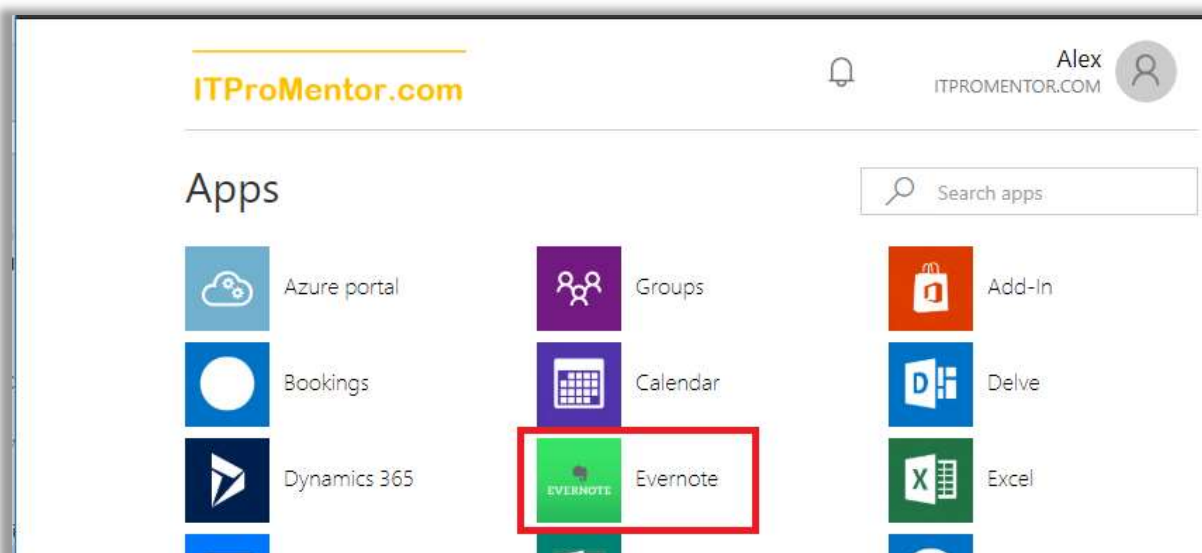


From Azure Active Directory, find **Enterprise Applications > All applications**. Click **New application**. There are a few thousand applications now available in the app gallery. You can search or browse by many different categories. If an application is not found here in the portal, then you can add custom (non-gallery) applications only with an Azure AD Premium P1 or P2 subscription.

By way of example only, I will search for and add an application from the Azure gallery—in this case *Evernote*. Next, I can assign the application to individual users.

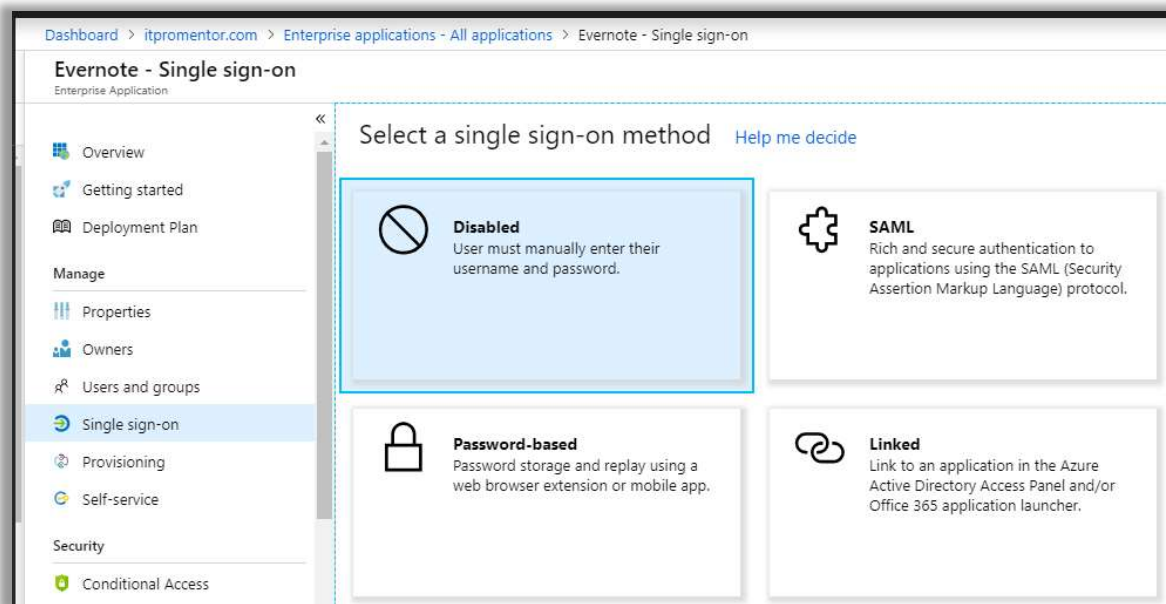


Once you have configured your apps and made your assignments, users will be able to access the application via the Azure AD access panel located at: <https://myapps.microsoft.com>.



Configure SSO to third-party applications

Find the **Single Sign-On** blade within the application. Not all applications will support "true" single sign-on (SSO), but almost any app will allow the user to store their credentials within the Azure AD portal (similar to LastPass, if you are familiar with that concept). The various SSO methods are depicted in the following screenshot.

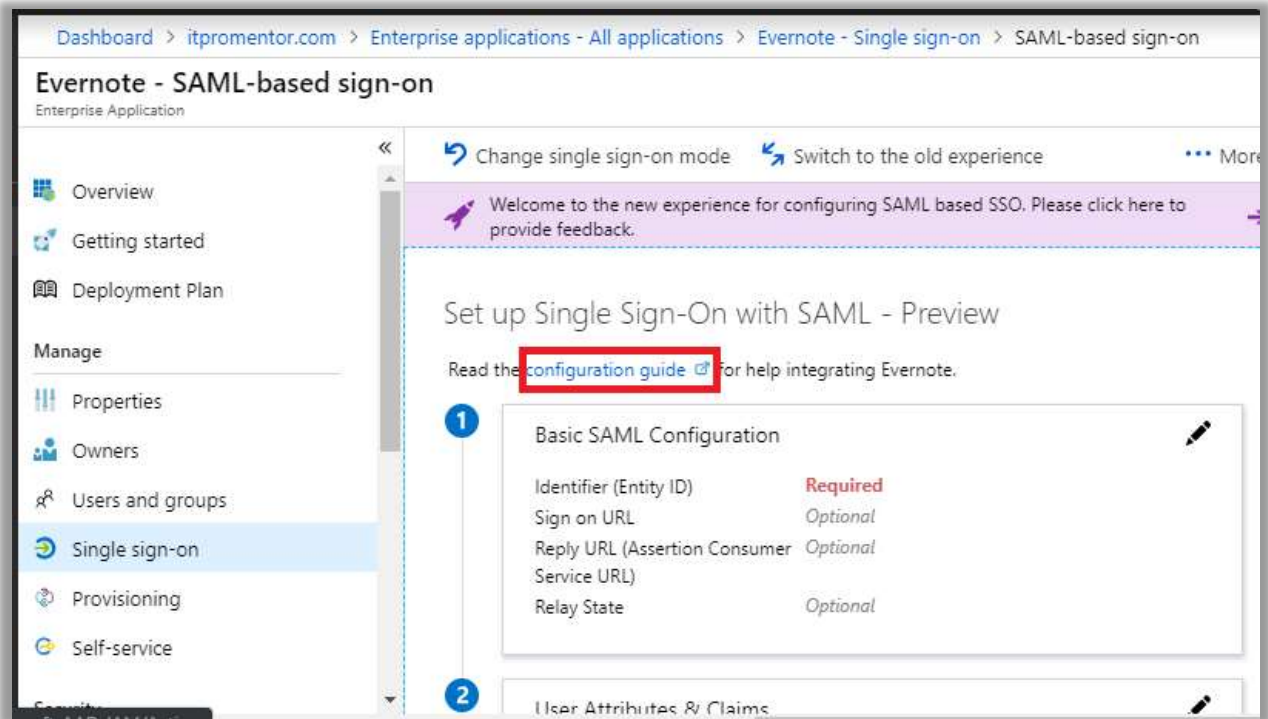


- **Disabled** – Just like it says, essentially this will just make the application tile available in the app portal, but there is no SSO experience. The end-user would need to provide their unique log-on ID and password for that app in order to log in, every time they click the tile.
- **SAML** – If the app supports SAML (Security Assertion Markup Language), this is what you want. SAML provides “true” SSO, where Azure AD becomes the app’s Identity Provider, and all authentication requests are logged against Azure AD—whether they come in via the app portal, or not. This is the most secure option and recommended wherever possible.
- **Password-based** – Otherwise, if the app does not support SAML but still uses some type of username/password, then you can choose “password-based” SSO. This option simply stores credentials in Azure AD, and replays them into the third-party app on demand, to give the user an “SSO-like” experience (without being *true* single sign-on). The user can input and update their own password, or it can be managed by an administrator, and the user doesn’t have to know the password at all.
- **Linked** – You would use this option if you already had an application linked via another Identity Provider. You may choose this option if you are slowly migrating from another identity service such as Okta or AD FS, for instance, and wanted to publish links via the new portal before you switched them over to SAML.

*Note: if you are able to implement SAML, that will also open up other options within the **Provisioning** and **Self-service** blades, where users may be allowed to request access and provision their own accounts, for example. Plus, you don't have to use the app portal at all with SAML—logging in at the third-party app will automatically redirect the authentication to Azure AD.*

I will not go into the full details of setting up a SAML-based SSO experience, but I do want to give you some guidance to get started. The security benefits are just too great to ignore, since you can reduce the number of identities you manage and centralize the security logs in Azure AD. None of this is that hard to do, so don't be afraid of it.

Every app is a little bit different in terms of its deployment, although they all have similarities. Here are some basic guidelines I can give you: Microsoft links to a **configuration guide** for many common gallery applications.



In almost all cases where SAML is available, you will need to provide Azure AD and the third-party application portal with some URLs, certificates and/or XML files, so that each side can understand and talk with the other. Note that sometimes certain entries are optional. Microsoft and/or third-party vendors will likely have support documentation available, as pictured here in the case of Evernote.

Input the URLs and other details about your Evernote tenant into Azure AD.

* Identifier

In the Identifier textbox, type the URL:

4. Check **Show advanced URL settings** and perform the following step if you wish to configure the application in SP initiated mode:

Show advanced URL settings

Sign on URL

In the Sign on URL textbox, type the URL:

5. On the **SAML Signing Certificate** section, click **Certificate(Base64)** and then save the

It is difficult to express just how important this Enterprise Application feature could be for your organization or practice. Even if you cannot configure true SSO with SAML to every one of your applications, just the fact that you can *track* application assignments to users alone is huge. Most small organizations have no software inventory to speak of. Which is too bad, because it is often required to have an inventory for various compliance bodies out there.

Poor inventory means blind spots; blind spots mean weak protections. Weak protections are one of the primary reasons why SME's are still the most vulnerable targets out there. From the point of view of an attacker, the average security posture for small businesses out in the wild looks a lot like Swiss cheese—and it has gotten worse with the addition of so many SaaS products in the last few years.

Bottom line: you cannot protect what you don't even know you have. Once you *know* what you have, then you can start taking steps to better protect it—SAML, MFA, Conditional access, limiting privilege, etc., etc. But it all begins with knowing, taking stock of what you've got.

Microsoft 365 can help you wrap your arms around this whole cloudy mess: identities, applications, devices, *and* data. Additionally, with the option for SSO in many cases, this corporate access panel solves a big piece of the puzzle—so make it a point to start bringing your applications into the fold!

Hybrid support in Microsoft 365 Business

Although Microsoft 365 Business now officially supports a hybrid infrastructure, this was not the case when the product first launched. Hybrid—the ability to work with the same identities for both traditional on-premises servers and new cloud-based services—was a feature initially reserved for the Enterprise SKUs.

Hybrid is enabled through a tool called Azure AD Connect, which establishes a relationship between a traditional on-premises Active Directory and Azure Active Directory in the cloud, including Single Sign-On (SSO) and password hash synchronization, among other things.

The idea here was that large enterprise organizations would need more time and tools to transition into a cloud-based identity management platform, whereas small businesses would be able to jump off more quickly, and would be more likely to choose mobile-first, cloud-first solutions, ditching traditional Windows Server infrastructure altogether.

In practice, the initial limitations surrounding hybrid prevented widespread adoption of the Business SKU, since the transition to a completely cloud-based environment does not happen overnight—even for small-sized enterprises! Sure, it's okay for “born in the cloud” start-ups, but for established businesses it can be much more difficult to leap into a completely untethered environment, just like that.

However, in the spring of 2018 Microsoft finally [announced official hybrid support](#) for Microsoft 365 Business—and this made it much easier for SMB/SME customers to adopt the new SKU. Nevertheless, it is important to remember that Microsoft's fundamental stance toward hybrid in the small business space is this: Windows Server products are on their way out the door within the next few years for the SME, and therefore you should leverage hybrid as a temporary solution *only*, in your transition to a 100% cloud-based computing model.

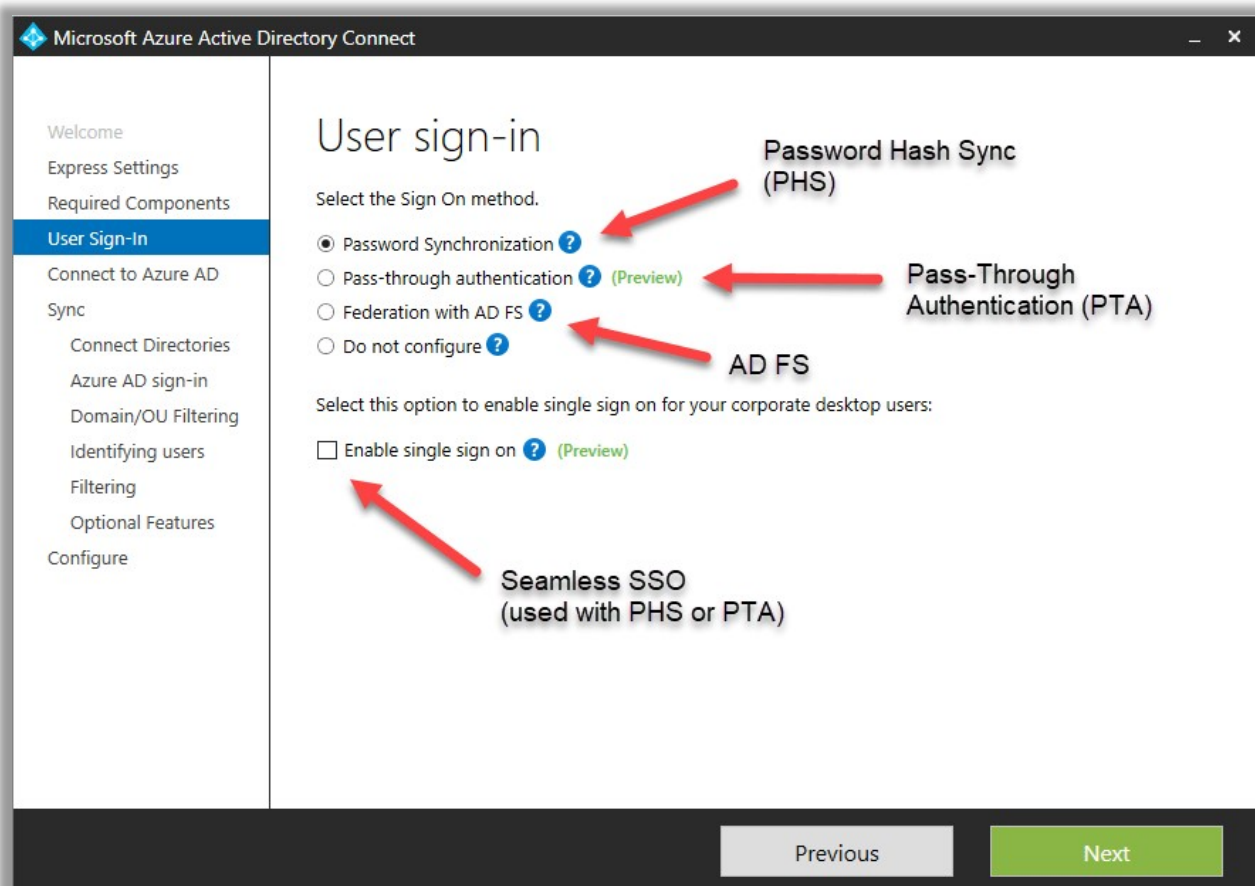
This is to be contrasted with the Microsoft 365 *Enterprise* SKUs (E3 and E5), which are designed to support hybrid infrastructures long-term. We will NOT be covering the Enterprise bundles here—just know that many of the additional features are there to support hybrid, and to bring the power of cloud computing into the Enterprise datacenter.

Understanding User Sign-in options

Before you install Azure AD Connect you should gain an understanding of the various *user sign-in* options that are available. There are three primary methods we can use to enable single sign-in:

- Password Hash Synchronization (PHS) with Seamless SSO
- Pass-Through Authentication (PTA) with Seamless SSO
- Active Directory Federated Services (AD FS)

I am going to start with the last option, which was, in fact, the original. Many early adopters of the Office 365 platform ended up with this type of configuration.



Active Directory Federated Services (AD FS)

With AD FS, you need to deploy an on-premises service called Active Directory Federated Services, and it's best if you make this service highly available. In this configuration, passwords never leave the on-premises Active Directory. When someone attempts to sign in to the Azure AD application, there is a configuration bit in the tenant that says, "I'm not in charge of authentication, I have to go check in with <insert corporate AD FS web address here>."

This is super cool for security and compliance, because all authentication attempts are still logged against the local Active Directory. But it is super *un*-cool for many small businesses, because it requires setup and installation of AD FS, which also means that the cloud-based applications are dependent on the local Active Directory.

So, if the corporate internet connection is down, your email is down too. Wait a minute...why did we move our email to the cloud again? To prevent this scenario, our design would need to include:

- Properly configured AD FS infrastructure with SSL Certificates
- At least 2x AD FS web servers on separate links/ISP's for HA
- Planned recovery from total loss of this site/infrastructure

AD FS is not a popular option for these reasons (complexity + dependency).

Pass-Through Authentication with Seamless SSO

Pass Through Authentication or PTA is the simplified cousin of AD FS. Like AD FS, it means that all logins rely on the local Active Directory for authentication and sign-in—we still have that same annoying dependency. However, because the cloud authentication takes place via the local Azure AD Connect service and does not require a complex AD FS server infrastructure or SSL certificates, it might be preferred in some scenarios.

You would still want the redundancy/high availability, but there are no additional requirements. Therefore, if you are faced with the challenge of keeping passwords and authentication events on-premises, and the customer also wants to keep the complexity down with a lighter on-premises footprint, then PTA is your best option (be sure to also enable SSO in the AAD Connect configuration wizard when choosing this option).

Password Hash Sync with Seamless SSO

This last configuration is the most common, and the one I recommend for most small businesses. In this model, there is no on-premises dependency. Via password hash synchronization, the local AD passwords are salted, hashed, and synchronized to Azure AD.

Additionally, you can enable the Seamless Single Sign-On option, and corporate desktop will have the same SSO benefits (there will not be further credential prompts to use Outlook, OWA, other apps, etc.). The best part? If your local on-premises systems or internet connection is down, users can continue working in their cloud apps, without noticing.

Prepare for Azure AD Connect

Let's say your on-premises domain name is **companyname.local**—that means users probably sign in with something like [username@companyname.local](#), or `company.local\username`. Unfortunately, these identities are meaningless in Azure AD.

In the cloud, we have to ensure that your users can sign-in using their email address as the username, e.g. [username@companyname.com](#). To get these disparate identities matching one another, we might have some adjustments to make. Don't worry—most of the time they are painless.

Microsoft's recommendation is to ensure that your entire UPN logon name (prefix and suffix) be setup to match the email address *before* configuring hybrid identity via Azure AD Connect.

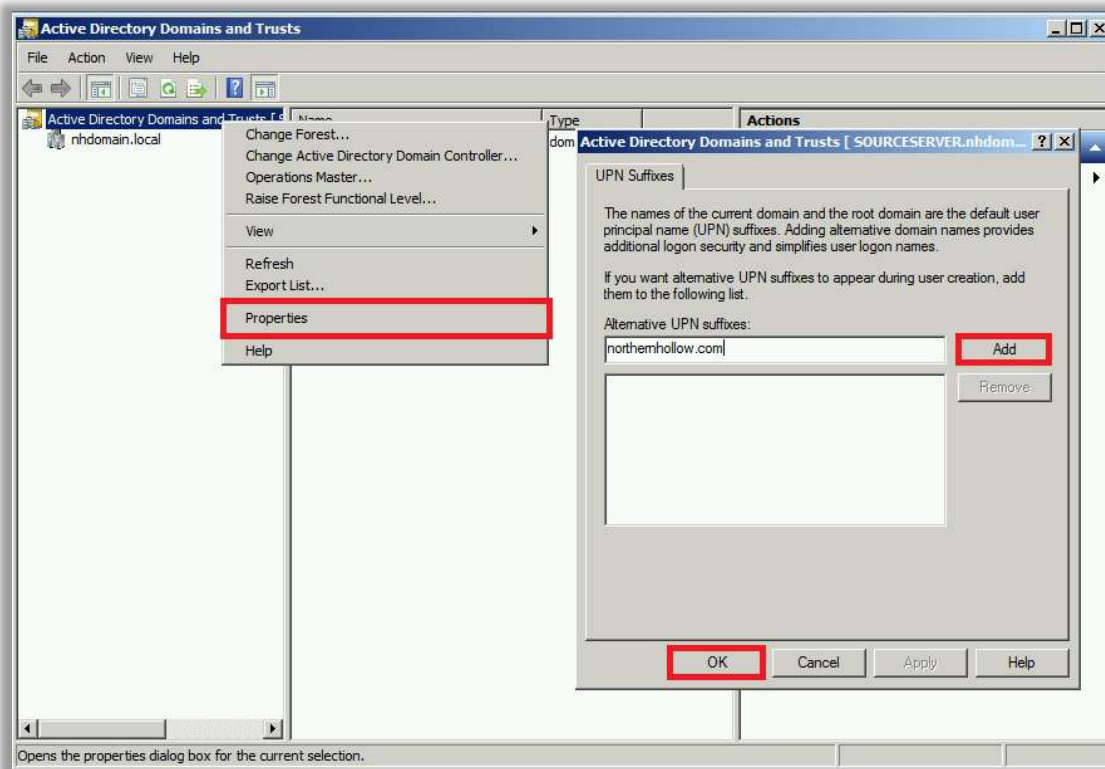
Adjusting the suffix from, say, a *.local* address to an internet-routable *.com* or *.org* address is very easy, and has no impact on user sign-in experiences. So, we'll start there, and discuss the UPN *prefix* afterward.

Adjusting the UPN suffix

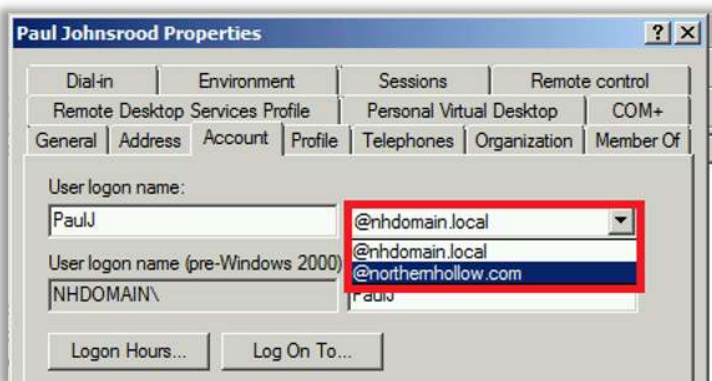
Be sure that you have already verified your custom or "vanity" domains in the Microsoft 365 admin portal, and that you have the UPN suffixes for these domains available and assigned to your users on-premises. We have already covered adding custom domains in the introductory section of this guide.

Now, to add UPN suffixes on-premises, open the **AD Domains and Trusts** Microsoft management console, and then right-click **Active Directory Domains and Trusts** at the root of

the tree, and select **Properties**. If it isn't already listed in here, then enter your external email domain name(s) and click **Add**. Click **OK**.



The reason you do this is so that you can assign users the UPN suffix that matches their primary email domain name. In **Active Directory Users and Computers**, check the **Properties/Account** tab on your user objects. Note: It is possible to bulk-select users and edit the suffix field en masse.



Performing the UPN suffix switch will have no impact on end-user sign-in, except that they could (if they wanted) start signing in with [username@emaildomainname.com](#) instead of domain\username (though both will continue to work).

Adjusting the UPN prefix

Now, if your on-premises users have a sign-in name like: [BobSmith@domain.com](#) or domain\BobSmith, but their email address looks more like: [BSmith@domain.com](#), then you

should change the UPN attribute on-premises to match the email address. *BobSmith* should become *BSmith*.

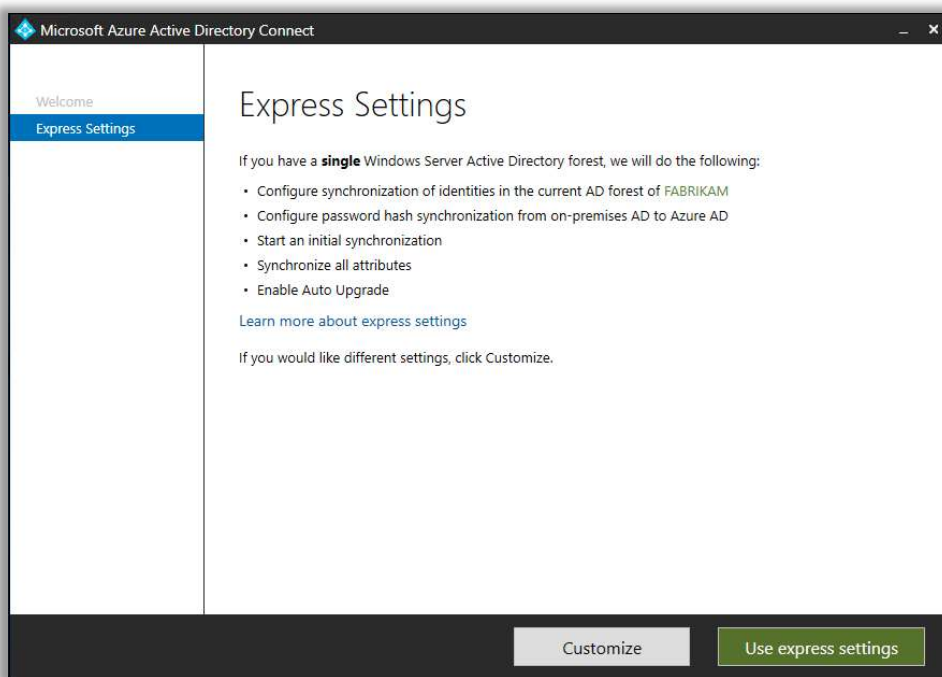
If the values already match, then you should be good to go without making any further changes. But if they don't match, then this change is going to impact on-premises sign-in experiences, obviously. Therefore, you will need to communicate this change in advance, so that users are aware of when they need to start signing in to the domain using their email address instead of the legacy format.

Again, it is possible to get around this using an "alternate ID"—something other than the UPN attribute—but Microsoft recommends against it, and encourages us to make the UPN match instead.

Glad that's out of the way! Now we should be ready to install Azure AD Connect.

Installing Azure AD Connect

You can install Azure AD Connect on either a Domain Controller, or a Member server within your on-premises environment. Note that Windows Small Business Server (SBS) and Windows Server Essentials (WSE) are not officially supported. Therefore, use a separate member server in these environments.



In case it isn't obvious yet, I am about to cover a step-by-step, screen-by-screen setup of Azure AD Connect. I waffled on whether or not to include this, or instead just slap down some links to Microsoft's own documentation, but ultimately I decided that I should include it. So here's the thing:

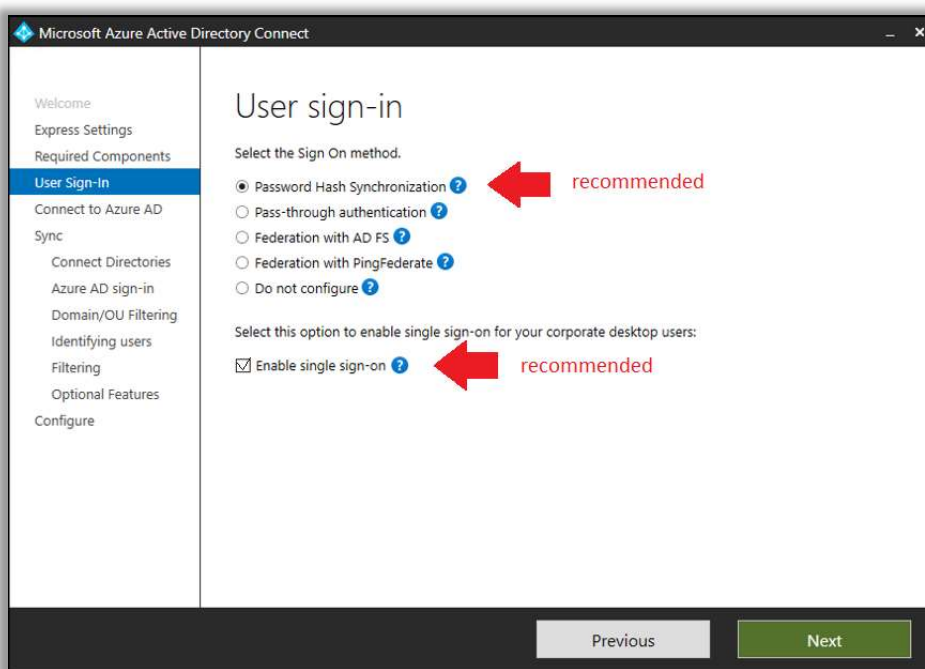
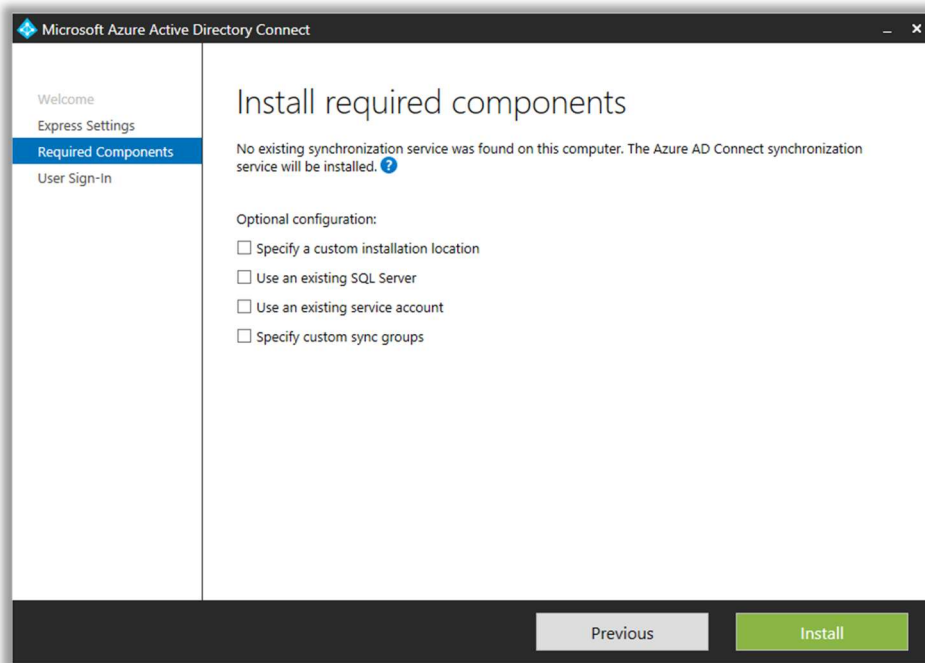
1. If your UPNs already match the email addresses, you *could* just opt for the "[Express Settings](#)" option, which takes out a lot of the guesswork and makes this process a bit quicker. The express settings will just sync *everything* from the directory, with UPN as the

logon name, and password hash sync for sign-on. So very vanilla—nothing wrong with that.

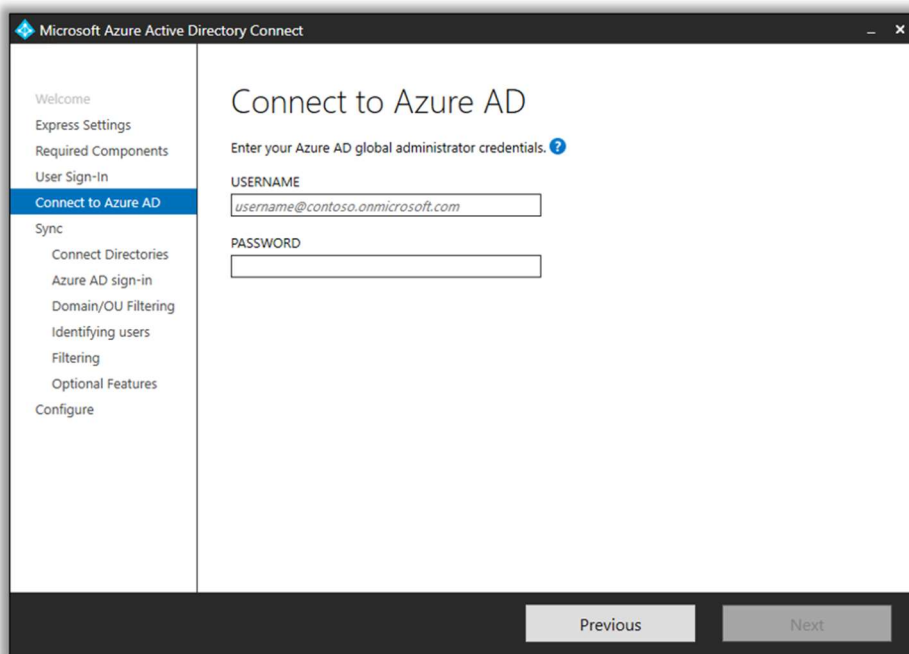
2. However, there is value in the option to “*Customize*.” For example, I generally recommend that you constrain the number of objects syncing to Azure AD; I sync only active accounts for users and shared mailboxes, leaving any service accounts or disabled users out of the mix. To do that, you need to pick *Customize*. If you could not (or would not) setup the matching UPN as I described above, then you will have to go this route anyway.

In the instructions that follow, I will keep it vanilla as possible, with Password Hash Sync, etc., but I’ll recommend that you use OU or group filtering to limit the synced objects. If you want something different, such as PTA or otherwise, check out Microsoft’s guidance on a [Custom install](#) of Azure AD Connect instead.

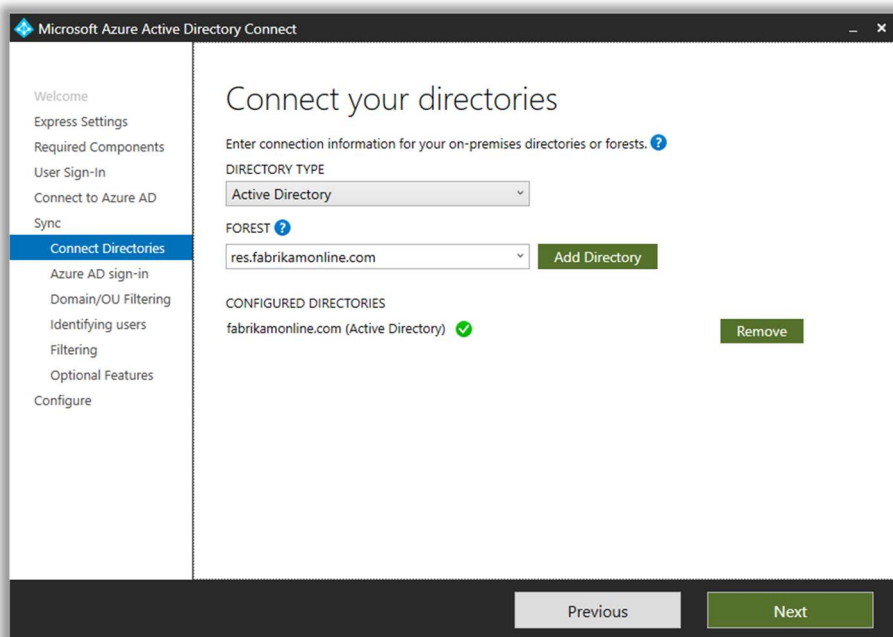
To get started, Download the latest version of the Azure AD Connect tool from Microsoft and launch the MSI. Accept the terms, and on the **Express Settings** screen, click **Customize**. You can choose to change certain settings here, such as install location, SQL instance, and service accounts, but I usually just pick **Install**, with the default selections.



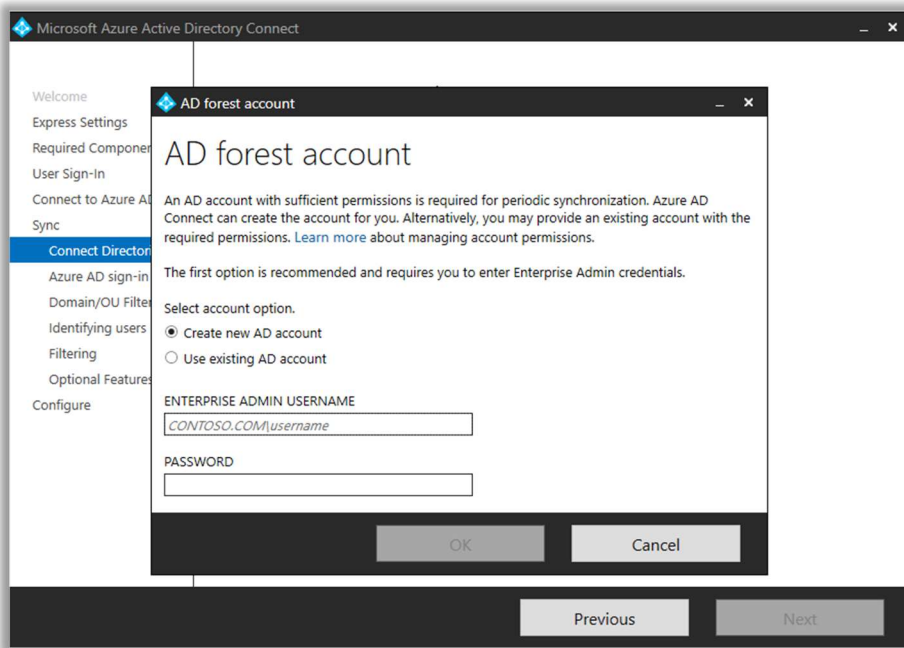
You are free to make your own decisions, of course, but I recommend **Password Hash Synchronization** and **Enable single sign-on** (Seamless SSO). Click **Next**.



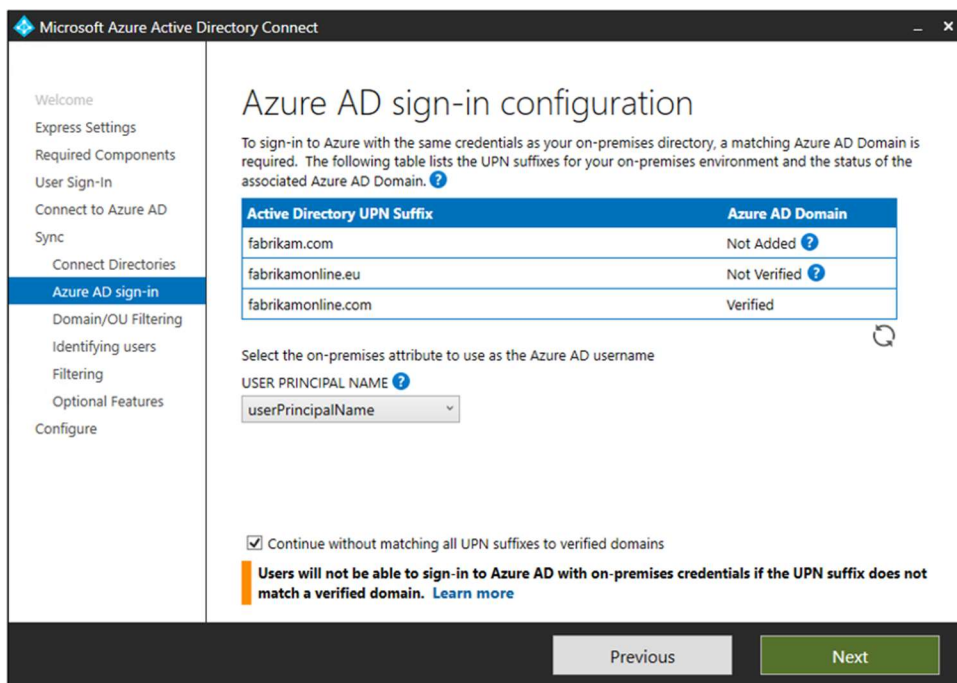
Connect to your Azure AD tenant using a global admin account. Next, we will connect to your local AD forest using an Enterprise admin account.



After adding the forest name and clicking **Add Directory**, a pop-up dialog will appear. At this stage, I typically choose to let Azure AD Connect **Create new AD account**, which will be used by the service to read and synchronize data out of the local AD database. In order to create the new account, you must provide credentials for a valid Enterprise admin, below.



This next screen is crucial. You will want to make sure to get your UPN attribute selection correct here. First, you can review domain UPN suffixes that are available on-premises and in the cloud—so hopefully you have already verified the domains you own via the Microsoft 365 admin center.

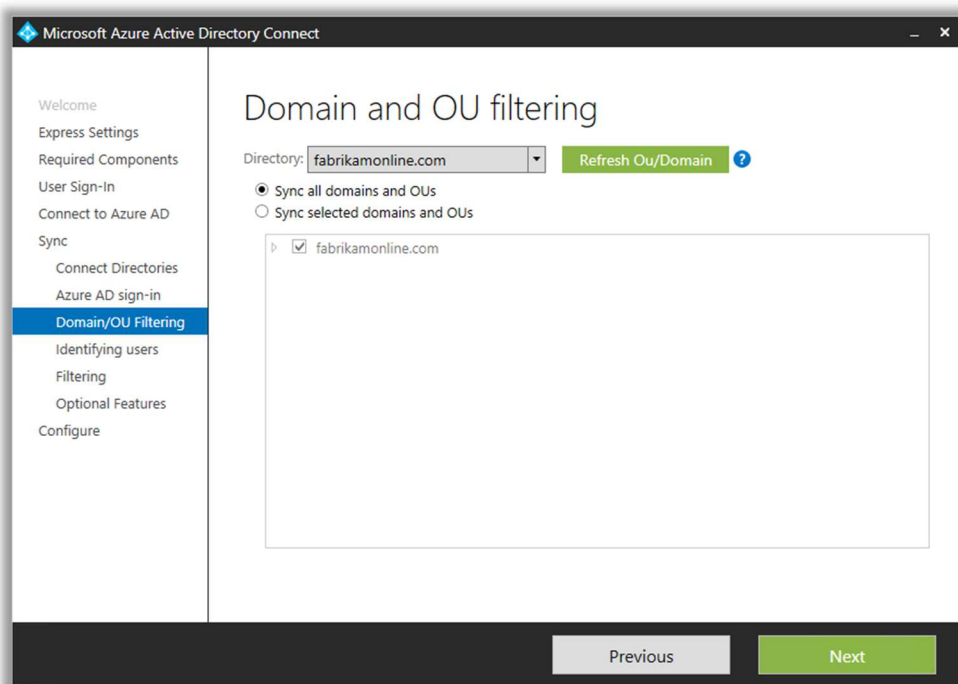


Now, we have to select the attribute to use for the Azure AD username. By default, it selects the UPN (userPrincipalName) attribute. Leaving it set to the UPN is what Microsoft recommends, however, **be sure that your UPN on-premises is already setup to match the Internet-routable email address**, per our discussion above.

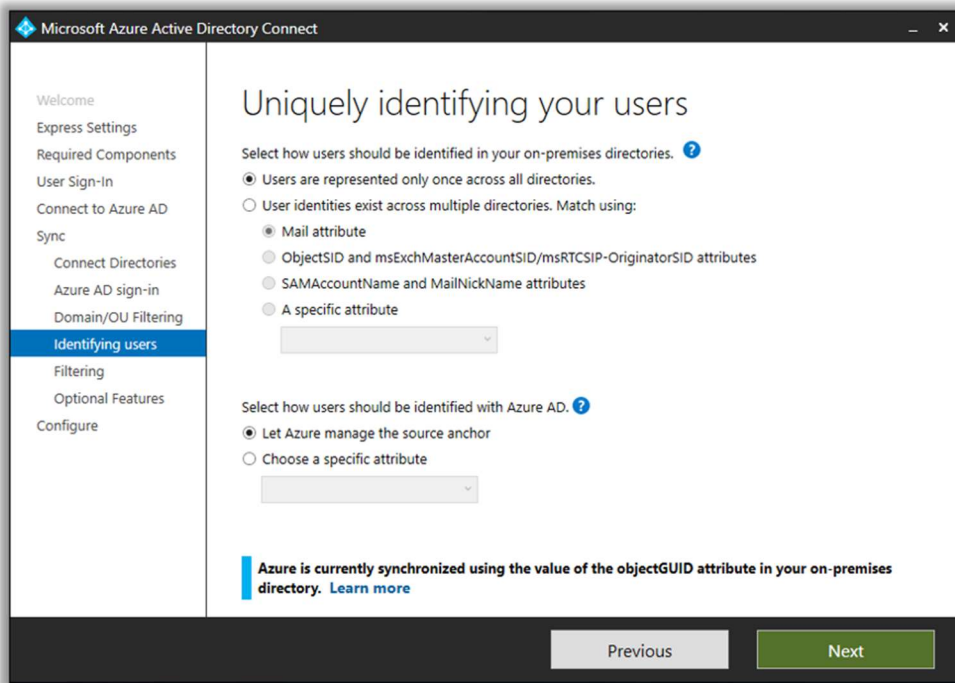
Otherwise, know that it is also possible to change the UPN setting to use the **mail** attribute instead. This will force the user's email address to become the username in Azure AD. Going with the mail attribute is known as configuring an Alternate ID. Read up on the extra considerations with this type of ID [here](#).

If you are only using Azure AD Connect as a bridge, with the goal of eventually ditching on-premises servers, then using an Alternate ID such as the mail attribute should not be a problem.

On the next screen, it is possible to filter out OUs that do not need to be synced. I recommend constraining the objects that are synced from on-premises AD. After all, there are likely many accounts that do not need to exist in the cloud. An easy way to do this is to pick specific OUs that contain active user accounts and Exchange objects (e.g. Shared or Room mailboxes).

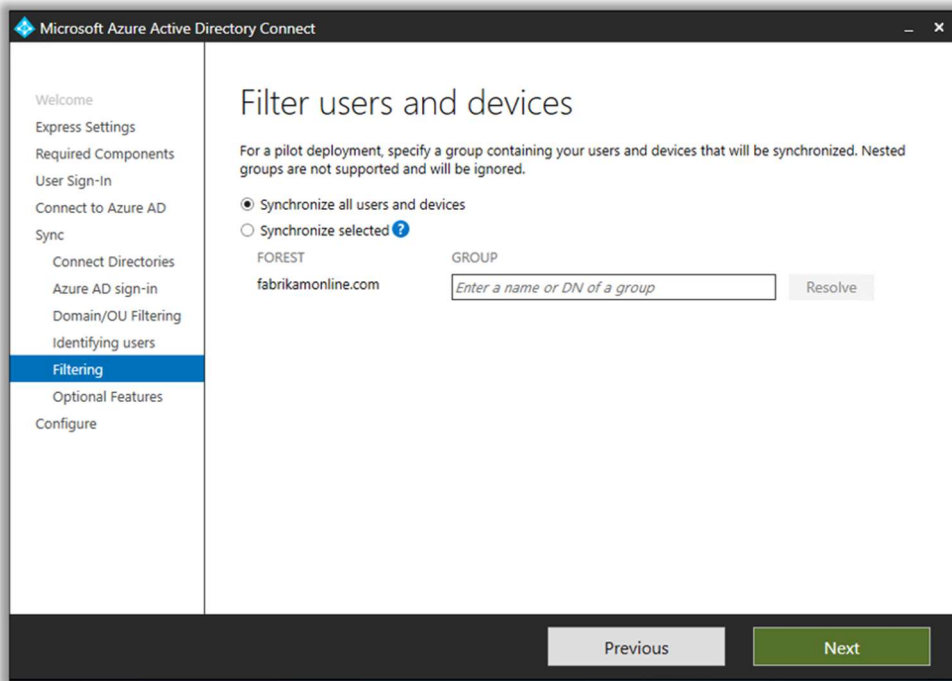


The next step about **Uniquely identifying your users** applies more to complicated Enterprise environments where you could have multiple identities across different forests. You can leave the defaults alone and click **Next**.

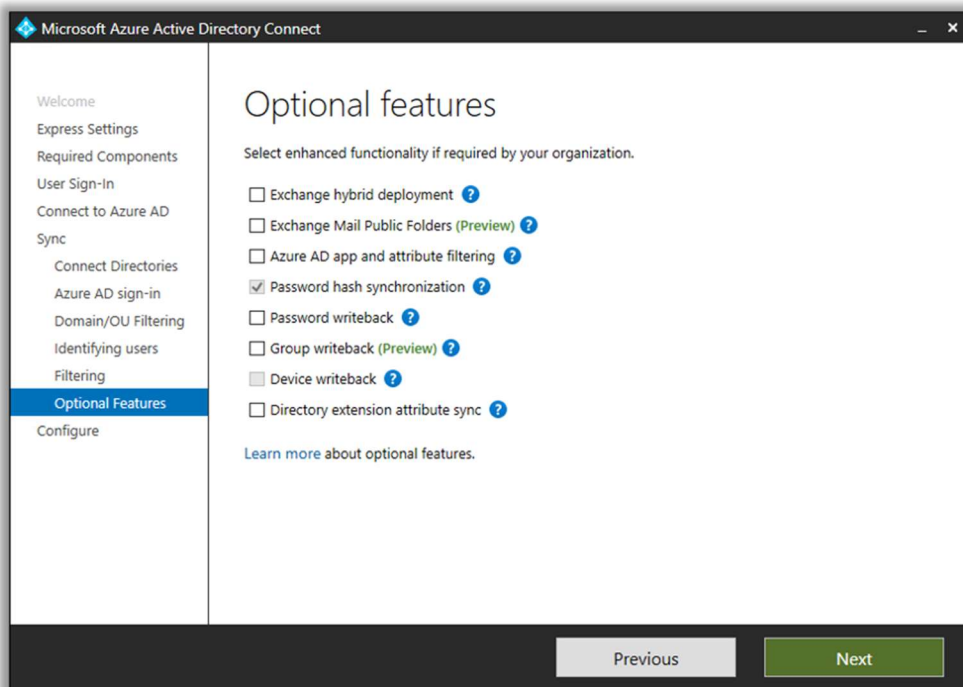


You can also choose to filter users based on group membership. I would not recommend using this option in conjunction with OU filtering. Just know that OU filtering is applied first, so the group and all members of the group would need to be included in the OUs selected for sync—just be careful. This is just one more option which can help us prevent syncing unnecessary objects.

I never use group filtering, to be honest. Instead, I implement a radically simple OU structure (synced vs. non-synced accounts). Any remaining GPOs in the organization are filtered by security group, rather than OU. Perhaps you would find this setup a bit drab, but the way I see it, this old domain is on its way out anyway.



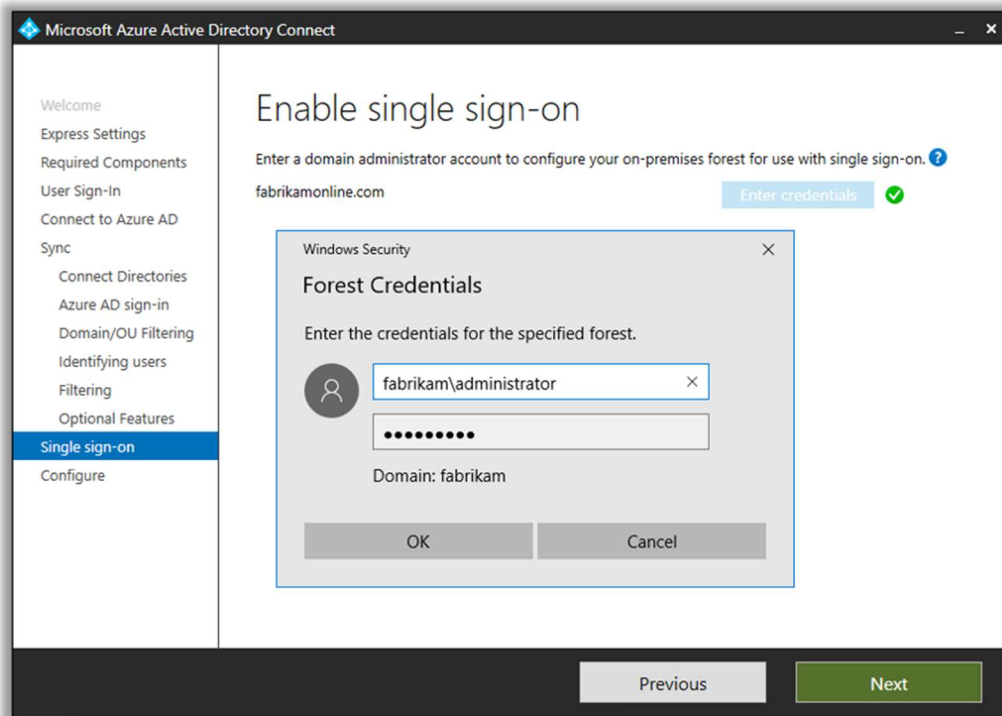
This next page is getting a bit gnarly with all the new **Optional features** that have been coming out lately. If you have Exchange on-premises (or you had it at one point and the attributes still exist), then you should select **Exchange hybrid deployment**. This sets you up nicely for hybrid migration later on.



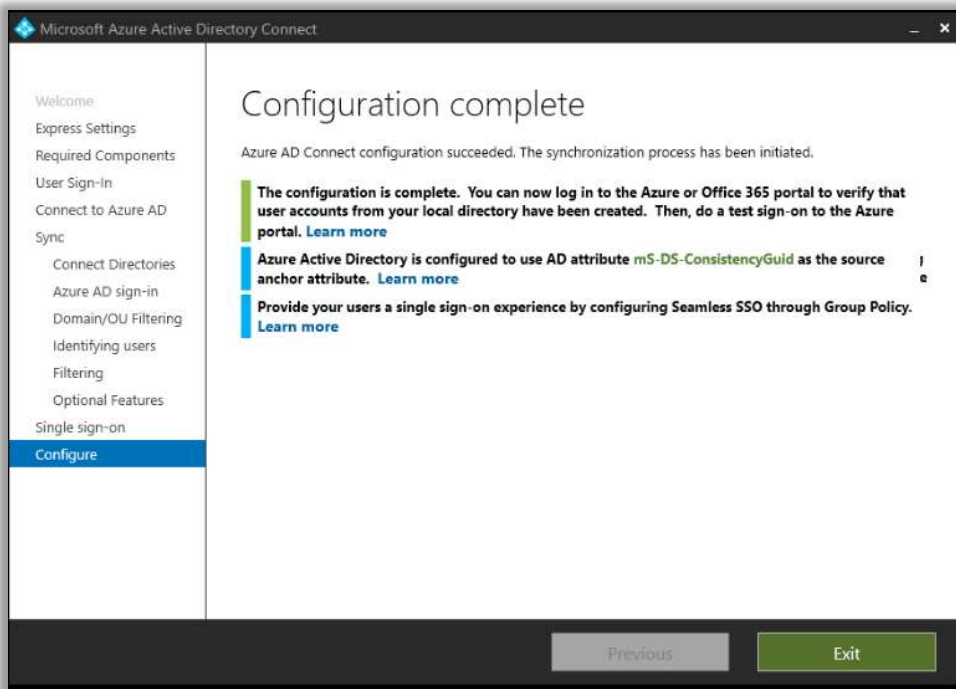
You might also configure **Password write-back**—but there is more required to set this up than that checkbox lets on. We'll go over this option in more detail soon.

I will not cover the option to constrain attribute syncing, or any other optional features.

On the **Enable single sign-on** screen you will need to provide a domain admin account in order to create a computer object in AD that is used for SSO. The credentials are only used at this time (not stored, not for ongoing services).



Click **Next** to review your settings—I usually allow the synchronization process to start when configuration completes (I do not enable staging mode). Finally, hit **Install** to complete the wizard. When the process is complete, you can review any messages and follow-up items it has for you.

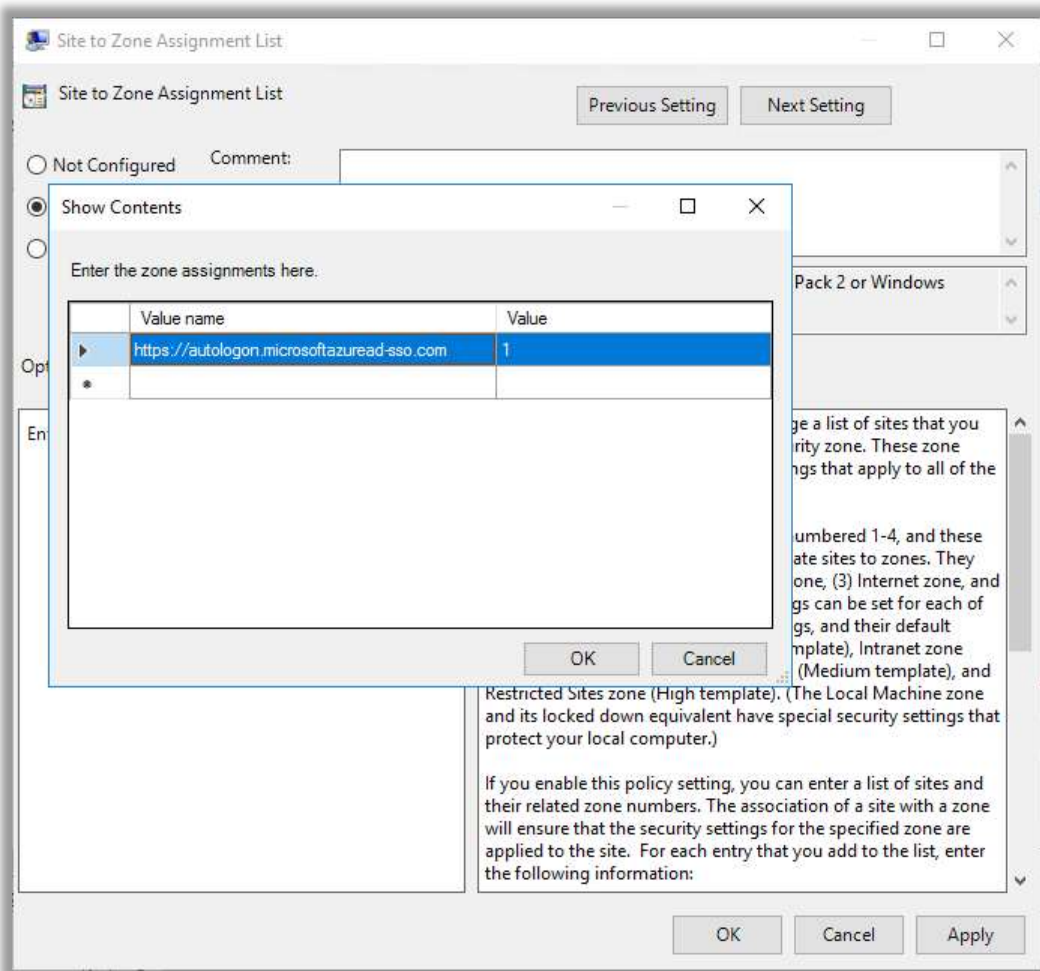


You may notice a link to **Learn more** about configuring a Group Policy for Seamless SSO. Let's do that. There are two options discussed in this link, but I'll demonstrate the one that does not allow users to modify their Zone settings.

Deploy group policy for Seamless SSO

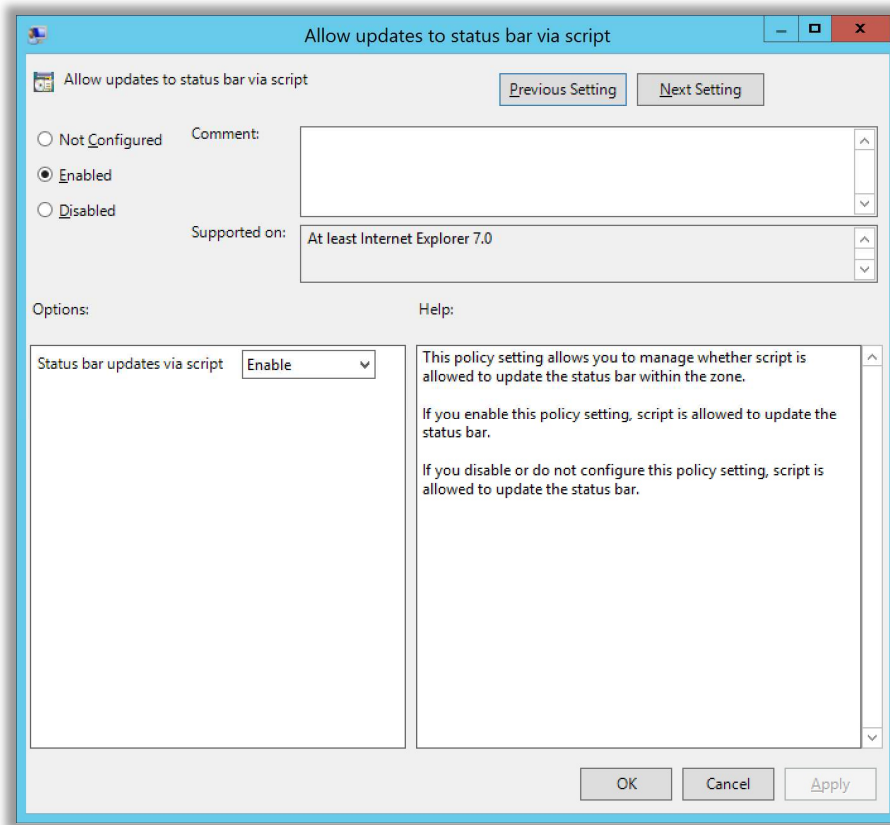
Go to your domain controller and open the **Group Policy Management** Microsoft Management Console

1. Create and edit a new GPO that will be applied to all users. Name it **AAD Seamless SSO** (or something similarly descriptive).
2. Navigate to **User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page** and select **Site to Zone Assignment List**.
3. Enable the policy and enter *Value name*: **https://autologon.microsoftazuread-sso.com** and *Value*: **1** as depicted.
4. Click **Ok** twice to finish.



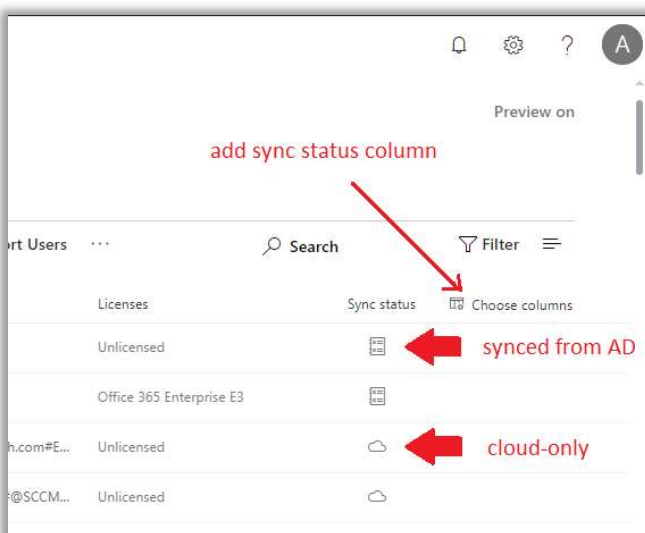
5. Next browse to **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone**. Then select **Allow updates to status bar via script**.
6. **Enable** the policy setting, and then select **OK**.

Whew. We are officially all done configuring Azure AD Connect with Seamless Single Sign-On.



Understanding the Source of Authority and Hybrid management of Exchange Online

Be sure to visit the Microsoft 365 admin portal also, to verify that your user accounts are showing up in the cloud. You may have to add the Sync status column from Choose columns, to view the source of each account; AD accounts synced to Azure AD are represented by a building whereas accounts that are in Azure AD only are depicted as a cloud.



Once you are in a hybrid relationship with Azure AD Connect, you must keep in mind where the Source of Authority lives: for synced accounts, it is still with your on-premises Active Directory server.

This means that new accounts will always be born here. Make sure they are created in an OU that is setup to sync to Azure AD, so that the account gets created in the cloud appropriately upon the next Azure AD Connect sync cycle. After the account is synced and setup correctly—that is the appropriate time to assign licensing in the cloud.

Here is the complete (supported) procedure for creating new hybrid user accounts:

- Create the identity on-premises first, with matching UPN, etc., and let it sync to Azure AD. You can force a sync from the Azure AD Connect PowerShell module if you are impatient:
 - `Start-ADSyncSyncCycle -PolicyType Delta`
- Make sure you enable the remote mailbox using the following Exchange cmdlet from your on-premises Exchange Management Shell:
 - `Enable-RemoteMailbox username -RemoteRoutingAddress username@tenantname.mail.onmicrosoft.com`
- Assign licensing via the Microsoft 365 admin portal
- Confirm sign-in works for the user on-premises first, then in the cloud

An alternative to this that also works is to create the user and mailbox on-premises and then migrate the mailbox to the cloud using the Remote Move method. I usually stick to the former option.

Another important thing to understand is that editing certain user attributes, such as email address aliases, must be performed on-premises and not in the cloud. If you attempt to change some of these mail attributes in the cloud, Microsoft 365 and/or Exchange Online will bark at you. Therefore, most changes and management must be done on-premises.

The big shocker for people is that in order to run in a supported configuration, you must keep an on-premises Exchange sever around, even well after the last mailbox has been migrated to Office 365 Exchange Online.

Why? Because Microsoft does not have any other supported mechanisms for supporting hybrid co-existence of identities that maintain Exchange attributes. Therefore, to edit any mail-related information within the on-premises user object, requires Microsoft Exchange Server. I know, facepalm.

Enterprises generally will keep a “Hybrid-only” management box around, and Microsoft even gives them a free license to do it! But the Business SKU does not give us access to a free Hybrid Exchange Server license, unlike the Enterprise SKUs. And most SMBs want to get rid of their legacy Exchange boxes in the worst way. Here are your options:

1. Dismantle hybrid and remove Azure AD Connect (and then finish getting rid of your servers)

2. Add at least one E1 license to your tenant, then register for a free hybrid key at <https://aka.ms/hybridkey>, and finally install a new hybrid Exchange Server to replace your old one
3. Color outside the lines, be a rebel, and break the rules (as much fun as that sounds, this is not an endorsement)

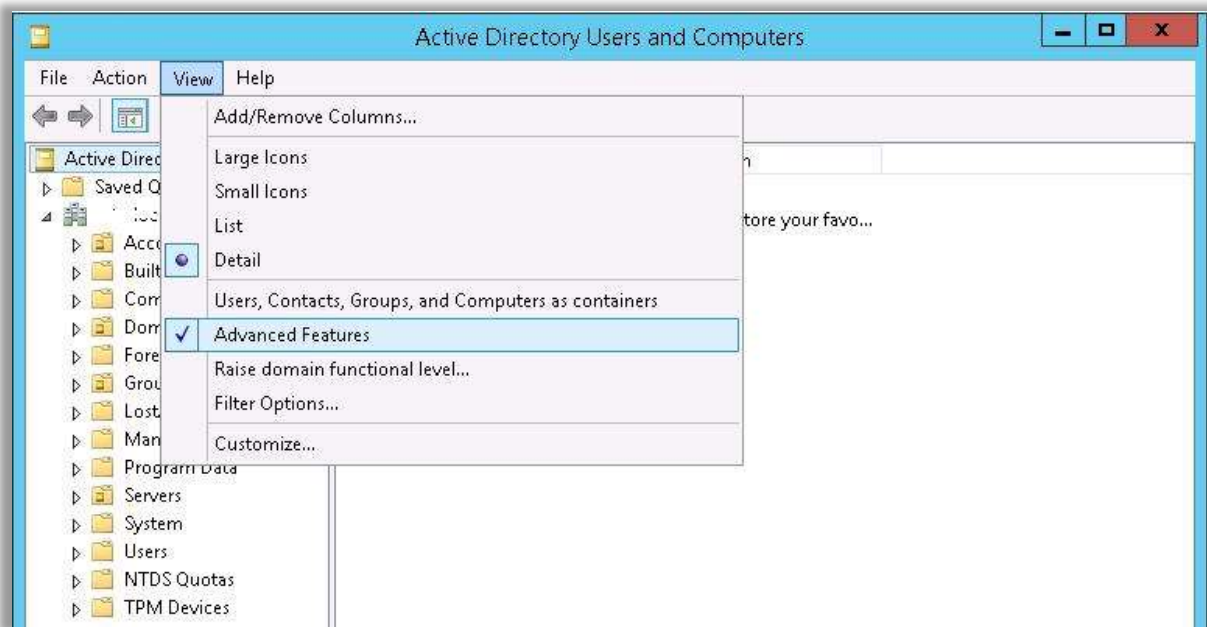
If you decide to operate Office 365 Exchange Online with Azure AD Connect in place, and without an on-premises Exchange server, which is possible, just know that it is also not supported. This is what it looks like (again, at your own risk, and this is not supported).

1. Disable Outlook Anywhere, remove the on-premises SCP and all other references to the Exchange server that you know about (MX, Autodiscover, etc. should match Office 365 settings).
2. Regarding the removal of Exchange server: if you uninstall the last Exchange server you will lose your Exchange attributes which will break your Exchange online mailboxes—because your Azure AD accounts rely on those attributes, which came from the on-premises environment. Two options:
 - a. Do not remove the last server properly, just power it down permanently—this gets dicey with SBS, but it is possible to whack references that are no longer needed manually via DNS management and ADSI edit...OR
 - b. Export all of the Exchange attributes such as email addresses, etc. to a CSV file. Disable and remove Azure AD Connect. Remove Exchange Server. Re-run the AD schema extensions for Exchange Server from setup media. Reimport the exported attributes. Finally, reinstall Azure AD Connect.
3. You can look up how to do that stuff on your own. Once you are all done carefully sweeping up the environment using one of those methods described above, you will need to be careful how you manage accounts moving forward.

I will illustrate some common management tasks and how to perform them in a hybrid environment *without* an Exchange server (remember that none of this is in any way supported):

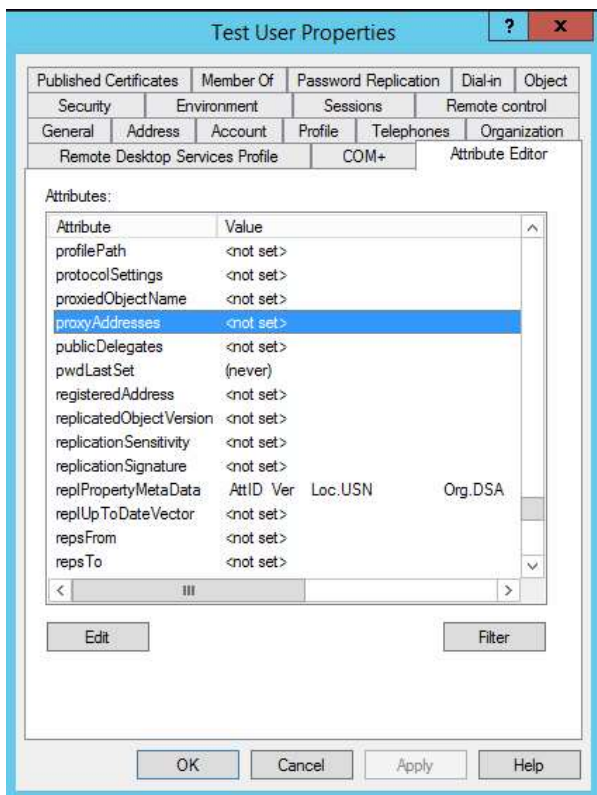
- New user accounts
- Adding new email aliases
- Hiding from address lists
- Enabling archive mailboxes

First, from Active Directory Users and Computers, you will want to enable **View > Advanced Features**. This is necessary so that we can see the **Attribute Editor** tab on any given user account. Another alternative is to find the user in ADSI edit and manipulate the attributes there.



New user accounts

Just create the user like normal. As always, be sure that the UPN suffix matches the email domain, and that the email address attribute is properly filled out. But, you should also do the following on the **Attribute Editor** tab in Active Directory.



Find the **proxyAddresses** attribute and add both the primary SMTP address if it is not already present, as well as a secondary "lowercase" smtp address. The entries should look as follows:

- **SMTP:username@domainname.com** (this is the primary email address of the user)

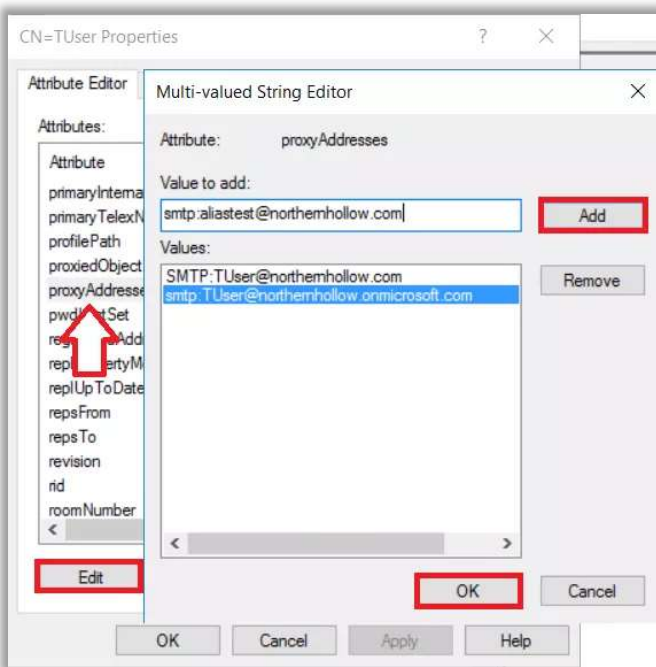
- **smtp:username@tenantname.onmicrosoft.com** (this is the alias for the Office 365 domain)

Once the account synchronizes to Exchange Online, assign your licensing, which will create the mailbox in the cloud. Verify sign-in first on-premises, and then in-cloud.

Adding alias addresses

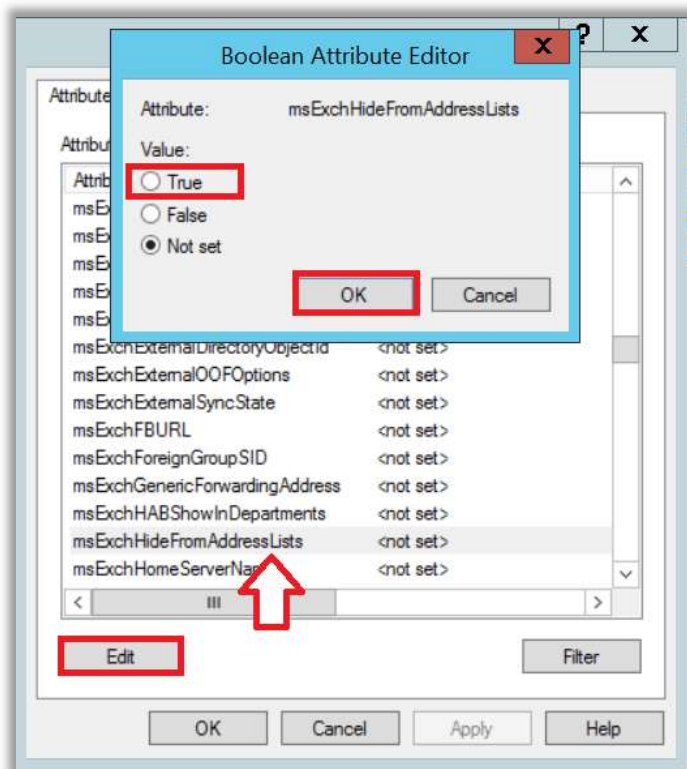
From the **Attribute Editor** tab, scroll to find the **proxyAddresses** attribute. Add the address as follows:

- **smtp:aliasname@domainname.com**



Hide a mailbox from the GAL

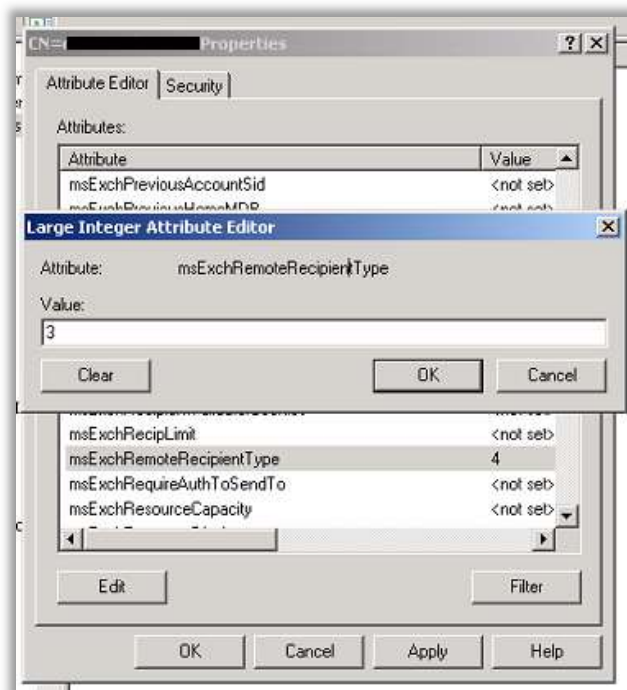
Find the attribute called **msExchHideFromAddressLists**. If you wanted to hide this user from the Exchange Global Address List (GAL), you would need to update the value to **True**.



Enable an online archive mailbox

Find and modify these attributes in the attribute editor:

- **msExchArchiveName** = (give this any name like "Personal Archive – Username")
- **msExchRemoteRecipientType** = (change the value to 3)



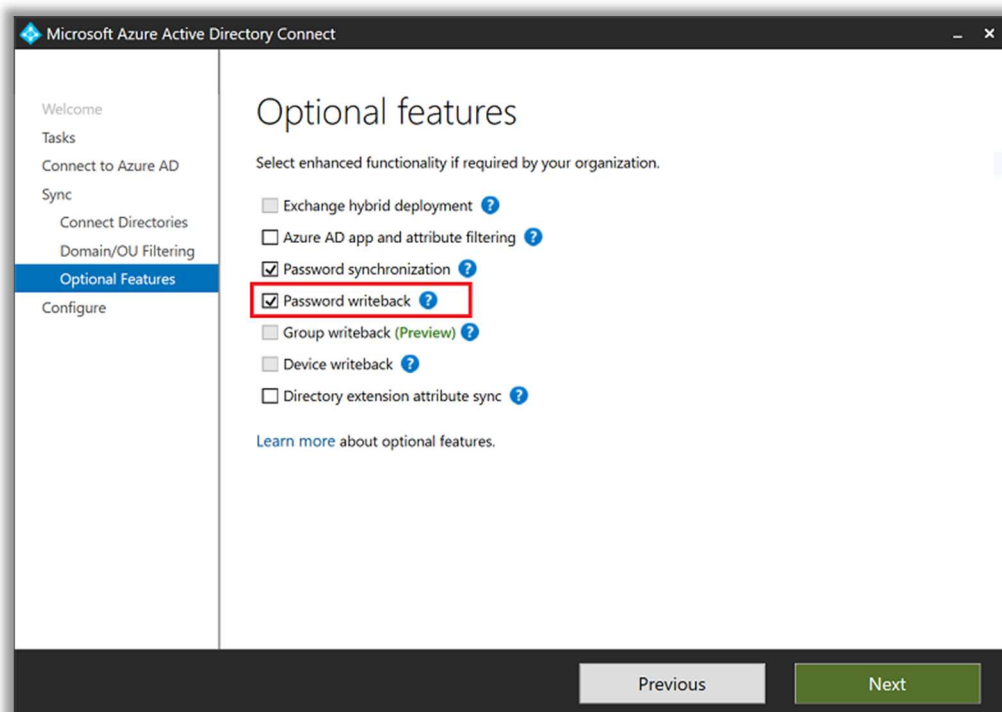
Hybrid SSPR with password write-back

To enable Self-Service Password Reset with password-writeback for hybrid identities, you will need to make some configuration changes in three different places:

1. **Azure AD Connect** – to enable password write-back
2. **On-premises AD** – to delegate permissions for password changes to the service account
3. **Azure AD admin center** – to enable the functionality online

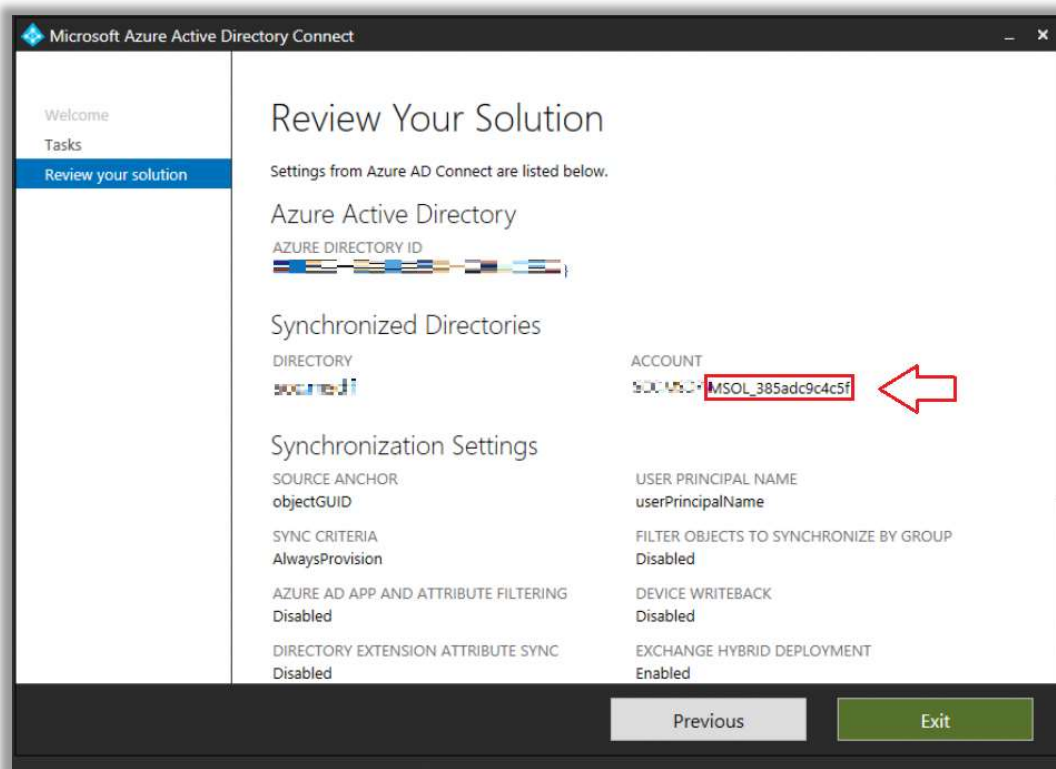
Step 1. Enable password write-back

You may have already enabled the password write-back bit in Azure AD Connect during installation. If not, you can launch the tool again. From **Additional tasks**, choose **Customize synchronization options** then **Next**. You can just step past the next few screens, providing an Azure AD admin credential, etc. You want to find your way to **Optional features**, and select the checkmark box for **Password writeback**, then finish out the wizard to apply the setting change.

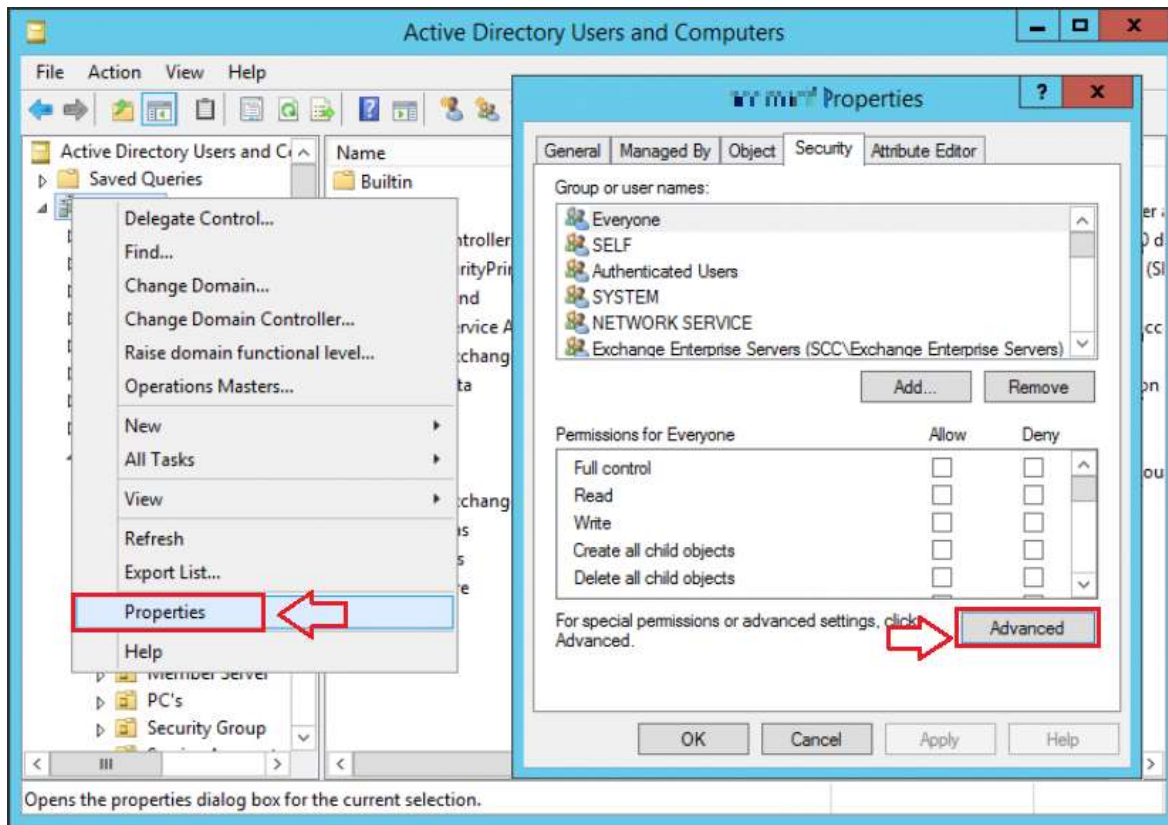


Step 2. Delegate permissions

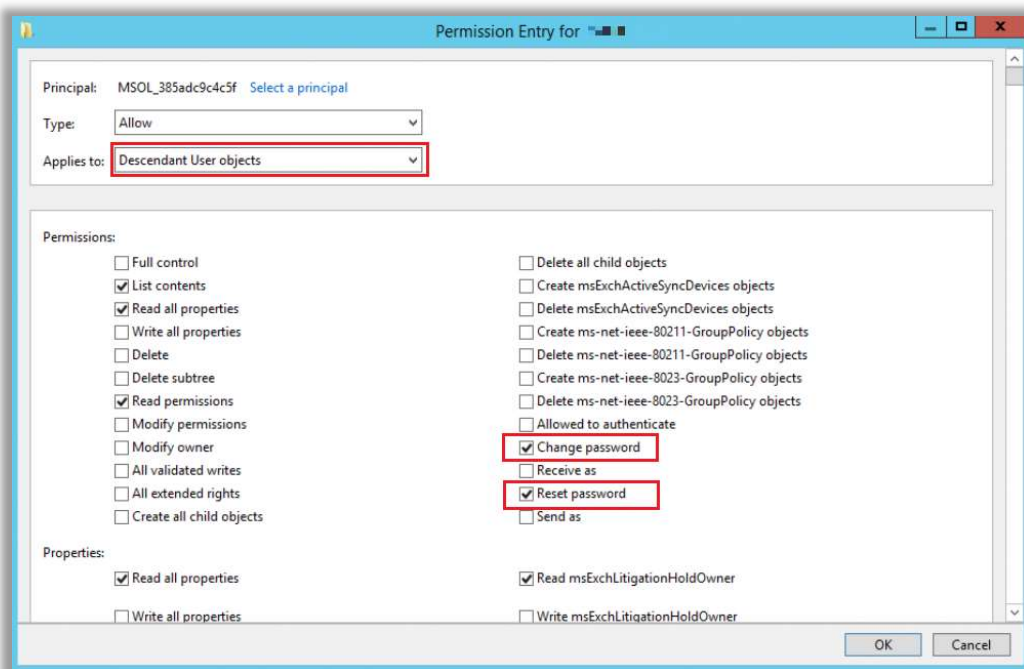
Launch Azure AD Connect again. From **Additional tasks**, choose the option to **View current configuration** and click **Next**. Find the account that is being used by Azure AD Connect. You need to delegate permissions to this account.



From AD Users and Computers, ensure you have **Advanced features** enabled from the **View** menu. Then right-click the root of the domain and go to **Properties**. From the **Security** tab, click **Advanced**.



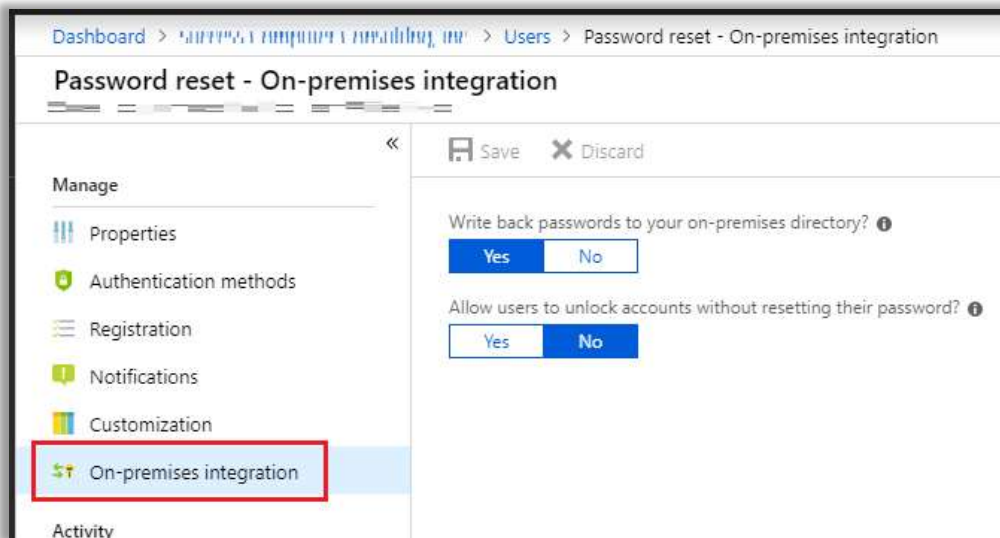
From the **Permissions** tab, select **Add**. Select the username (principal) you identified above via Azure AD Connect. In the **Applies to** drop-down list, select **Descendant User objects**. Under **Permissions**, select the boxes for **Change password** and **Reset password**.



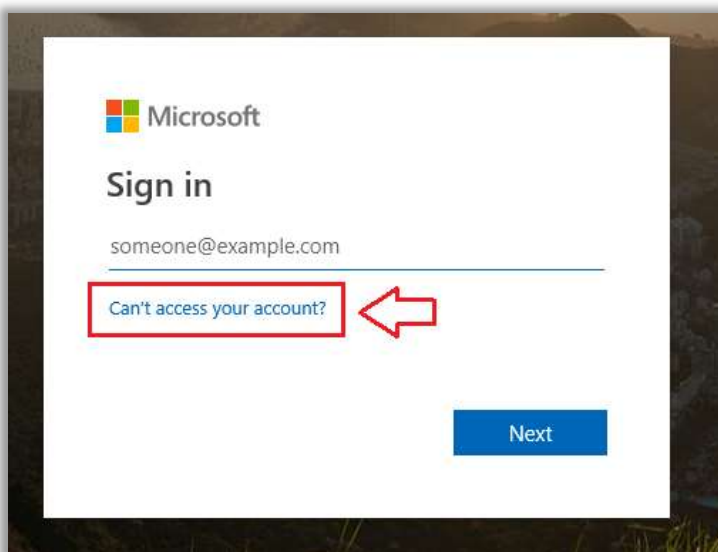
Scroll down further, and under **Properties**, select the boxes for **Write lockoutTime** and **Write pwdLastSet**. Finally, you can **Apply** the changes and **OK** to exit.

Step 3. Configure Azure AD SSPR settings

From the Azure AD Admin center, go to the **Users** blade, and find **Password reset > On-premises integration**. From here you can customize the settings—granting or denying the ability for users to perform self-service “unlock” in addition to self-service reset. (By default a password reset also unlocks the account).



In case you have trouble getting this feature to work, check out Microsoft’s article titled “[Troubleshoot password writeback](#).” If it is working, however, then you should be able to verify by visiting any Microsoft 365 sign-in page and clicking the link: **Can’t access your account?**, then following the steps to perform a reset from there.



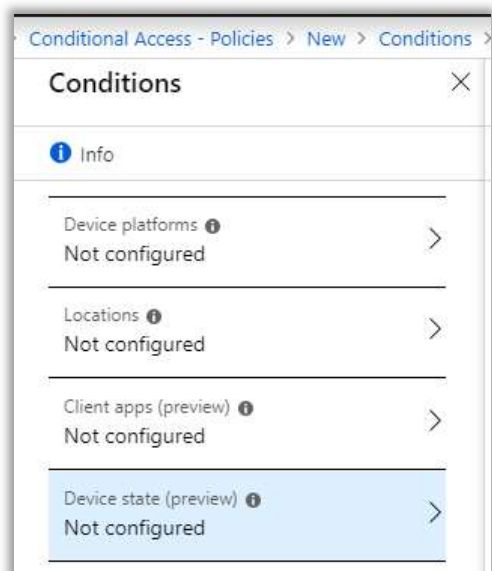
Conditional Access for the SMB

Conditional Access is now included with Microsoft 365 Business plans. As you begin to work with this amazing tool, you will quickly see how powerful of a technology it is.

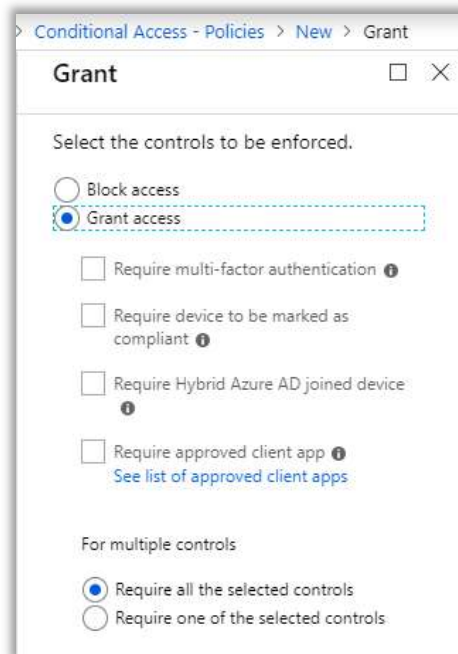
Conditional Access

Conditional Access is a killer security feature which allows administrators to create policies based on various *conditions*, and then apply *access controls* based on those conditions. If you are managing additional enterprise applications, you can also design conditional access policies which apply to them. This provides us a whole new level of security, which is hard to understate.

Specify Conditions (IF):



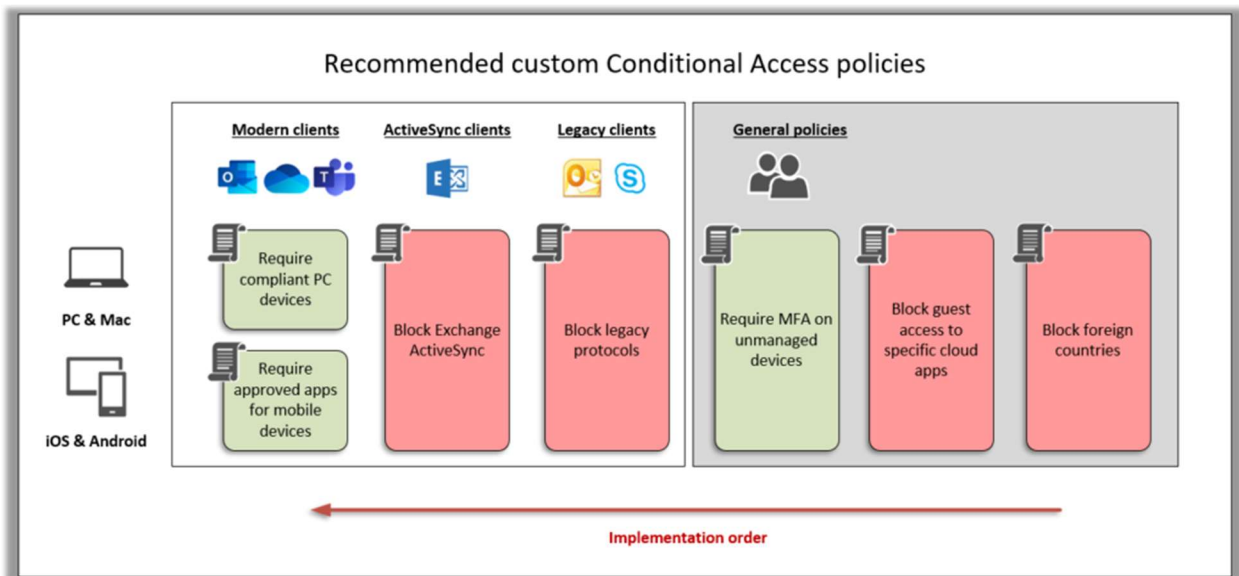
Specify Access Controls (THEN):



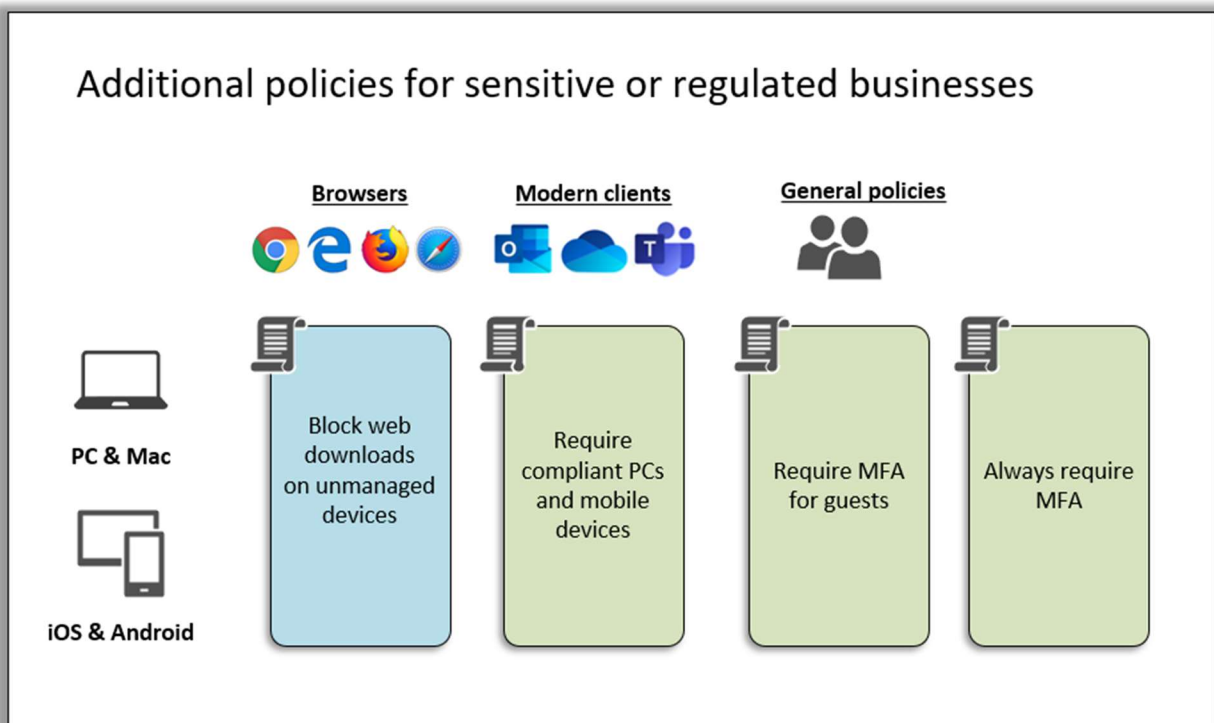
The policies can also be targeted or scoped to specific users, groups, applications, etc. Examples of Conditional Access policies in action include:

- Require devices to be compliant with Intune policies before granting access
- Require Windows 10 devices to be joined to the corporate domain
- Require MFA under certain conditions (e.g. untrusted devices or locations)
- Restrict access from Web browsers
- Deny legacy apps, untrusted locations or devices, etc.
- And many more

With a well-designed set of Conditional Access policies, you also gain a very important foothold in terms of security: an inventory of devices connecting to your cloud-based applications and data, automatically registered in Azure AD. This goes back to the point I made before about knowing what you have in your environment—it's often more than half the battle.



I have [another guide available](#) specifically about Conditional access, including information about the free baseline policies which are available in every tenant, as well as several custom policies that I recommend for the SMB. I also detail a few policies targeted at more sensitive industries, for example those in the healthcare or financial services sector.



Again, [my published guide](#) details all of these—their impacts, how to set them up, and so on. As well, I have a summary of the [policy design](#) available on GitHub—some find that to be adequate on its own.

Part 2. Device Management

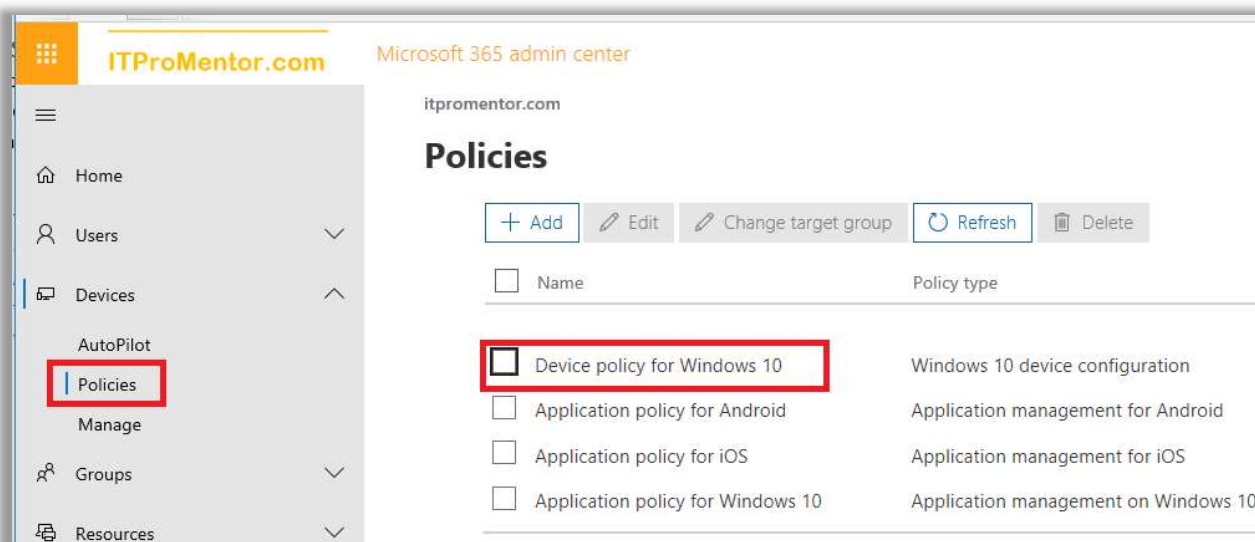
Windows 10 Management

I will cover Windows 10 devices first, separately from mobile devices. In small and mid-sized business, Windows 10 devices are most often corporate-owned, whereas mobile devices tend to be personal “BYOD” devices. This usually leads us to some distinctions in management approach, which we will cover as we describe the differences between MDM (Mobile Device Management) and MAM (Mobile Application Management).

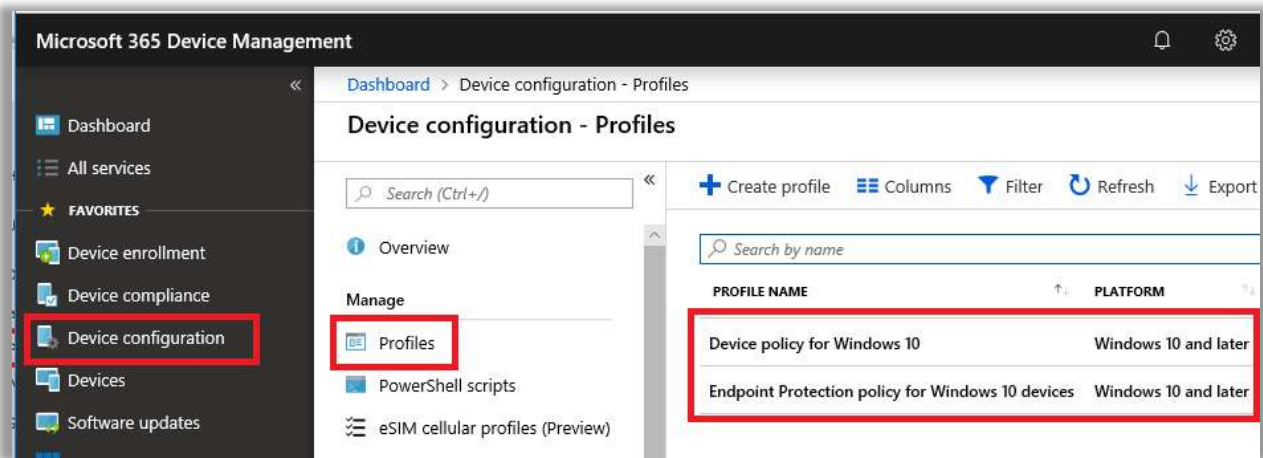
Windows 10 is the preferred operating system to use in conjunction with Microsoft 365 Business. Not that other operating systems are unsupported—they are, in fact (even macOS is supported)—but you get the best overall experience when you leverage Windows 10.

Windows 10 device configuration policies

When we initially set up the Microsoft 365 Business subscription, the wizard automatically created a Windows 10 device configuration profile. You can see this profile from **Devices > Policies** in the Microsoft 365 Admin center.



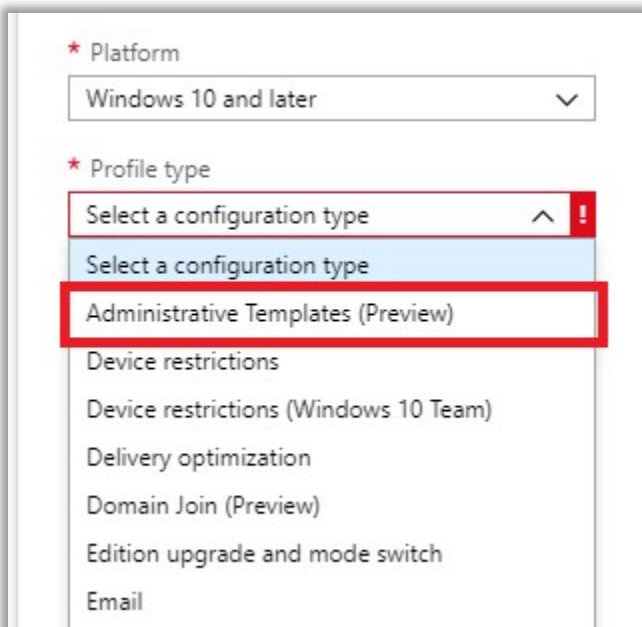
To see the same settings in Microsoft Intune, navigate to <https://devicemanagement.microsoft.com> and go to **Device configuration > Profiles**. The policy from the screenshot above is actually representing two policies, *Device policy for Windows 10*, and *Endpoint Protection policy for Windows 10 Devices*.



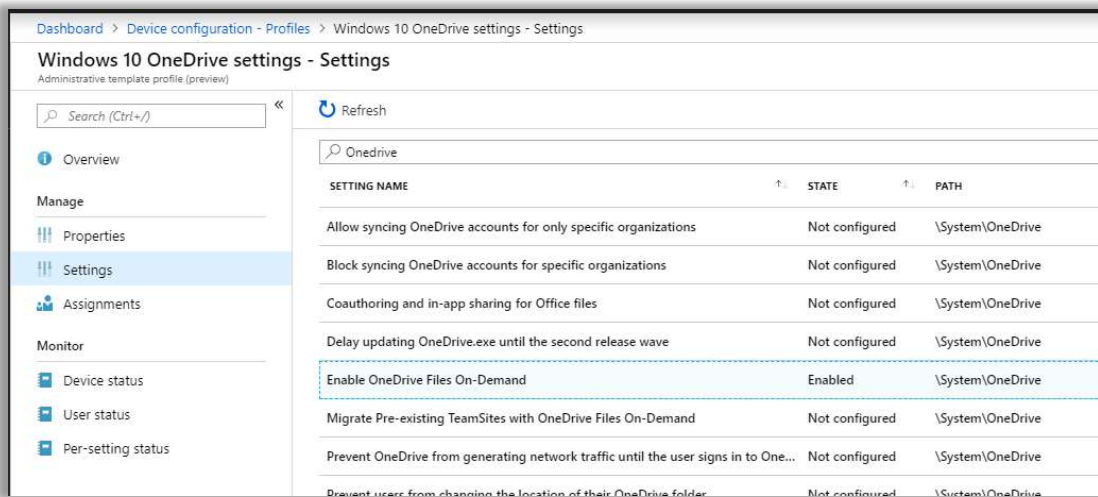
Now if you *did* decide to browse all of the various options inside of these policies, you would find that a laughably small subset of controls are exposed and enabled via the Microsoft 365 admin center. Just be aware, however, that it is not recommended to edit the default policies directly. Instead, it is better to create new profiles and new assignments, and to make customizations from there.

Note: The Business subscription may not support all of the features and settings that you see listed in these policies. For example, Windows Defender ATP would require Windows 10 E5.

Go ahead and create a new configuration profile by clicking on **Create profile**. Just so that you can see what other types of configuration profiles are available for Windows 10, pick **Windows 10 and later** as your platform, then see a list of the *Profile types* available. The **Administrative Templates (Preview)** option is worth mentioning, as they allow you to control settings similar to what you have seen in group policy, in the past.



You can filter the giant list using search. Some of my favorite settings here includes the ability to configure the OneDrive client. For example, I can enable Files On-Demand (so that I don't have to touch every PC to configure this setting on the OneDrive client). I won't recommend a lot of specific settings here—design your own policies as you would have previously with GPOs. This is just an example of what you can find and do with the Administrative templates, which we certainly expect to see expanded over time.

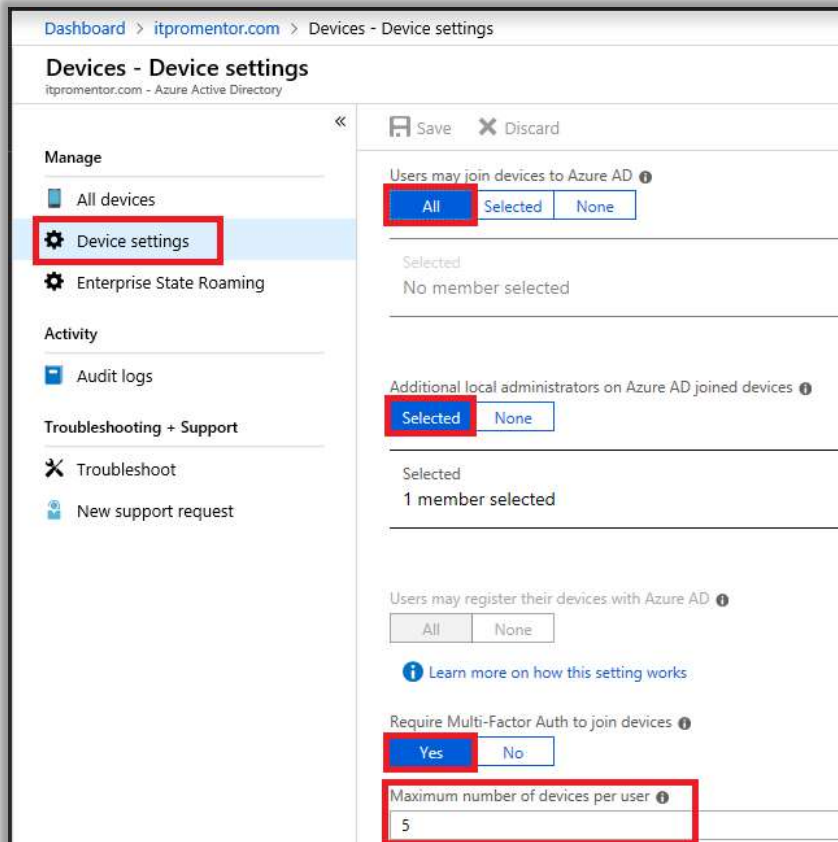


Device Settings and Enterprise State Roaming

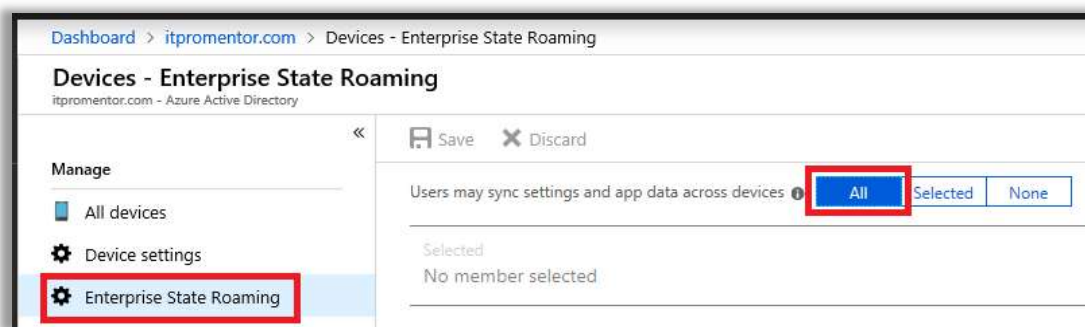
Make your way back to the Azure AD admin center. Find the **Devices** blade from the left menu, and select **Device Settings**. These settings apply specifically to Windows 10 devices. I recommend doing a few things in here:

- **Users may join devices to Azure AD – All;** In most SMB environments, anyone should be allowed to join a device, and this is the default setting. Still, it may not suit you; in some corporate environments this is sometimes restricted to IT admins.

- **Additional local administrators on Azure AD joined devices** – By default, only the user joining the device to Azure AD will be made an admin on the device. If you have another admin account you want to include, specify that here.
- **Require MFA to join a device to Azure AD** – Turn this on.
- **Maximum number of devices per user** – I recommend setting this very low, at 5 devices. The reason being: it keeps you on top of pruning stale devices, and it is easier to identify when there may be an issue/unauthorized device out there.



Also click to open the **Enterprise State Roaming** blade. I enable this for **All** users. It allows certain personalization and remembered settings to follow the user around to each device they register.



Understanding the device's relationship to Azure AD

Before we go further, I want to quickly make some distinctions for the reader, with regard to devices that we find in Azure AD. Depending on how it was configured, a Windows 10 device can show up as:

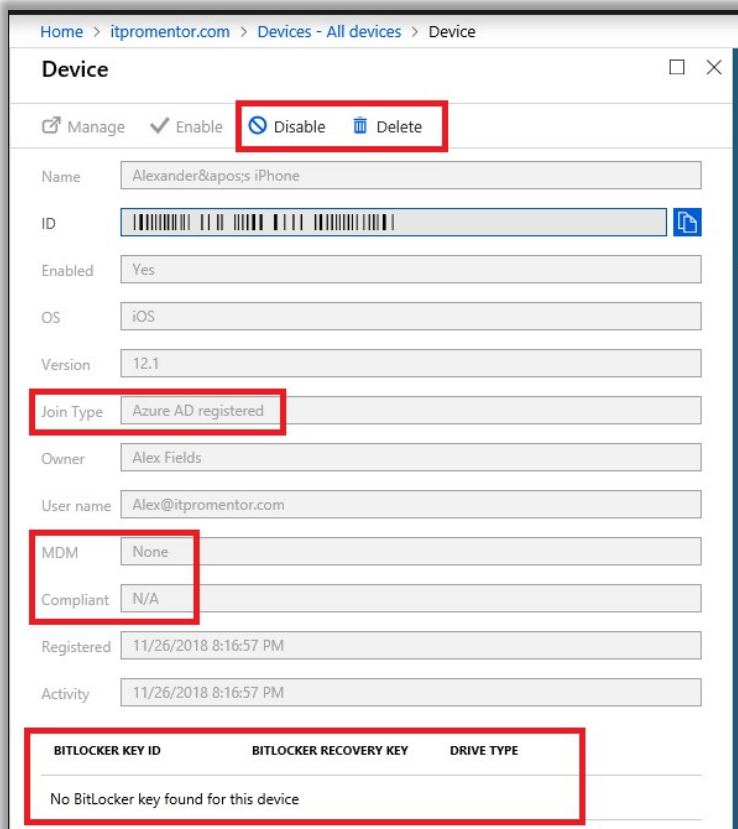
- Azure AD Registered
- Azure AD Joined
- Hybrid Azure AD Joined

And furthermore, any of the above device types could be managed by Intune device policies, or not! This is a confusing mess to some people, and we need to unravel it before we go any further.

Azure AD Registered

This is a weak association (but an association nonetheless), and basically it just means that the device exists, and is accessing Azure AD-based resources (such as Office 365). This join type can apply to *any* device—Windows, macOS, or mobile devices such as iOS or Android.

Registering is meant for “BYOD” scenarios and does not give admins much control over the devices themselves. We do however have the ability to report on these devices for inventory purposes, and to **Disable** or **Delete** the devices from Azure AD. If you care about security at all, then you should regularly prune inactive devices as a best practice.

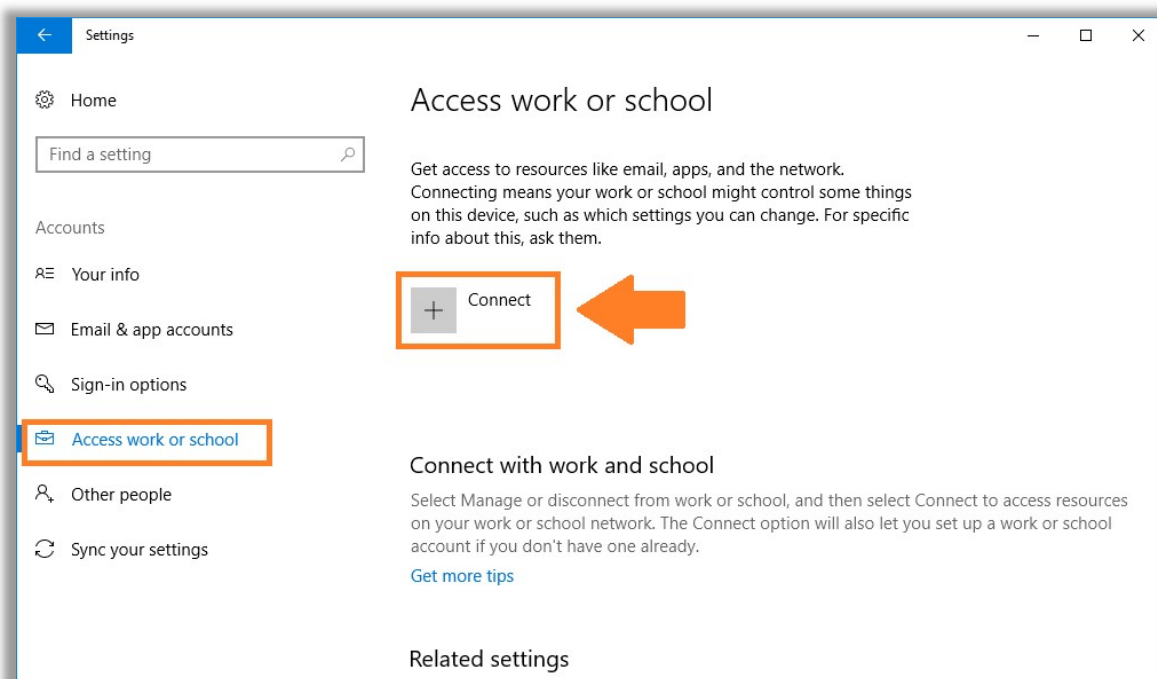


Notice in the screenshot above that the device **Join Type** is listed as *Azure AD registered*, and our available controls for this device are just **Disable** and **Delete**. Additionally, there is no MDM enrollment for this device, and no BitLocker keys. Know that it is also possible to have the device registered *and* enrolled in MDM, but in this case the device is not enrolled for MDM.

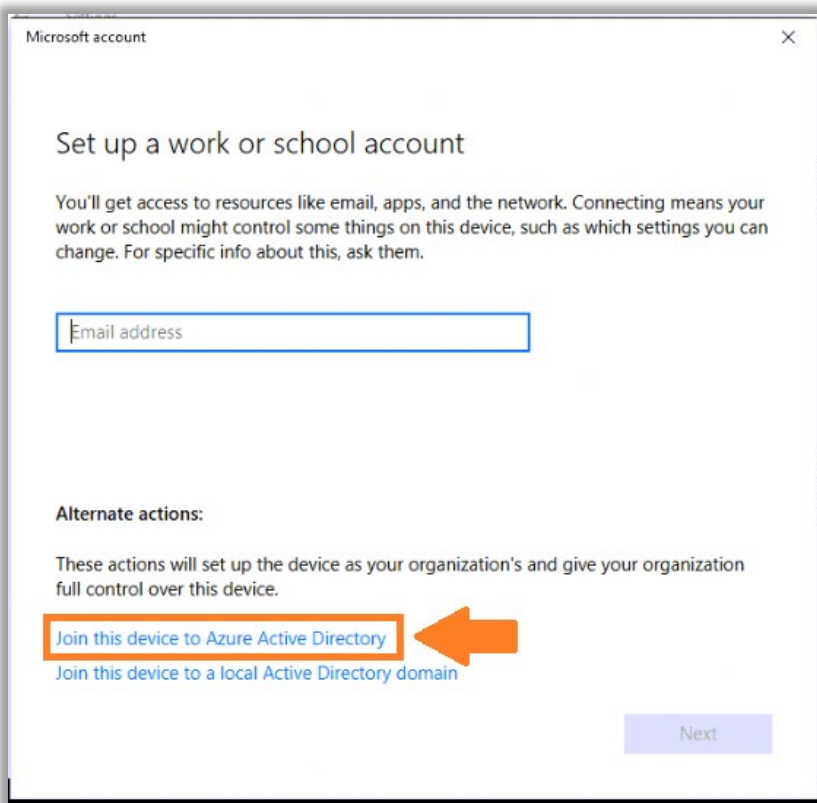
Azure AD Joined

Joining is just an extension of registering the device. They are nearly the same thing, except that in addition to receiving an identity in Azure that can be disabled/deleted, joining *also* changes the local state of the device, such that it is possible to sign-in to Windows 10 using Azure AD credentials. This join type only applies to *Windows* devices—it is possible for them to join Azure AD *instead* of joining a local Active Directory. This can be accomplished in several ways.

From the OOB or “first run” experience in Windows 10, a user can choose to sign-in using their Work or School account, and when they do, the device is thereby joined to Azure AD. Or, you can configure this option from another, local admin account on the device if it’s set up at a later time, after OOB. Navigate to **Settings > Accounts > Access work or school**. Click on **Connect**.

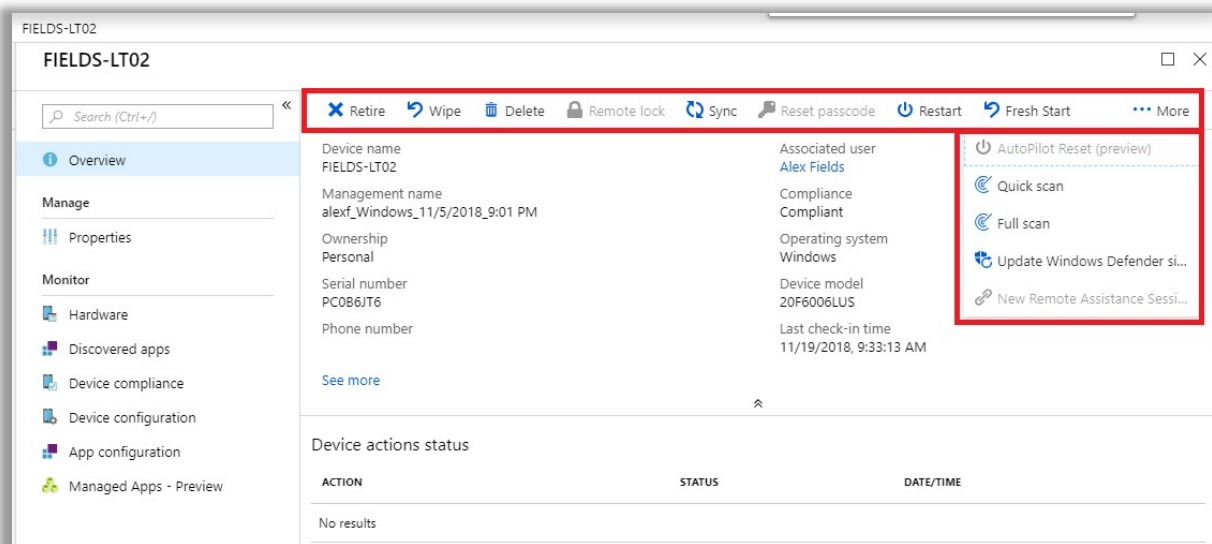


Do NOT simply fill in your work identity and click Next on this screen. That would have the effect of *registering* the device against Azure AD, only. Instead, you will choose **Join this device to Azure Active Directory** under Alternate actions. If you don't see this option, make sure you are fully up to date, and that you are *not* already joined to an on-premises Active Directory.



The benefits of joining Azure AD are that you will be able to sign into the device directly using your Azure AD / Office 365 credentials, and thereby enjoy Single Sign-On to all of your cloud-based resources.

In that example above, when we follow the link to **Manage**, we are brought over to the Intune console to manage the device. Just look at all the new options we have available! Perhaps most notably: **Wipe**. Since this is a Windows 10 device, there are also Windows Defender controls and some other goodies under the ellipses (**More**) —so don't miss those, either!



The primary benefits to enrolling in Intune are that you will gain much greater control over the device. With Intune, it's possible to:

- Wipe the device remotely (most commonly requested feature)
- Push certain policies, profiles and controls to the device
- Manage and push applications
- Enforce Device-based Conditional Access
- ...and more

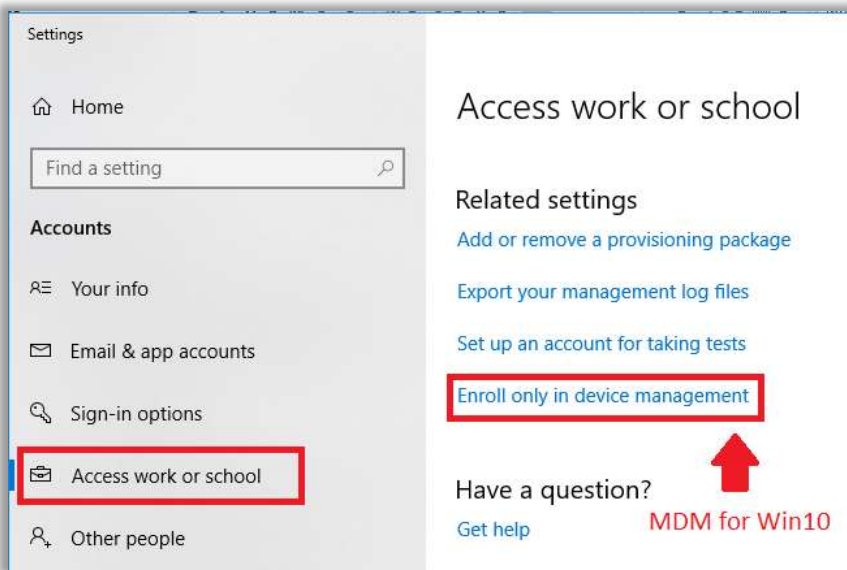
If you already setup your device policies when establishing your Microsoft 365 subscription, then any Windows 10 device that subsequently joins Azure AD will also become enrolled into Intune MDM automatically. The Windows 10 device policies you define should be applied upon joining.

Windows 10 Device management only (BYOD)

It is also possible for devices to become MDM enrolled, without joining Azure AD. This would be more intended for a BYOD scenario where a personal Windows 10 device is being brought into the corporate environment.

However, this option is not recommended as it does not support Conditional access. This would however force a registration against Azure AD (so it will show up in inventory, which, as you'll recall, is an important best practice in your overall security management protocols).

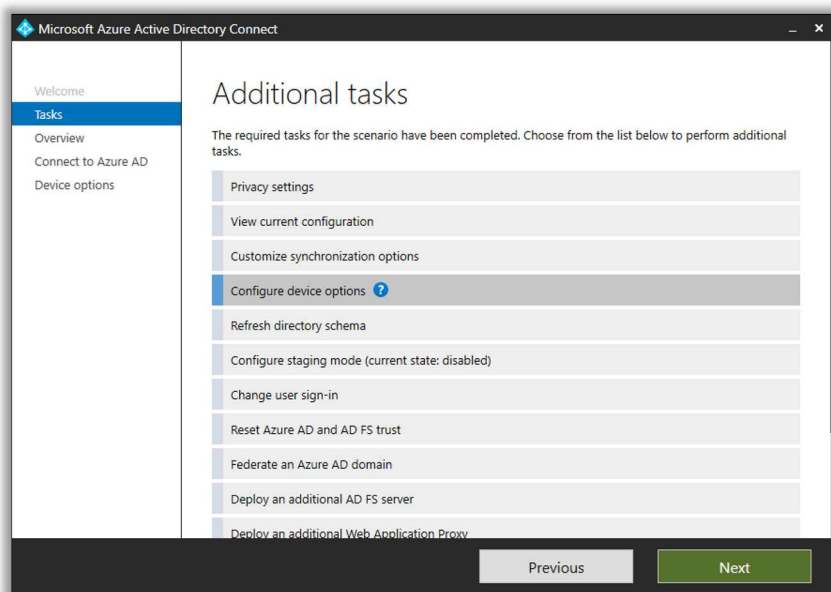
To manually enroll a Windows 10 device in MDM, go to **Settings > Accounts > Access work or school**. Find the link for **Enroll only in device management**.



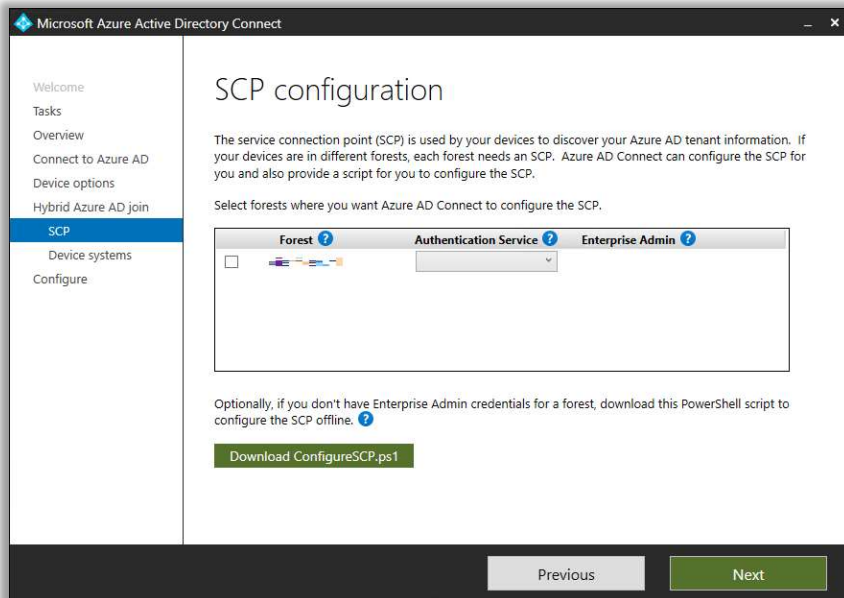
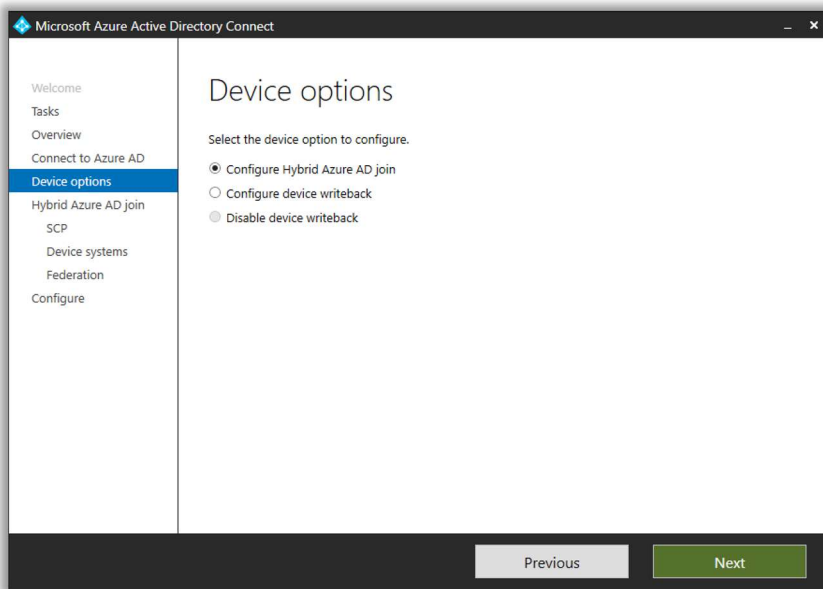
Enabling Hybrid Join for Windows 10 devices

In order to ensure that your Windows 10 devices that are joined to the local domain also become registered against Azure AD ("Hybrid-Joined"), you should check that the OUs containing the computer objects are syncing to Azure AD, and that the devices are all up-to-date.

Then, launch Azure AD Connect and pick the option to **Configure device options** from the *Additional tasks* screen.

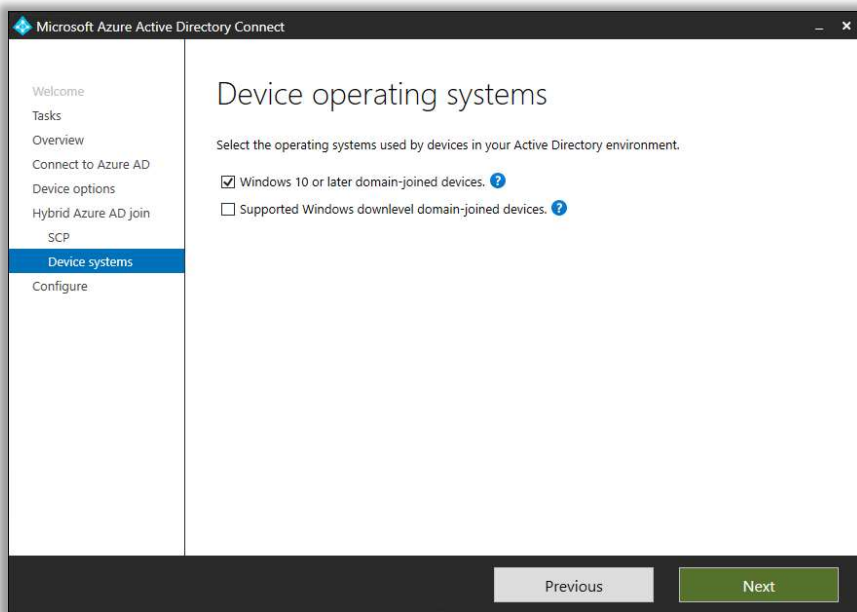


Go past the Overview screen and choose the option to **Configure Hybrid Azure AD join**.



Pick the forest, use the drop down to choose the Authentication Service and define an admin account with permissions to set the SCP. Otherwise, you can just download and run the PowerShell script on this page, which will configure the SCP. Click **Next**.

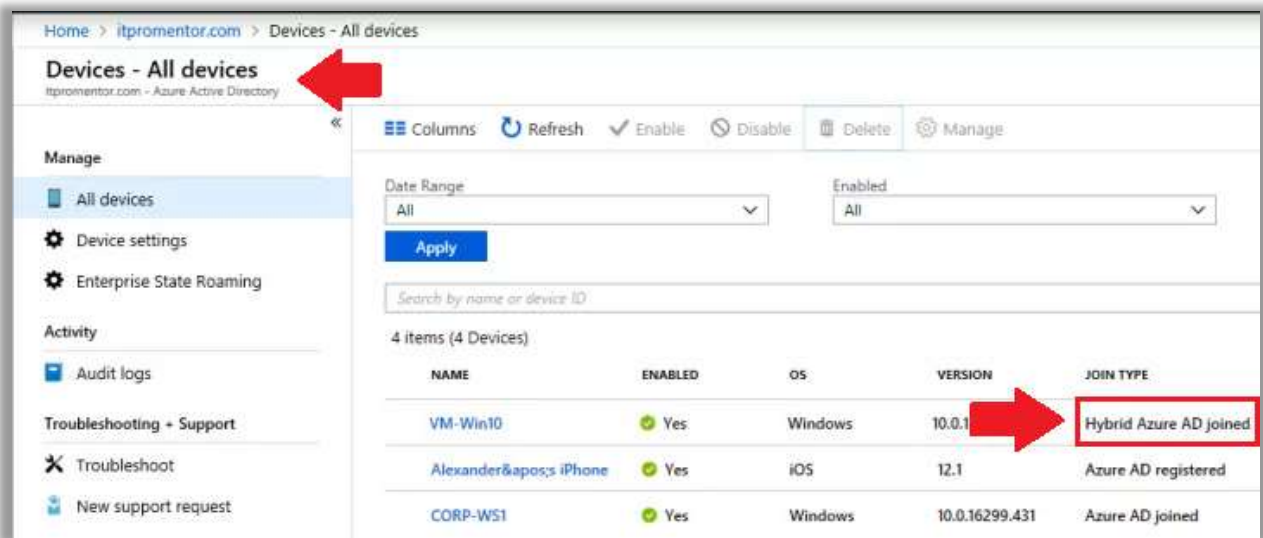
We aren't going to configure down-level devices—just Windows 10 (you get free upgrades, and there is no reason NOT to move to Windows 10, for 99% of SMB organizations). **Next** and **Configure** to finish.



Also configure this GPO setting for your domain:

- Create a new group policy object in your Active Directory linked to your Windows 10 Computer objects OU, or the root of the domain
- Name it (e.g. Hybrid Azure AD join)
- Edit and go to:
 - **Computer Configuration > Policies > Administrative Templates > Windows Components > Device Registration**
 - **Enable: Register domain-joined computers as devices**
 - For 2012R2: **Computer Configuration > Policies > Administrative Templates > Windows Components > Workplace Join**
 - **Enable: Automatically workplace join client computers**
- Apply and click OK

Now you should be good to go. You can confirm in the **Azure AD portal > Devices > All devices** that your local domain-joined Windows 10 devices are beginning to show up as “Hybrid Azure AD Joined.”



In case this isn't working for you, make sure you followed all the steps. Otherwise, you might try consulting this [troubleshooting guide](#) for hybrid join.

Windows 10 Deployment Options

Upgrade: Obtain Windows 10 installation media

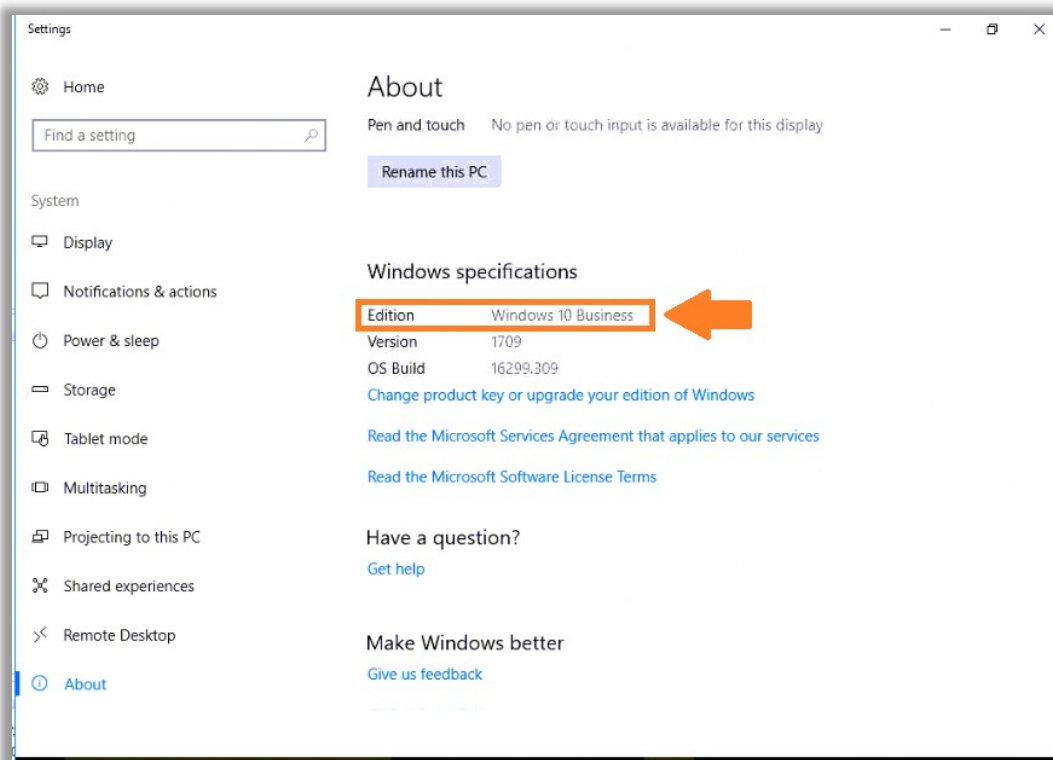
Microsoft has made it very easy for you to upgrade from earlier versions of Windows Pro. Since official support for Windows 7 ends in 2020, 2019 will prove to be a big year for Microsoft 365 Business indeed; the subscription entitles you to a free upgrade from 7, 8, or 8.1 Pro.

However, if any machines in your environment are 3 to 4 years old or more, just skip the upgrade—go right out and buy new Windows 10 hardware. Trust me, it's just better and you'll thank me—newer hardware from the last couple of years runs Windows 10 better than hardware that is older than that.

In broad strokes, the small business will usually perform a manual in-place upgrade to Windows 10, or, for new or reimaged devices, deploy Windows 10 using Autopilot, which is a new low-touch deployment method. Other classic deployment methods are also still available such as the MDT, WDS and so forth, but we won't cover those here.

You can create Windows 10 installation media from Microsoft's Media Creation tool found at [this link](#).

Once you install the new OS onto your device, and join the device to Azure AD, the Windows 10 upgrade rights will be applied. At this point the branding will change from Windows 10 *Pro* to Windows 10 *Business*. See this change under **Settings > System > About**.



Windows 10 Autopilot: Azure AD-Join

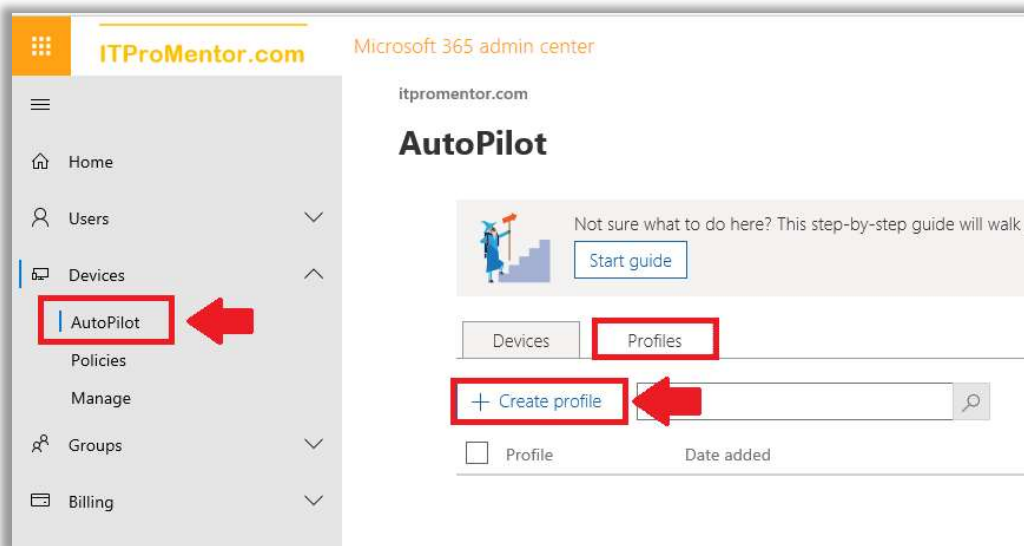
This is the easiest deployment method available to us, but it really applies only to newer hardware, or hardware that has been cleaned and repurposed. The goal is to get the device loaded with Windows 10 Pro, and sitting unconfigured at the OOBE setup screens. If you can make that happen, the end-user and Windows 10 Autopilot can do the rest, and all the user has to provide is their corporate credentials.

Quick aside: Using “Autopilot” with profiles and assigning devices in the portal—that’s all optional, technically speaking. The *full* Autopilot experience will mean that your device IDs will need to be provisioned in the portal before being sent out to end-users. This prevents the device from getting registered against any other tenant, and allows the user to get a “corporate-branded” OOBE (Out-Of-Box Experience).

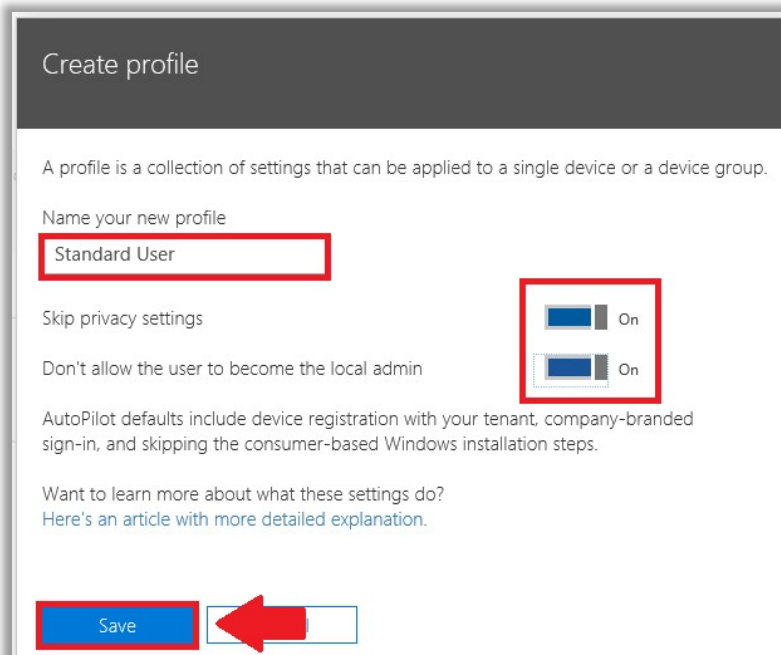
But, even without all this fanciness in place, the end-user could join any new device to Azure AD by specifying a work account during their OOBE setup, and *still* receive the necessary policies and enrollment, etc.—even the app deployments that you have configured. Nevertheless, *Autopilot* is recommended for a couple of reasons we will cover here, and it will probably get even cooler over time.

Create Autopilot profile

Create an autopilot profile from the Microsoft 365 Business admin portal. Navigate to **Devices > Autopilot**. Choose the **Profiles** tab and then + **Create profile**.



We don't have that many options at this subscription level, but they are the ones we want the most—**Skip privacy settings** and **Don't allow the user to become the local admin**. I recommend enabling both for most "Standard" user accounts.



Without Windows 10 autopilot configured, it is important to recognize that the default behavior will be to place the user who joined the machine to Azure AD automatically into the local administrator group. One of the primary benefits of getting Windows 10 autopilot going, then, is to prevent this from happening, and limiting privileged access on workstations.

Optionally, you can also create an **Admin User** profile, with the option **Don't allow the user to become a local admin** left set to **Off**. Then you can assign the different profiles to devices based on your requirements.

Add Autopilot devices

Today, there is no automatic way to get the necessary device ID information into Azure AD / Microsoft 365 Business. In the future, Microsoft promises to have some means of achieving this through hardware vendors (sounds like it will mostly apply to Enterprises—at least at first). Therefore, in order get the device ID manually exported from a device *today*, we need the help of PowerShell. Use this:

```
Install-Script -Name Get-WindowsAutoPilotInfo
```

```
PS C:\WINDOWS\system32> Install-Script -Name Get-WindowsAutoPilotInfo

PATH Environment Variable Change
Your system has not been configured with a default script installation path yet, which means you can only run a script
by specifying the full path to the script file. This action places the script into the folder 'C:\Program
Files\WindowsPowerShell\Scripts', and adds that folder to your PATH environment variable. Do you want to add the script
installation path 'C:\Program Files\WindowsPowerShell\Scripts' to the PATH environment variable?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

Untrusted repository
You are installing the scripts from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the scripts from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\WINDOWS\system32>
```

The script will be installed to this location:

```
C:\Program Files\WindowsPowerShell\Scripts\
```

To run the script, first enable unrestricted execution policy:

```
Set-ExecutionPolicy unrestricted
```

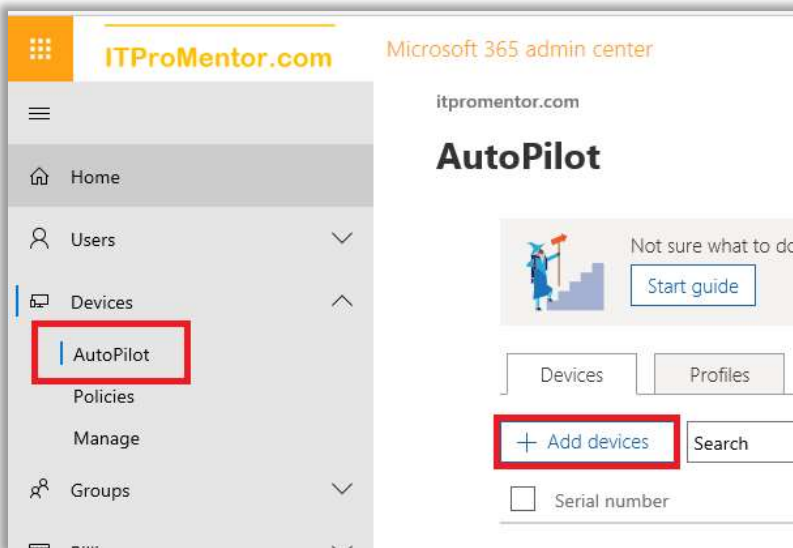
```
PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\WINDOWS\system32>
```

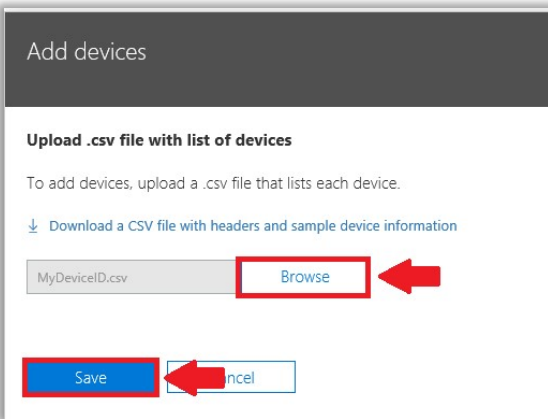
Finally, the command to execute the script is:

```
.\Get-WindowsAutoPilotInfo.ps1 -OutputFile .\MyDeviceID.csv
```

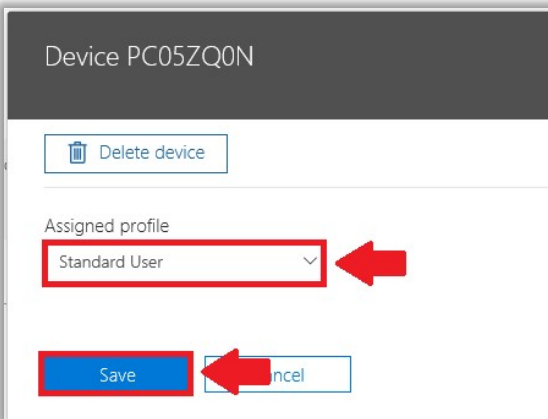
Once you have the csv file, you can upload this file into the Microsoft 365 Business admin portal. Go back to **Devices > Autopilot** and click on **+ Add devices**.



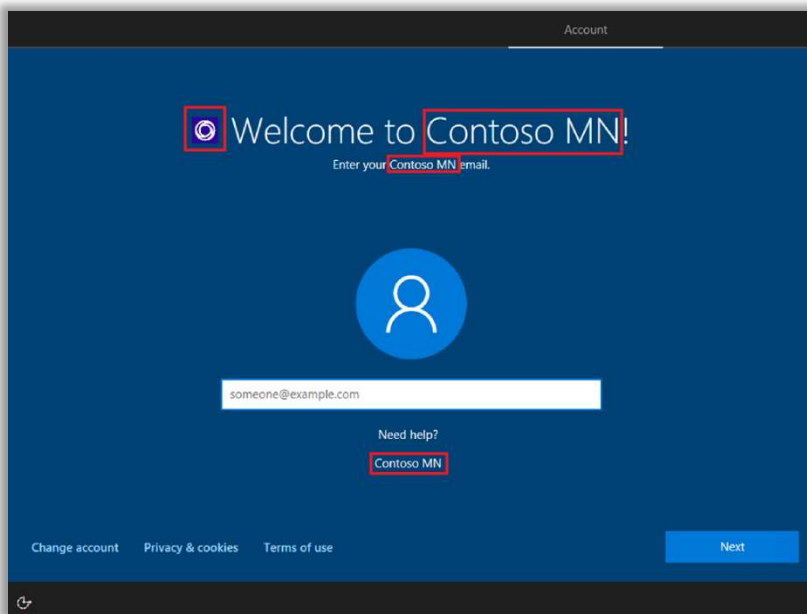
Browse to your csv file and upload it to the portal.



Once it is available, select your device and assign a profile to it. **Save.**



The result of this work, is that when a user identifies themselves to the device as belonging to the organization (signing in with their work/school account), then Azure AD will recognize the device and give the user a “low-touch” deployment experience, joining the device to Azure AD and enrolling it with the Intune service for MDM in the process.



If you remember the initial policies we configured via the Microsoft 365 Business setup, including the Windows 10 device configuration policies as well as the option to install the Microsoft 365 Business software, and manage the applications—all of that will also take place as part of the Autopilot deployment.

In case you need to do any troubleshooting with the enrollment process, check out [this Microsoft TechNet article](#).

Windows 10 Autopilot: Hybrid-Join

Autopilot was initially only possible for Azure-AD Joined devices (non-Hybrid). If you use the default method which is exposed via the Microsoft 365 Business admin center, then the device state of the local computer will be Azure AD-Joined at the end of the process.

However, using an on-premises Intune connector service, it is now possible to enable a Hybrid-Join experience with Windows 10 Autopilot. This feature is still in preview at the time of this writing, and is available only via the Intune portal (the option does not appear in the Microsoft 365 admin portal yet).

The major pre-requisites here are:

- You must already have Hybrid Join enabled and working via Azure AD Connect
- Elect a Windows Server 2016 server for the Intune connector service
- Delegate permissions to create computer objects to an Intune service account
- Autopilot devices must be on-site with the local Active Directory (VPN is not supported)

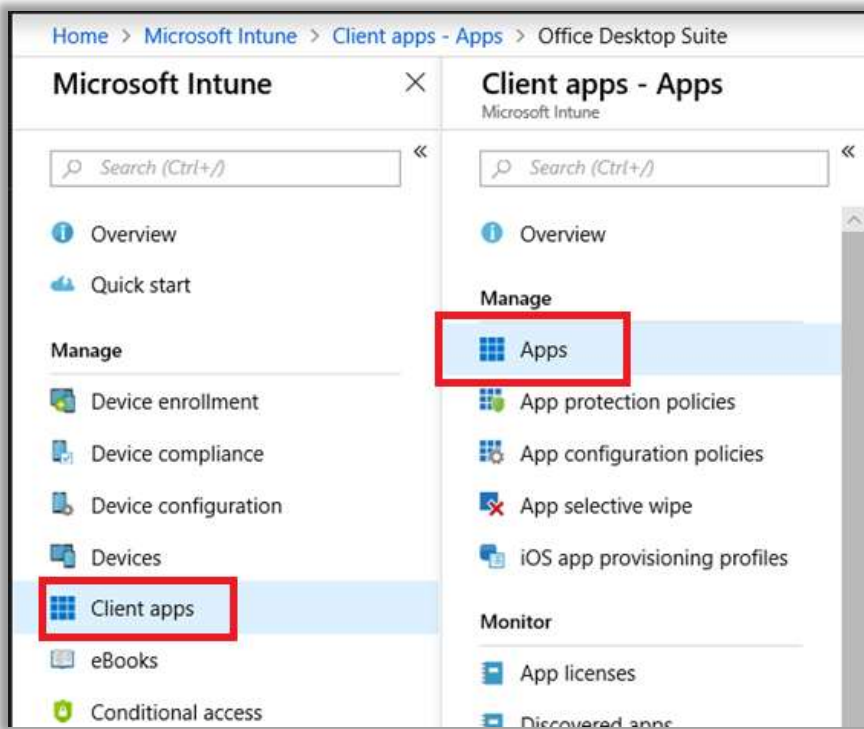
I am not going to cover this process—as I mentioned this feature is still in preview, and is targeted more at Enterprise environments with long-term hybrid coexistence needs. You may refer to the [full article](#) at Microsoft which describes the process in detail if it suits your needs.

Application Deployment

As we mentioned in the beginning of this guide, Microsoft 365 Business includes the ability to deploy the Microsoft Office applications automatically to Windows 10 machines over the air.

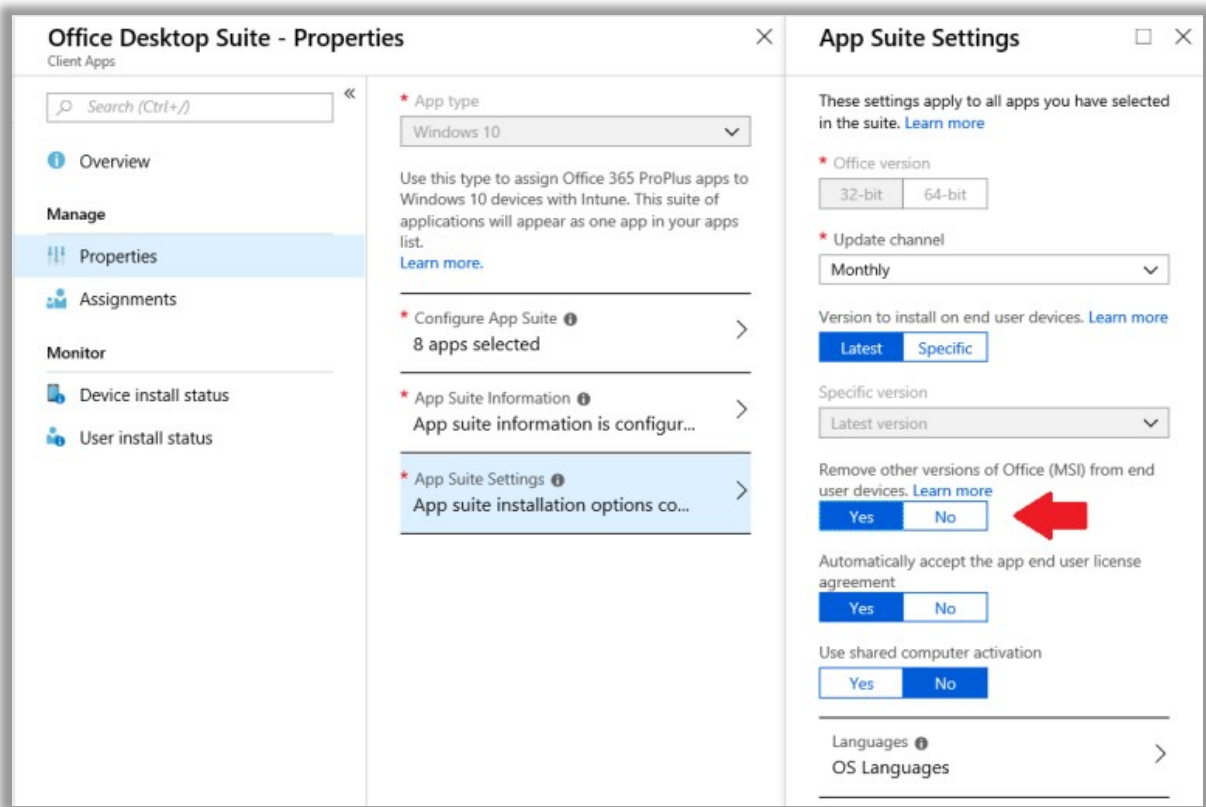
However, the default options for application deployment, via the 365 admin portal, leave something to be desired. Therefore, we can look under the hood at Microsoft Intune for ways to fine tune the deployment, and as a bonus, you will find that it is possible to perform many other types of over-the-air application deployments, and on multiple device platforms.

To create customized app deployments, we can navigate our way to the Intune Device Management portal. Go to **Client apps > Apps**.



Edit the **Office Desktop Suite** policy. You can ignore the references to ProPlus in here, since you do in fact have a *Business* subscription with Microsoft 365 *Business*. When your users sign into the applications only the bits for the Business edition will light up.

Here you can see some interesting additional settings. Check out **Properties > App Suite Settings** and find the option to **Remove other versions of Office (MSI) from end-user devices**.



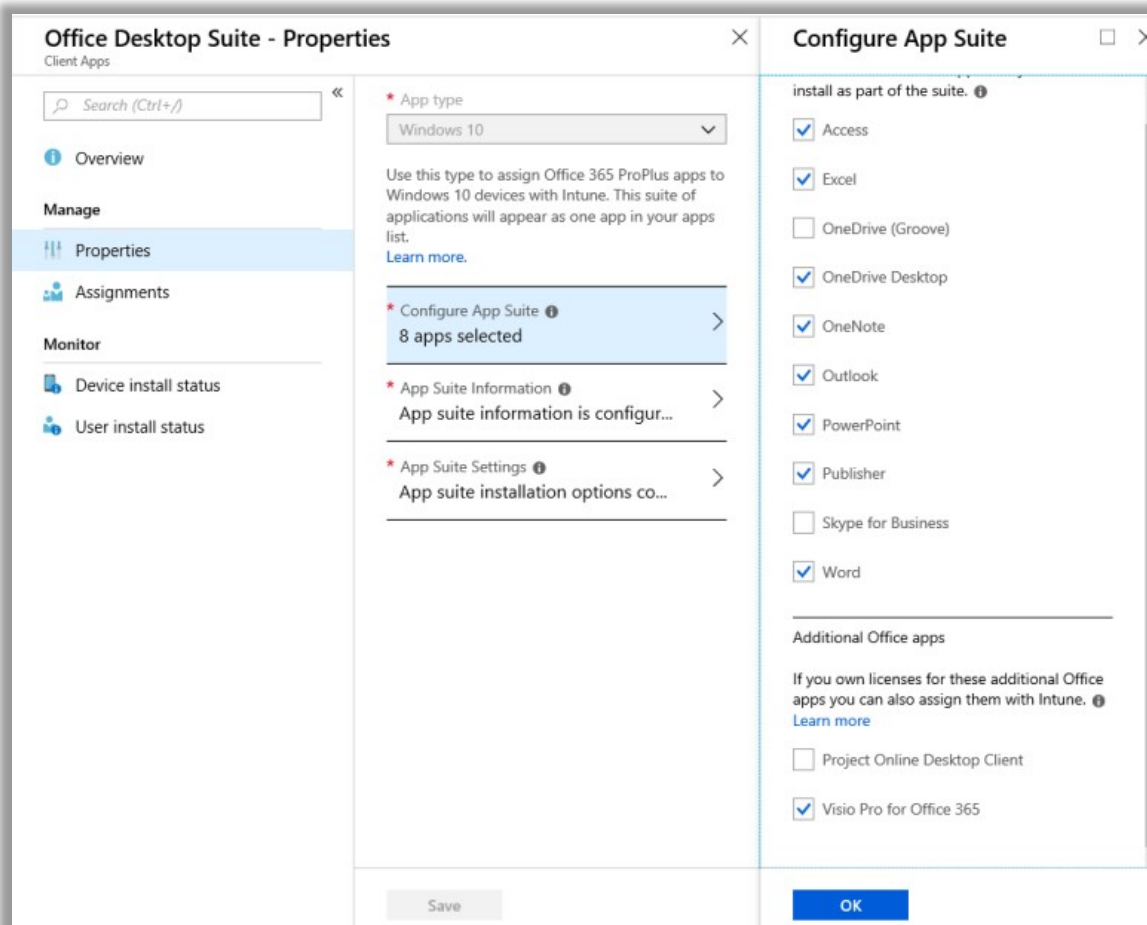
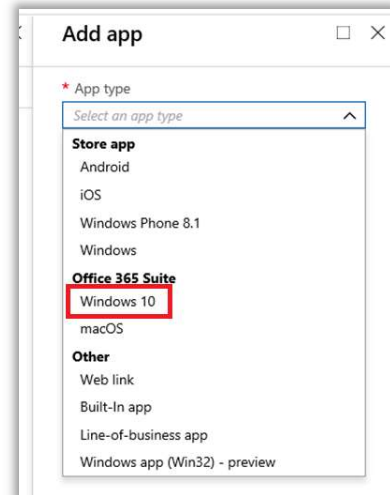
You will notice that this default policy is configured to deploy *32-bit* versions of the Office apps, but if 64-bit is a requirement in your environment, it would also be possible to configure another policy to deploy 64-bit, instead.

In general, I do not recommend modifying the policies which are created through the Microsoft 365 admin center. Instead, always be building your own custom policies.

Now, as you're building: you can also choose to assign apps from the Android, iOS and Windows Stores. You can configure Office 365 software assignments to both Windows 10 and macOS. You can also deploy Line of business applications and Win32 apps (MSI) as well. So as you can see, there's plenty to explore beyond what Microsoft provides via the 365 Admin center.

Just click on **Add** to add a new app. Let me create a policy that will deploy C2R versions that are 64-bit instead of 32-bit, and I'll include Visio, since I have a subscription for that software also. In this example I chose **Office 365 Suite > Windows 10**.

Then under **Configure App Suite**, choose the applications you want to deploy; I do not include OneDrive (Groove) or Skype for Business. But I will add Visio Pro—since several workers in my organization utilize this app heavily.

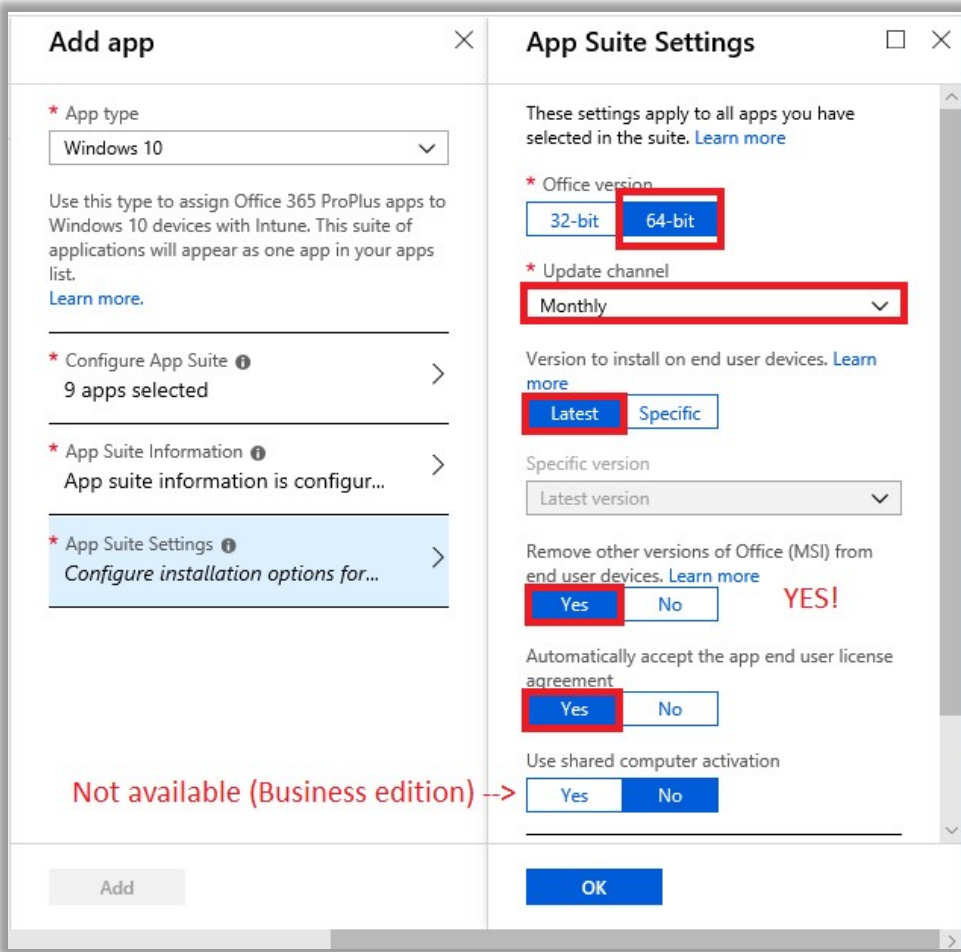


Then under **App Suite Information** I just have to fill in a name and description for this App suite.

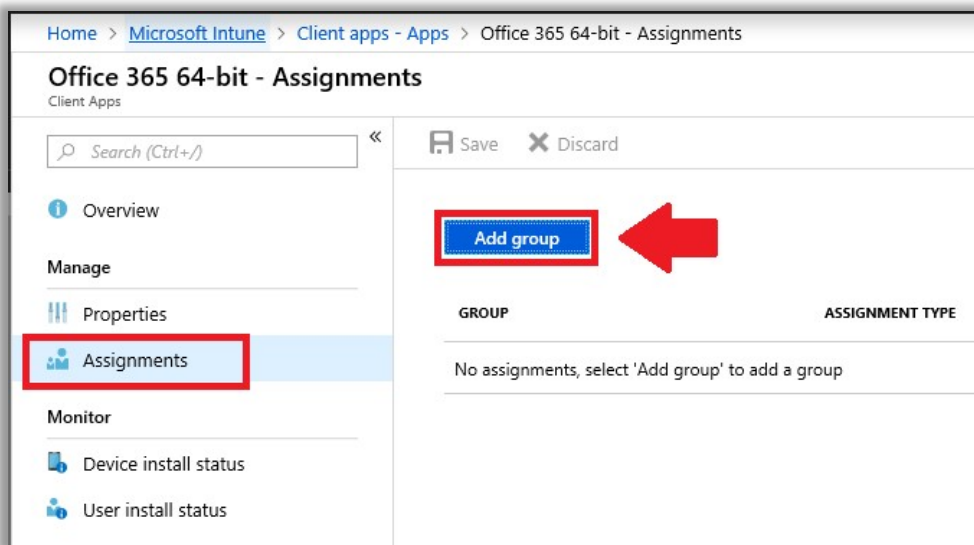
The image shows two overlapping dialog boxes. The left dialog, titled 'Add app', has a close button (X) in the top right. It contains a dropdown for 'App type' set to 'Windows 10'. Below this is explanatory text and a 'Learn more' link. There are three expandable sections: 'Configure App Suite' (9 apps selected), 'App Suite Information' (highlighted in blue, with the text 'Configure the app suite informati...'), and 'App Suite Settings' (with the text 'Configure installation options for...'). An 'Add' button is at the bottom left. The right dialog, titled 'App Suite Information', has a maximize button (square) and a close button (X) in the top right. It contains several fields: 'Suite Name' (Office 365 64-bit, green checkmark), 'Suite Description' (Office 365 64-bit, green checkmark), 'Publisher' (Microsoft), 'Category' (Productivity), a 'Display this as a featured app in the Company Portal' toggle set to 'No', 'Information URL' (placeholder: Enter a valid url, green checkmark), and 'Privacy URL' (placeholder: Enter a valid url, green checkmark). An 'OK' button is at the bottom center.

Click **OK** and switch to **App Suite Settings** to choose your options: **64-bit**, the **Monthly update**, and **Latest version**. Since my users already have 32-bit MSI Office installs, I want to **Remove other versions of Office (MSI) from end-user devices**. I will also choose to **Automatically accept...** for the EULA. Click **OK**.

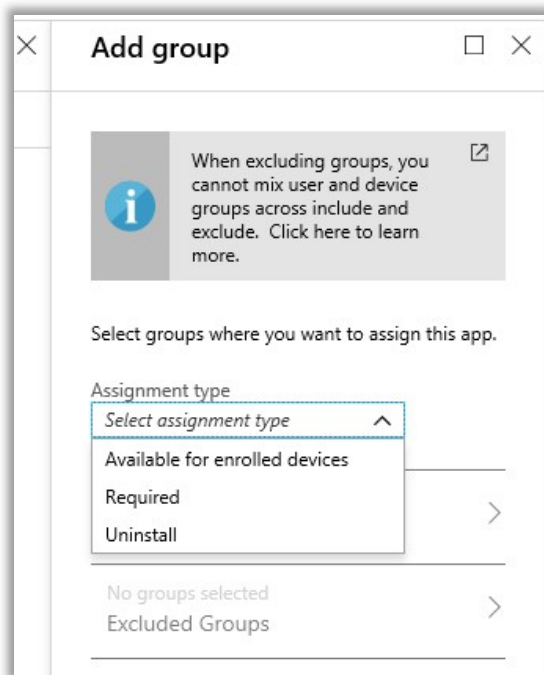
*Note: The option to **Use shared computer activation** is not available with the Business edition of the Office 365 apps; this feature is only available for ProPlus / Enterprise SKU's.*



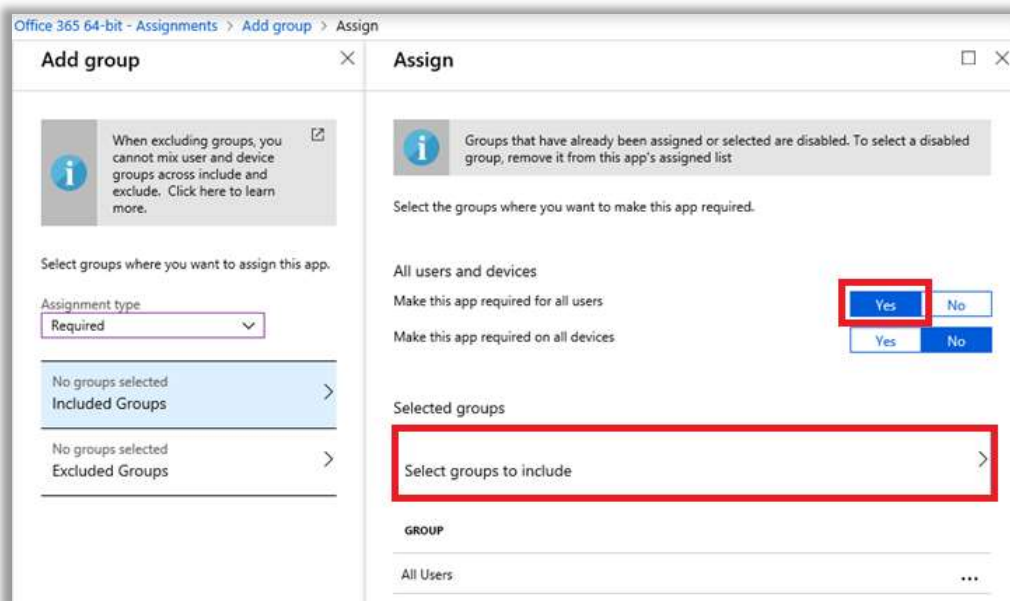
Finally, we just have to assign this application suite. Click on **Assignments**, then **Add group**.



For Assignment type, you would choose **Required**. Notice that one of the other assignment types available is **Uninstall**, so keep in mind that you can use this option, too, if you ever need to remove a previously assigned version, such as a 32-bit assignment.



To select a group, pick **Yes** for **Make this app required for all users**, or **Select groups to include** (I chose the **All Users** group in this simple example—but you can create groups to assign apps).



This app deployment stuff is a pretty magical experience for an IT admin, since it saves what would otherwise be manual installation steps (either for you or your users). Especially when you have to provision a few dozen new machines, that can add up to *a lot* of time.

We are getting to the point now where I can explain where all of this is leading. If you can gather a complete inventory of users, devices and their software applications, by leveraging Microsoft 365 you can:

1. Manage and protect the **user identities** using strong, modern authentication

2. Manage and protect the **devices**, forcing them to become registered and managed (and know which are assigned to whom)
3. Manage and protect your **applications** (and know which are assigned to whom)

And what this all means is...can you guess? Answer: *You can limit privilege*. The ideal scenario, then, is if you're able to assign a full inventory of applications, then you don't need to allow users to become local administrators (enforced via Autopilot). As soon as they pick up a new device, their apps and data will come to them, simply because they are able to provide their identity and a second factor of authentication.

Therefore, I recommend you spend a fair amount of time getting to know these capabilities, and learn how to deploy the apps that are used most frequently in your own organization or customer base.

Mobility Management via Intune: MDM vs. MAM

Microsoft Intune has two different built-in mobility management solutions: Mobile Device Management (MDM), and Mobile Application Management (MAM).

MDM, or device-based management, is often leveraged when you have corporate-owned and managed devices. Intune's MDM can manipulate every conceivable lever on a device and control a great many settings. For example:

- Push Wi-Fi and VPN profiles to the device
- Push business applications to devices
- Manage updates to devices
- Use corporate PKI and certificates
- Control use of apps, and access to the app store
- Lock down the use of certain device functionality

I normally only see larger-sized organizations entertaining these types of options, or generally situations where corporate-owned devices are being strictly controlled and "made the same" for various groups of users. In an Enterprise, you would likely configure different profiles and device rules for different kinds of users in various roles and locations.

| Mobility Concerns | MDM (corporate-issued) | MAM (BYOD) |
|-----------------------------|---------------------------|-------------------------------|
| Unauthorized access | Require device enrollment | Require protected app |
| Compromised account | Require device PIN | Require app PIN |
| Compromised device | Encrypt device data | Encrypt app data |
| Jailbroken device | Require compliant device | Check for jailbreak on launch |
| Lost or theft | Wipe device data | Wipe app data |
| Termination | Wipe account data | Wipe app data |
| Prevent data leakage | Manage device apps | Restrict copy/paste/save |

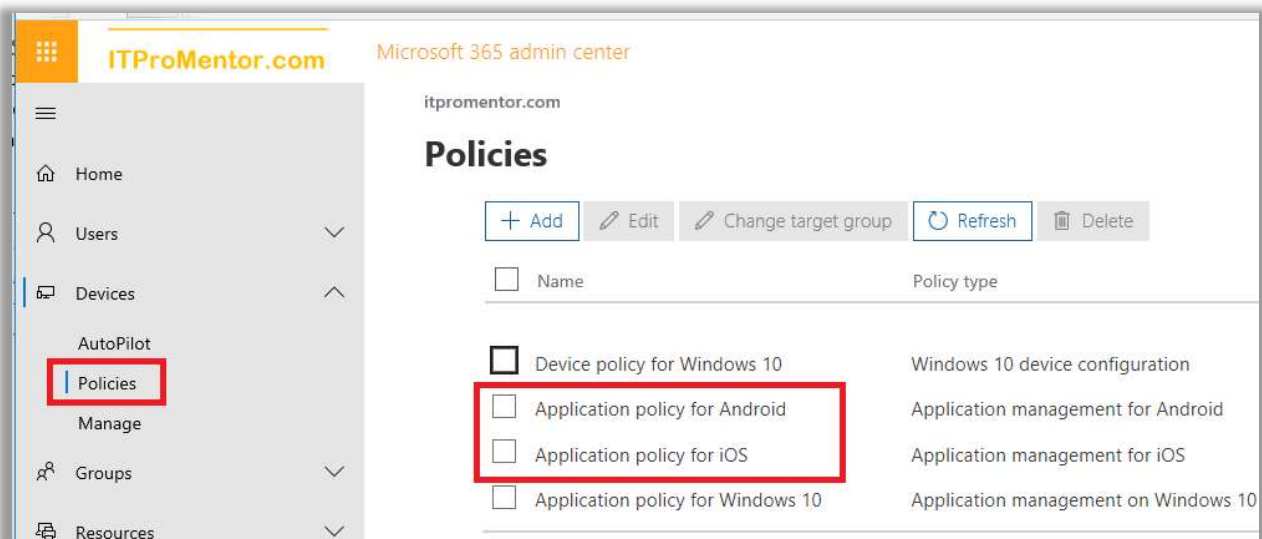
Mobile Application Management (MAM) is an alternative, which allows for BYOD scenarios. In the small to mid-sized business, almost all users are “BYOD” —using their own mobile devices to access corporate email and other digital resources. Thus, it makes sense to start with MAM, usually, in the SMB.

Notice too, that the Microsoft 365 Business device policies we deployed via the admin portal are really *application* policies (MAM). This follows the traditional setup where the business issues its users corporate-owned Windows 10 devices, but it’s assumed BYOD for mobile phones and/or tablets.

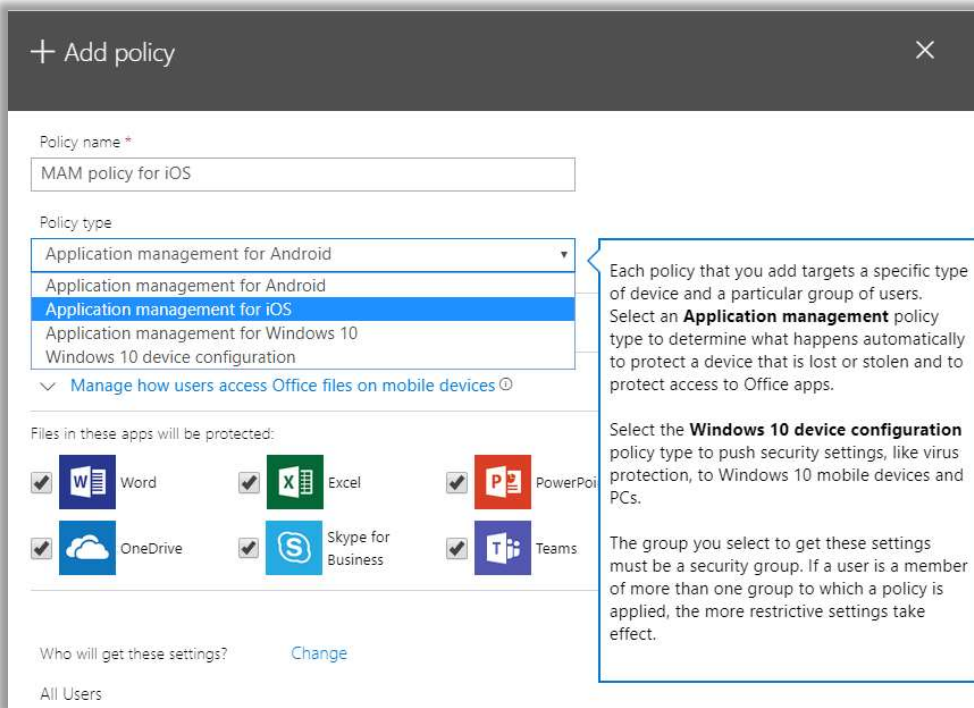
The best part about MAM: end-users have no enrollment process to speak of. Instead, they just get a one-time prompt that their application settings are being managed (and they have to restart the app). Therefore, MAM is a very attractive alternative to MDM, with many of the same benefits while being minimally invasive to users.

Configuring MAM for iOS and Android

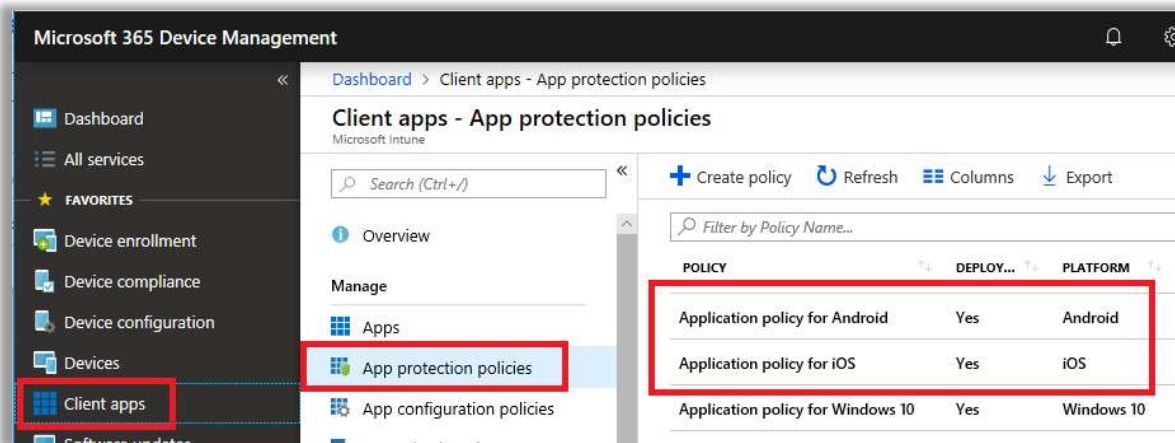
Navigate back to the Microsoft 365 admin center, and go to **Devices > Policies**. Review the application policies that we created when the subscription was first set up.



Or, if they are not set up yet, you can **Add** them now. The selections are very simple to make. Note that you can also scope different policies to different user groups.



Again, you can find the same policies from the Device management portal, at <https://devicemanagement.microsoft.com> > **Client apps** > **App protection policies**.



The same rules apply here as I described with the Windows 10 policies—if you make any modifications to these default policies, be sure to make them via the Microsoft 365 admin center. If you want customizations not covered here, create new policies and re-assign them, completely outside of the Microsoft 365 admin center.

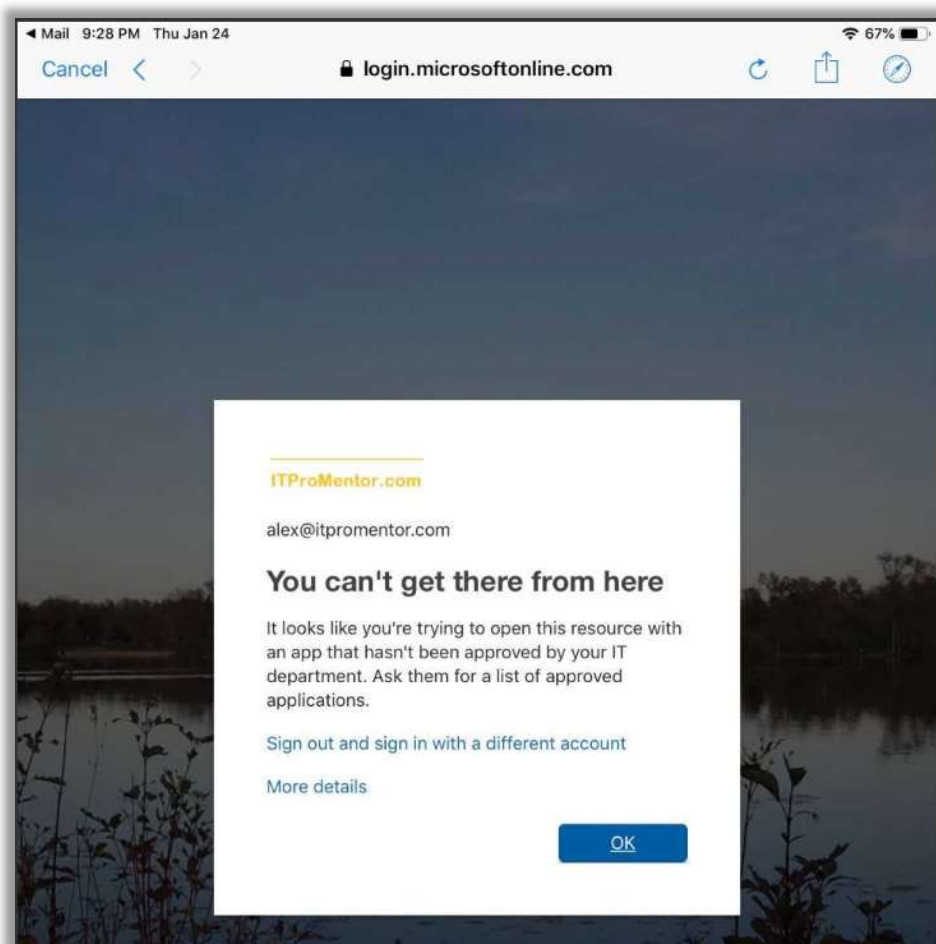
Use Conditional Access to require MAM for BYOD devices

At this stage, if your users were to download the Outlook app for iOS or Android, they would be protected by the settings that you specified in your app policies. But, without Conditional Access, there is no means of “enforcing” the use of Outlook for email.

Therefore, if your intention is to protect corporate data on mobile devices using MAM, then you are going to want a Conditional Access policy which requires the use of “managed” (read:

Microsoft) apps, and those apps alone. This is one of the major oversights, in my opinion, within the Microsoft 365 Business subscription. Why give us MAM and then leave out the one tool that would allow us to enforce the use of the supported apps?

The experience we want for end-users is this: adding an email profile to the native mail app on a mobile device will result in the access being blocked, with a message about using a supported app.

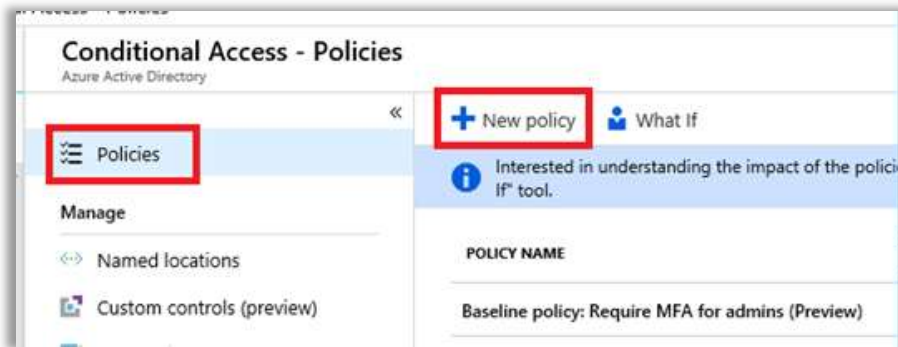


This will require two policies: one that targets modern authentication clients, and one that targets Exchange ActiveSync clients.

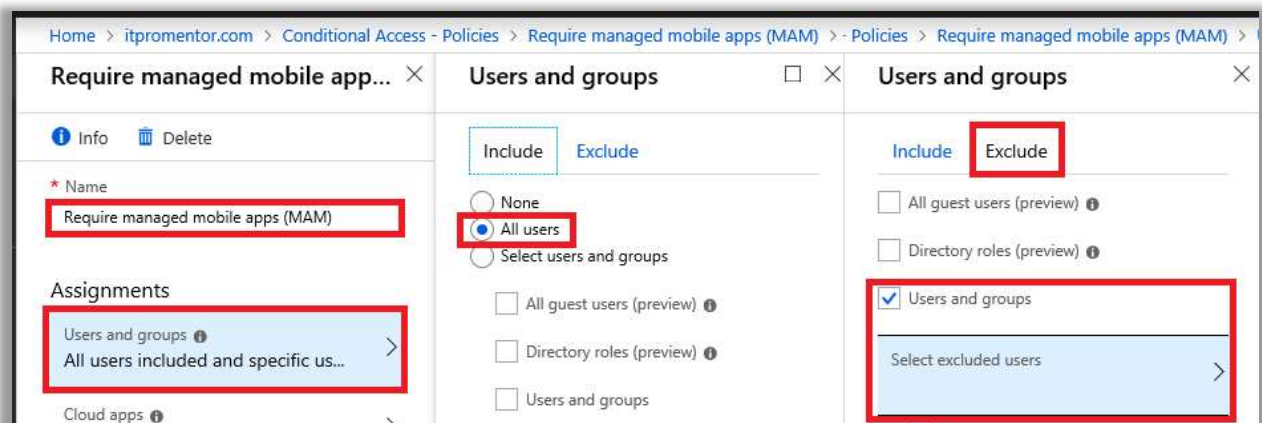
Warning: *If the user has an existing native mail profile, then enabling this policy means they will get a password prompt—it just stops working. However, if you attempt to add the account as a new profile to the native app, it will display a message to the end-user after sign-in, explaining that the app is unsupported. Therefore, instruct users to move to the Outlook app in advance, if possible, and warn them they should expect to lose access to email on the old app.*

Policy #1: Require MAM for modern clients

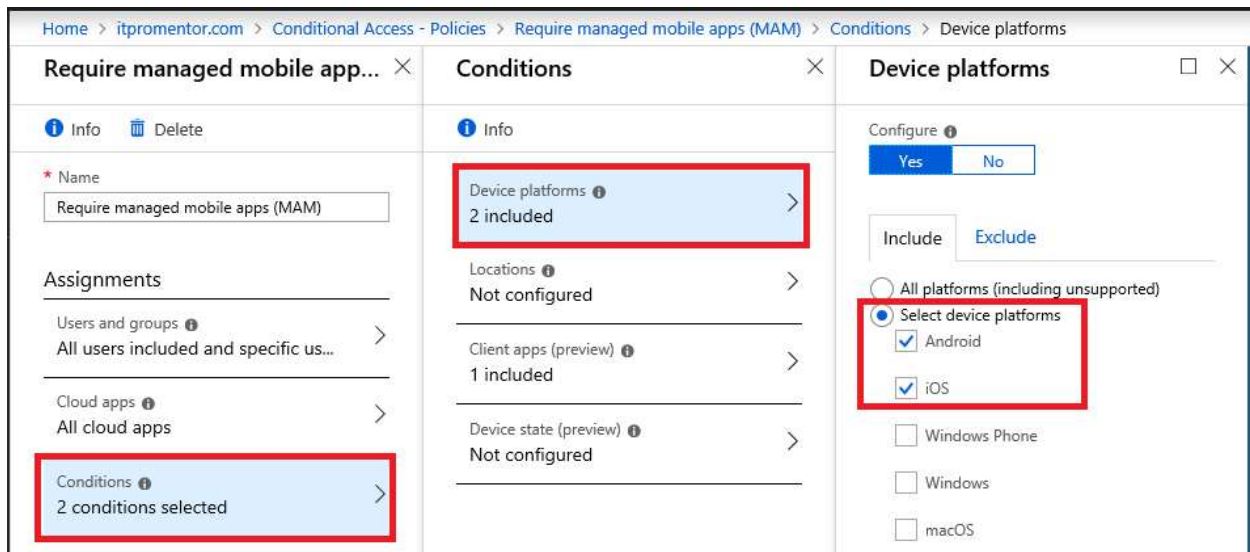
Select **Policies** > **+ New policy**.



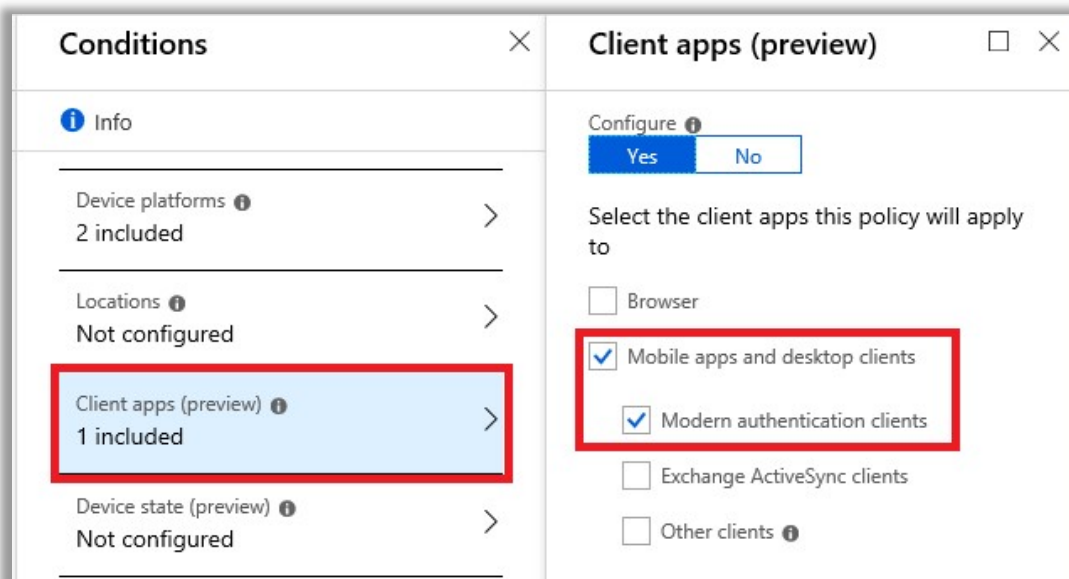
I will name my policy "**Require managed mobile apps (MAM)**" and pick my assignments. I want this policy to apply to **All users**, but you can (and probably should) scope it to a group, and/or exclude at least one admin account. Otherwise, you can also constrain the assignment to a security group such as *BYOD Users*, populated with individuals who will bring their own mobile devices.



Choose **All cloud apps**. For **Conditions**, under **Device platforms**, select only **Android** and **iOS** (these are the only platforms that support the access control "*Require approved client app*").



The only other condition you need to specify is **Client apps**; select **Mobile apps and desktop clients** and the option for **Modern authentication clients** only.



Now, under **Access Controls**, pick **Grant** and make the selections pictured—**Require approved client app** and **Require all of the selected controls**.

Home > itpromentor.com > Conditional Access - Policies > Require managed mobile apps (MAM) > Grant

Require managed mobile app... ✕

Info 🗑️ Delete

All cloud apps >

Conditions 📘 >
2 conditions selected

Access controls

Grant 📘 >
1 control selected

Session 📘 >
0 controls selected

Enable policy

On Off

Grant 🗑️ ✕

Select the controls to be enforced.

Block access

Grant access

- Require multi-factor authentication 📘
- Require device to be marked as compliant 📘
- Require Hybrid Azure AD joined device 📘
- Require approved client app 📘
[See list of approved client apps](#)

For multiple controls

Require all the selected controls

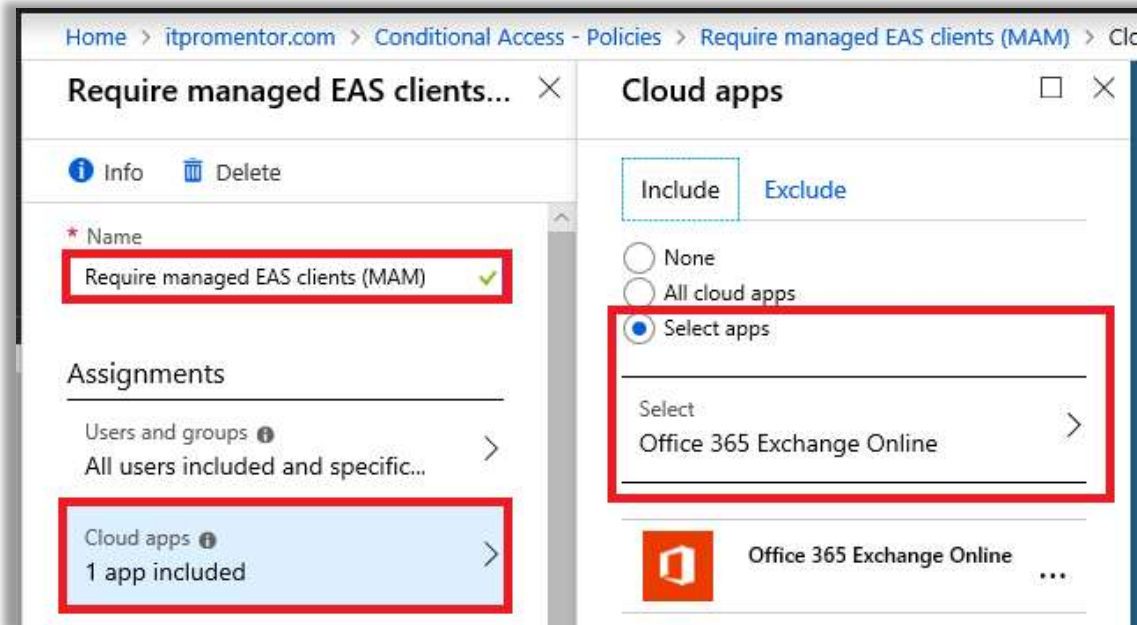
Require one of the selected controls

Policy #2: Require MAM for EAS clients

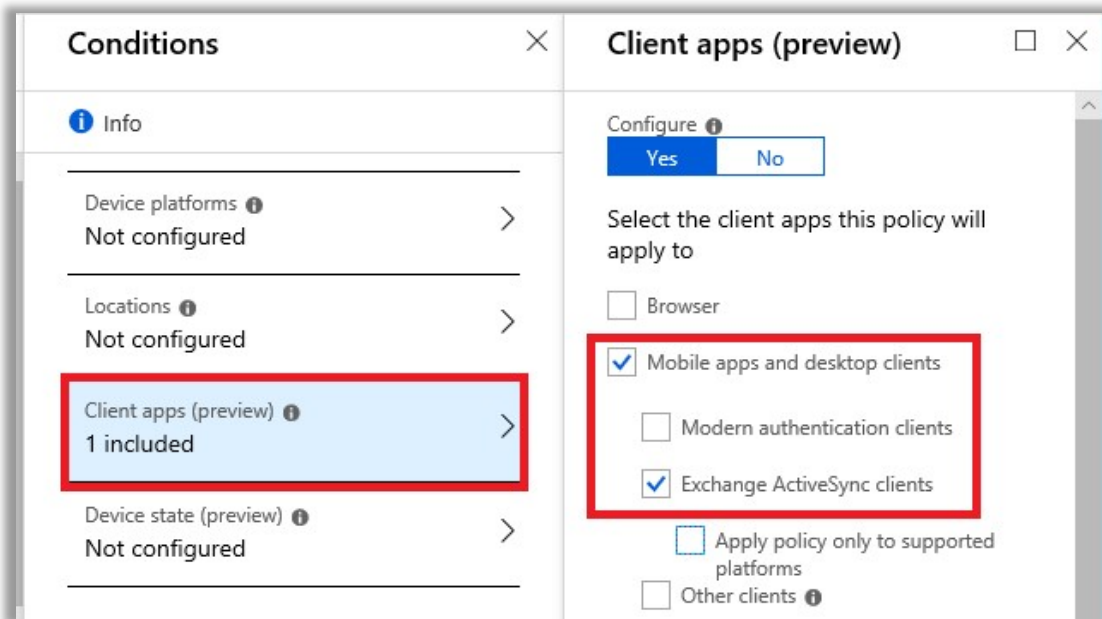
Microsoft does not support mixing Exchange ActiveSync (EAS) client targeting with any other conditions or client types. Therefore, we need a second policy to protect EAS clients, or those which do not support modern authentication.

Create a new policy. Name it something descriptive like *Require managed EAS clients (MAM)*. I will again assign the policy to **All users**, excluding an emergency admin account. Or, again, an alternative group such as *BYOD Users*.

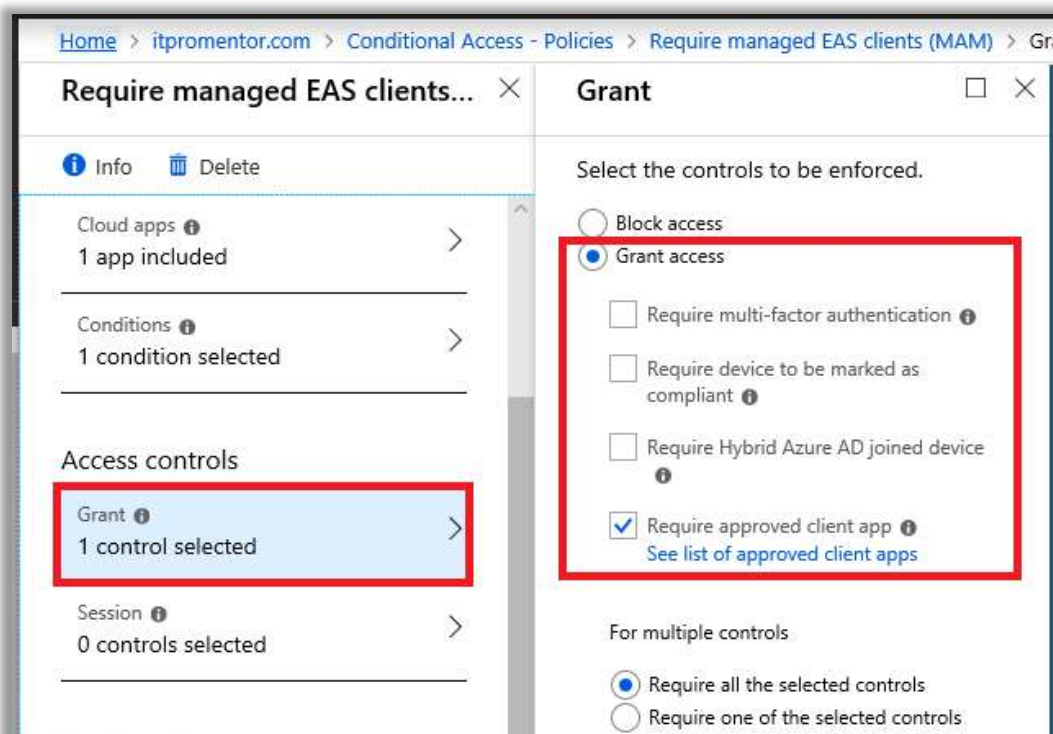
Under **Cloud apps**, select only **Office 365 Exchange Online**.



Microsoft does not support mixing EAS-targeted policies with any other conditions, or any other client types. Therefore, under **Conditions**, you will need to make the selections as pictured, for **Client apps** only, **Mobile apps and desktop clients** > **Exchange ActiveSync clients**.



Finally, based on the **Access controls**, go ahead and **Grant access** with **Require approved client app** as pictured.



Configure MDM for iOS and Android

As previously mentioned, full MDM is sometimes required by organizations, especially where corporate-owned devices are being issued to individuals, or where very strict compliance rules require it—in these situations, the company typically prefers to maintain a lot more control over

their property. To get a basic MDM deployment up and running, we will need to complete five steps:

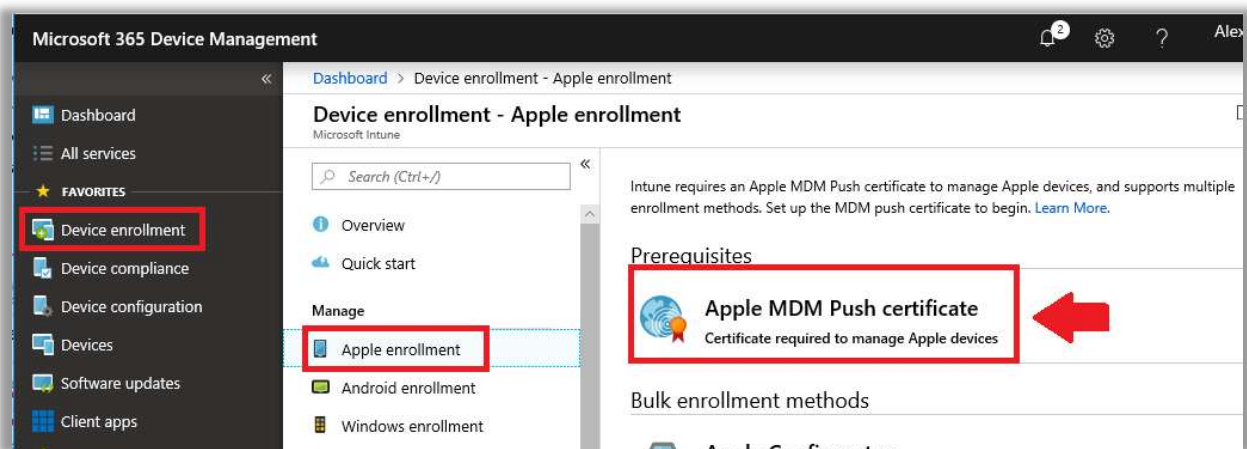
- Configure Apple MDM Push certificate
- Configure Device compliance policies
- Configure Device configuration profiles
- Setup Conditional Access
- Enroll the mobile devices

There are many other things that Intune can do—but completing these items are generally where you would start. The scenario that I will cover here describes a very basic MDM deployment:

- Managed email profile (this means email auto-deployed to the *native* mail app)
- Enforce passcode / device encryption
- Prevent jailbroken devices

Configure iOS Enrollment

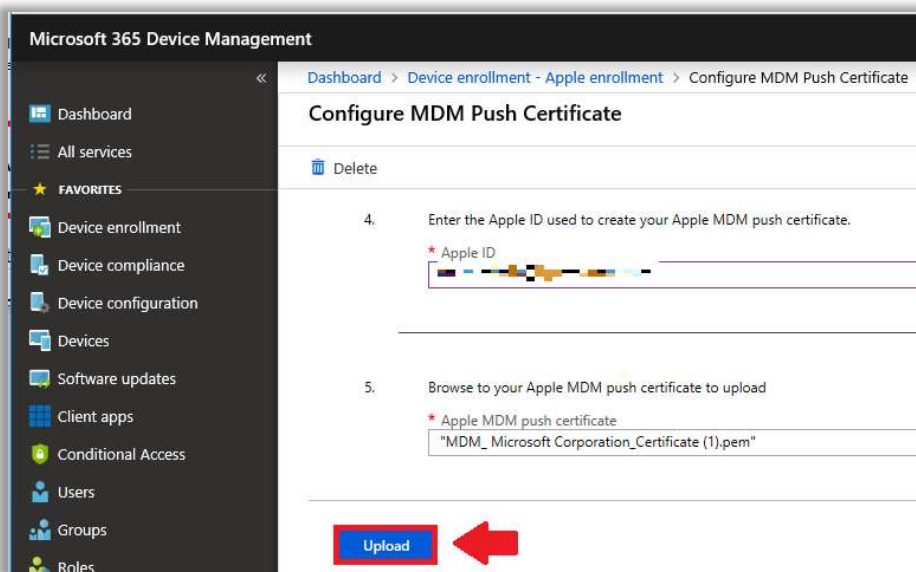
Before you can enroll Apple devices for full MDM, you need to obtain an Apple Push Notification Certificate. This is pretty easy to do. From the [Device management](#) portal, go to **Device enrollment > Apple enrollment > Apple MDM Push certificate**.



Simply follow the process laid out on this page—basically you just need to download the CSR (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](#).



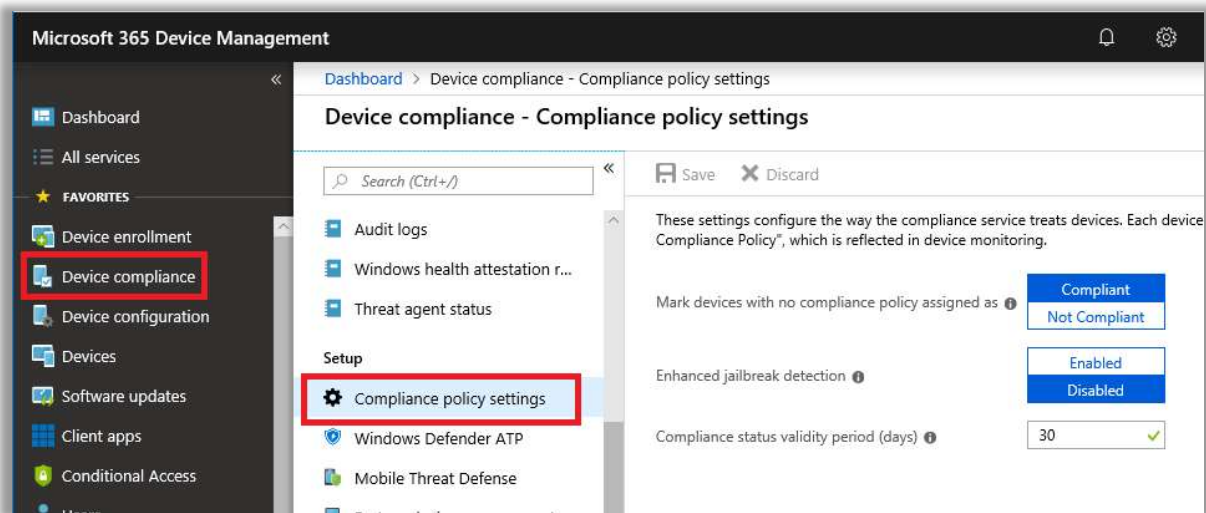
Upload the CSR to Apple, and then download the certificate that Apple provides you with. You will return to the Microsoft 365 Device management portal and upload the certificate here.



Device compliance policy settings

A *device compliance policy* ensures that your organization's devices maintain a minimum baseline that you, the administrator, have intended for them. For example, you can require passcode and device encryption, as well as minimum acceptable OS versions. Device compliance flows through to Conditional Access policies (meaning that non-compliant devices can be blocked from access).

Before we configure a device compliance policy, look at the settings which govern device compliance generally, from **Device compliance > Compliance policy settings**.



The first option is very important: **Mark devices with no compliance policy assigned as:** *Compliant* or *Not Compliant*. Please be careful with this—obviously it is better from a security standpoint to treat devices without a policy as *Not Compliant*, however if you have previously configured a Conditional Access policy which grants access based on the conditions of device compliance, then this could impact users and devices which do not yet fall under the scope of a compliance policy. At the time of this writing the default is still *Compliant*, but *Not Compliant* is on the horizon to become the default soon, according to Microsoft—so be aware of this setting. Ideally you will onboard your devices first, then change this setting second.

Enhanced jailbreak detection will require the device to check in with Intune more frequently, and has an impact on battery life due to location services. It is off by default and I don't know many admins who prefer to turn it on. Here is a list of what it does, from Microsoft:

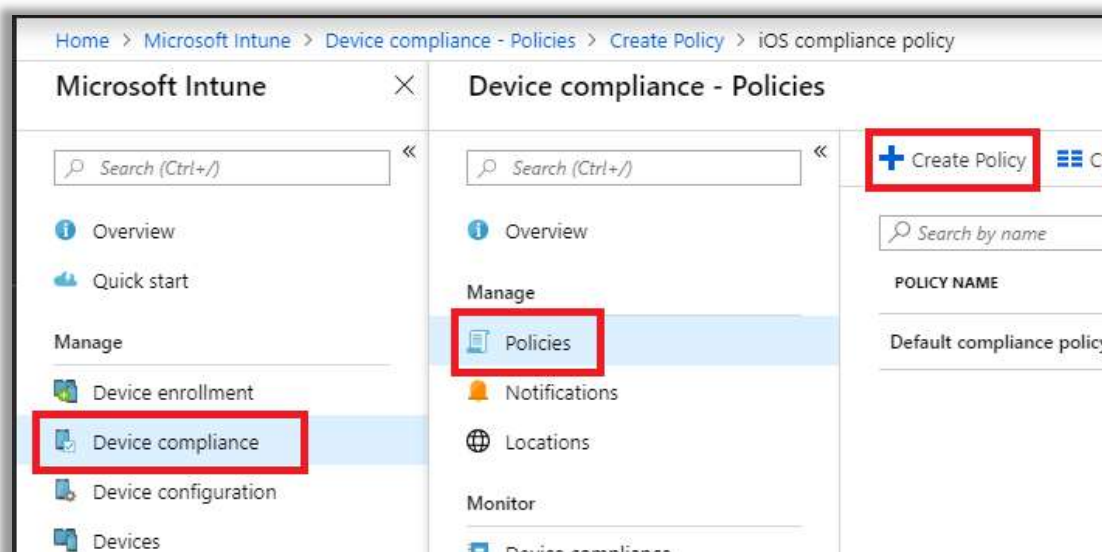
Enabling this setting requires devices to:

- *Enable location services at the OS level*
- *Allow the company portal to use location services*
- *Evaluate and report its jailbreak status to Intune at least once every 72 hours. Otherwise, the device is marked not compliant. Evaluation is triggered by either opening the Company Portal app or physically moving the device 500 meters or more. If the device doesn't move 500 meters in 72 hours, the user needs to open the Company Portal app for enhanced jail break evaluation.*

The default value for **Compliance status validity** is *30 days*. It is like a timeout value: if no status update from the device is received within this timeframe, then the device will be marked non-compliant. I usually dial this down to a more moderate 15 days.

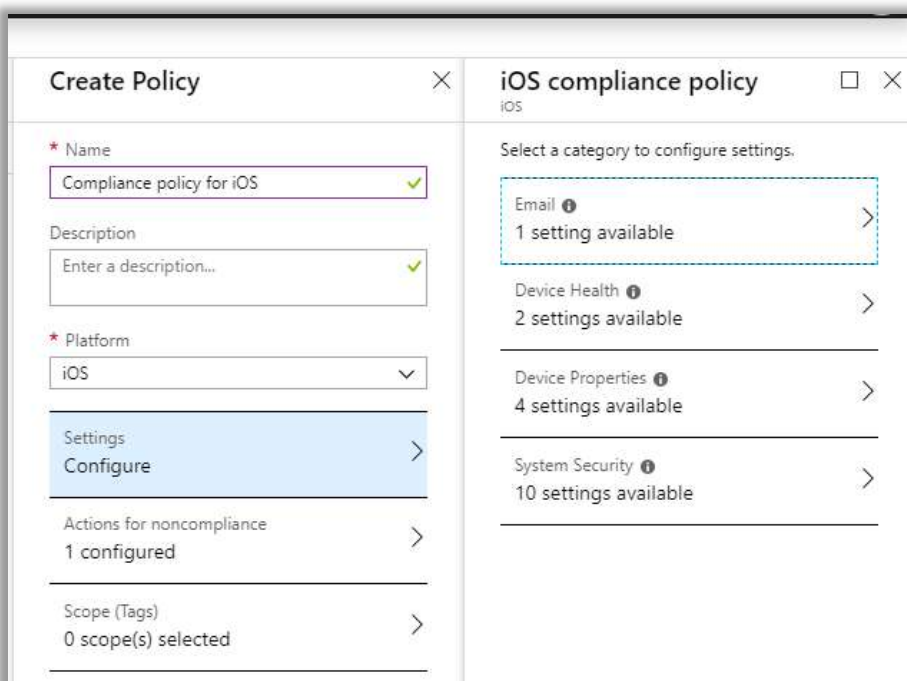
Configure a device compliance policy

You should configure at least one compliance policy for each platform. Go to **Device compliance > Policies > Create Policy**.

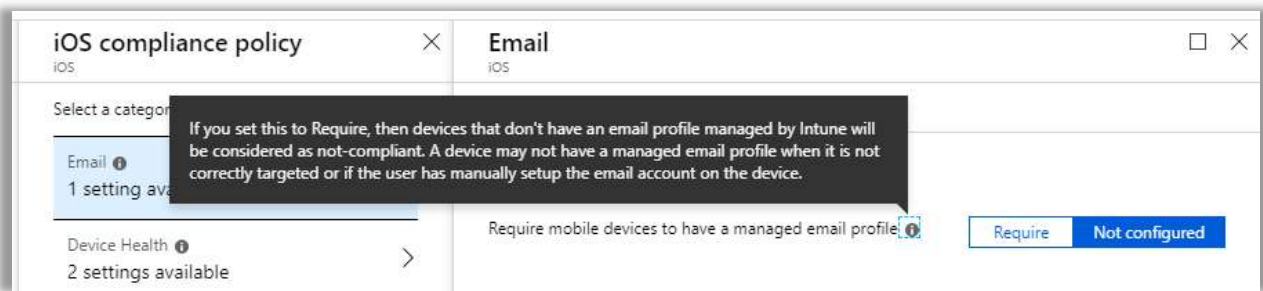


You can only select a single platform for any given policy. You will notice that Windows, iOS, Android, and even macOS have support in Microsoft Intune/Device management. You would want to create policies for each type of device that you expect to have in the organization.

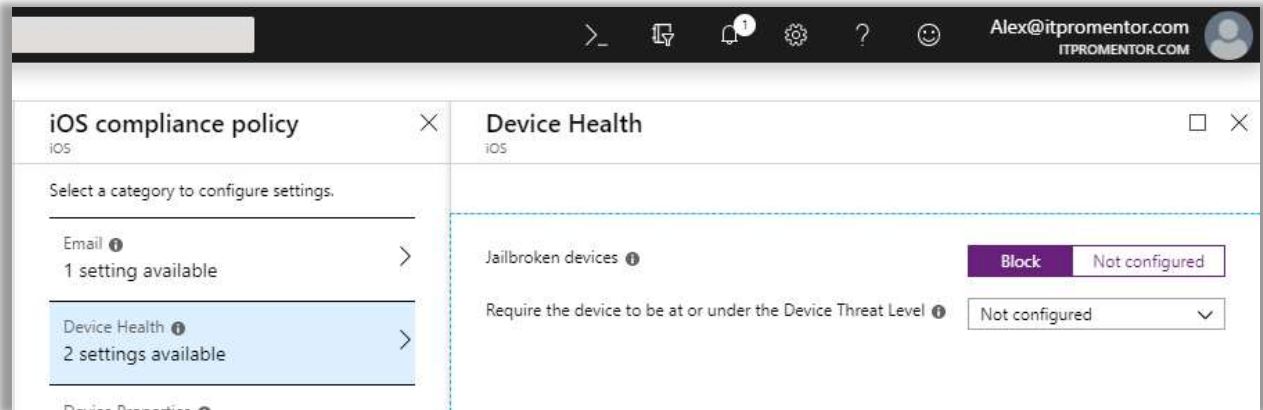
In this example I have selected iOS, but they are all very similar in how they work.



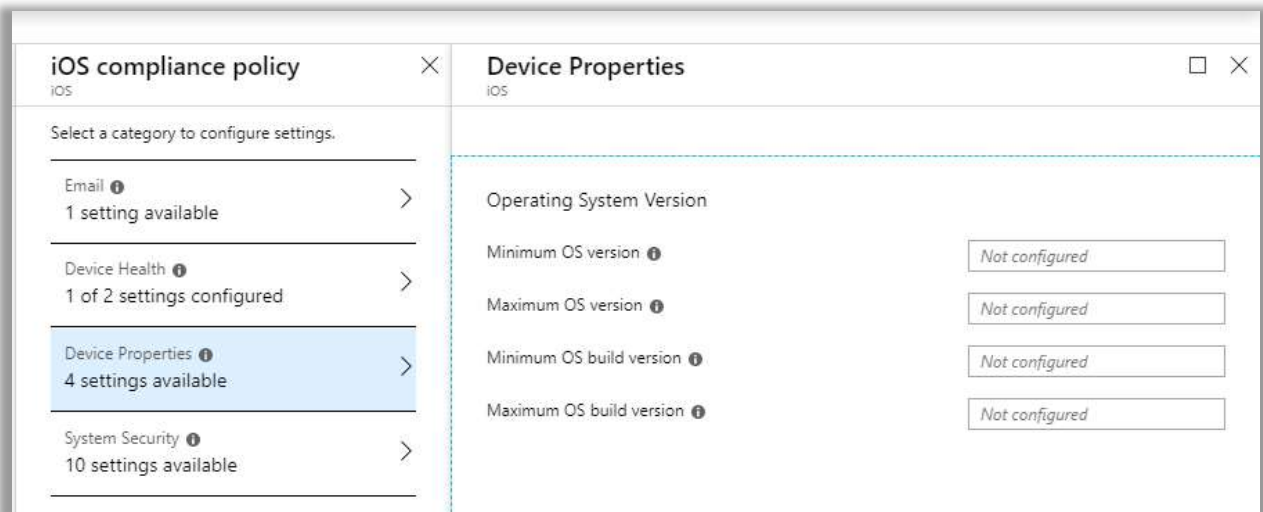
Check out **Settings > Email**. From here, you can tell Intune that it is necessary to require a managed email profile. Note: this means the native mail app on the device; manually added accounts do not count. Do not enable this setting if you want users to install Outlook for iOS and Android, for instance (it is possible to require both MDM and MAM for example). In this example, we will **Require** the managed email profile.



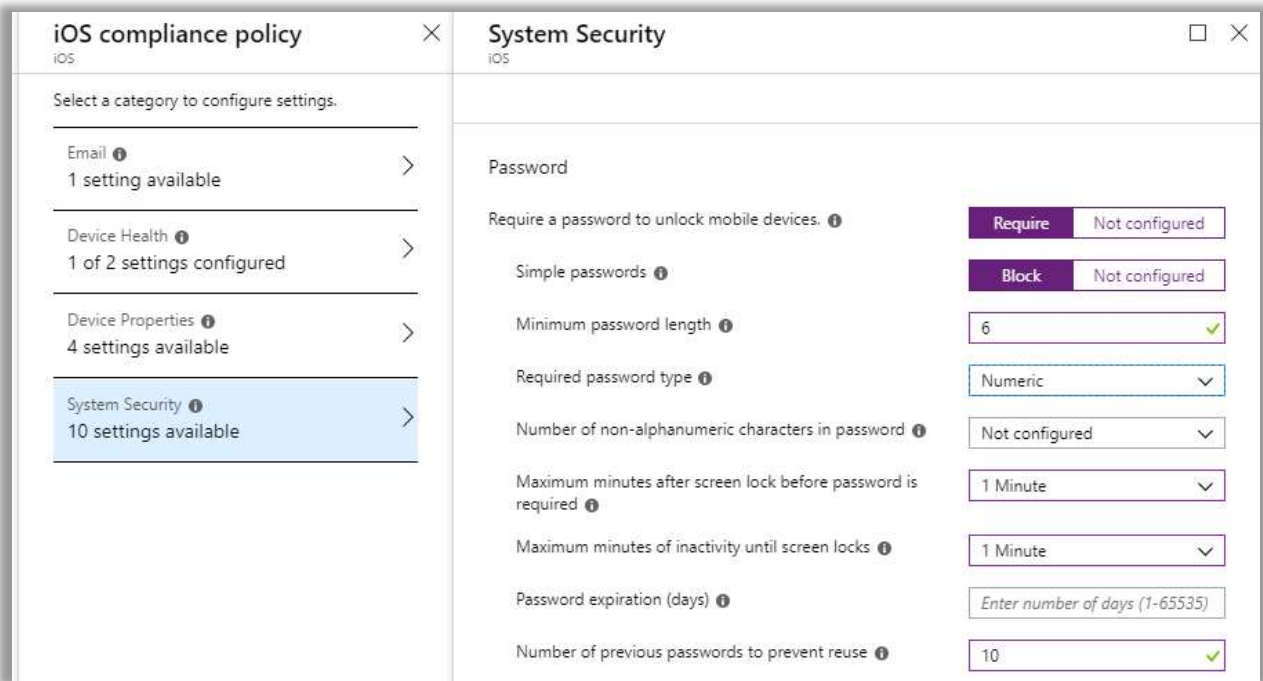
Under **Device Health**, we can choose **Block** for *Jailbroken devices*.



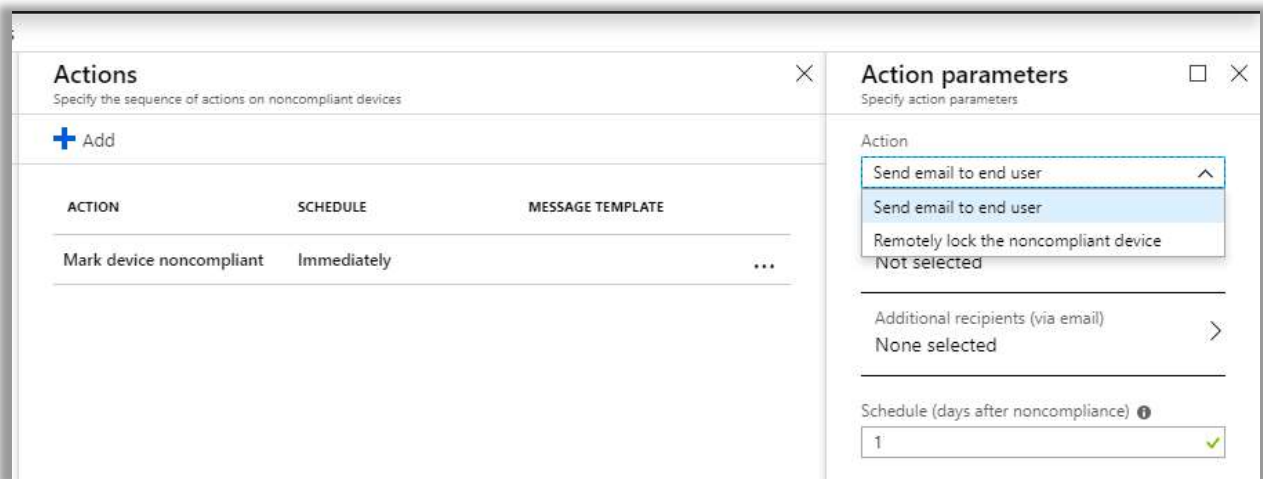
Device properties allows you to set minimum and maximum OS and build versions. We won't in this example.



System Security is where you can set a passcode requirement and associated parameters.

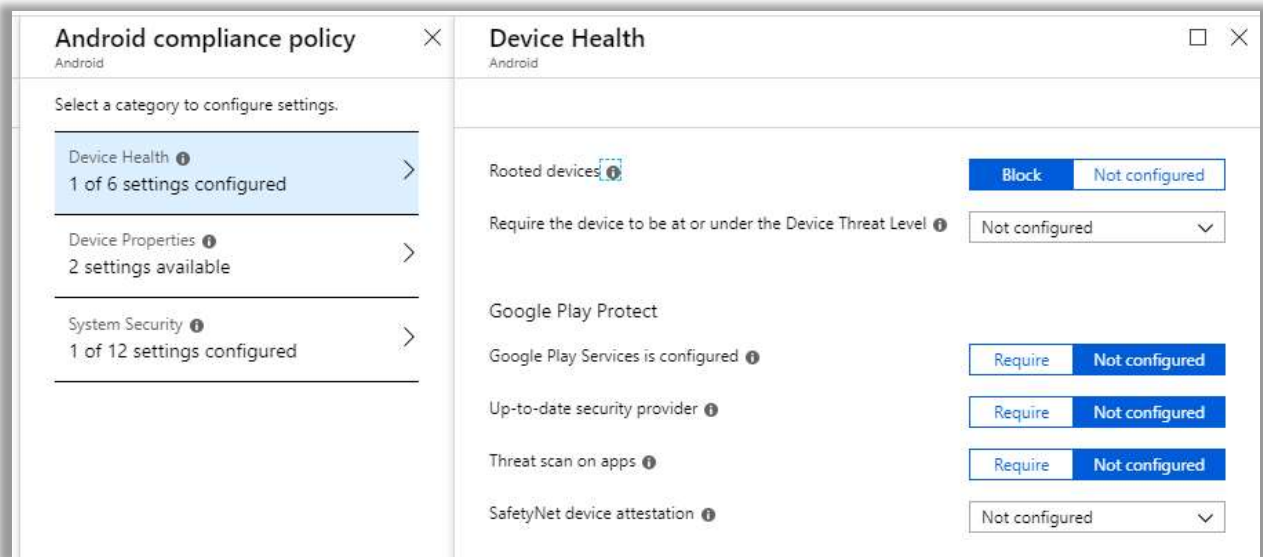


[OPTIONAL] On the **Actions for noncompliance blade**, one default action will be present (*Mark device noncompliant*), but you can also specify other actions such as *Send email to end-user*, and *Remotely lock the noncompliant device*. You can also have multiple actions, so you might have the default action, and then add email notifications after 5 or 7 days, etc., and finally, at some point, *Remotely lock the device*.

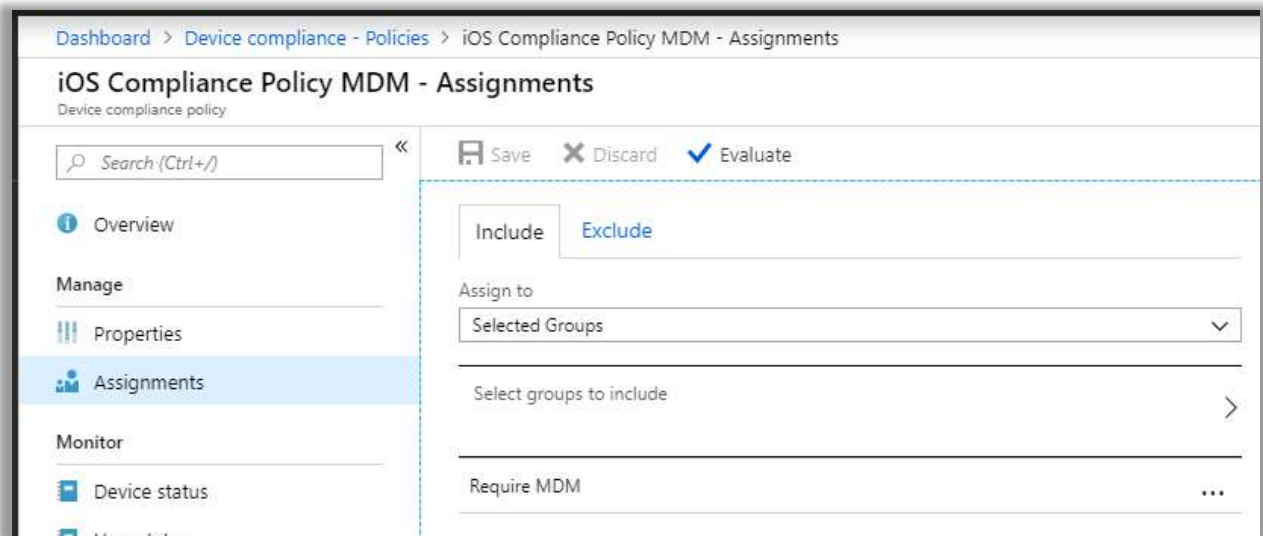


For a basic compliance policy, *Mark device noncompliant* is all that you really need. If you pair this with a Conditional Access policy that requires device compliance, then any device that is noncompliant with the policy would be blocked from access anyway.

Android policies (or any other platform) basically work the same way as what we're depicting here with an iOS-targeted policy. But, you will find differences in the settings available because different platforms will provide different options. For instance, you may see references to Google Play and other Android-specific settings.



Once you have your policies all configured, you will need to scope them to specific groups. This is done under **Assignments**. Don't skip this step or your users will not fall under the requirements of the policy! After you have assigned it either to *All users* or *Selected groups*, such as *MDM Users*, **Save** the selection.

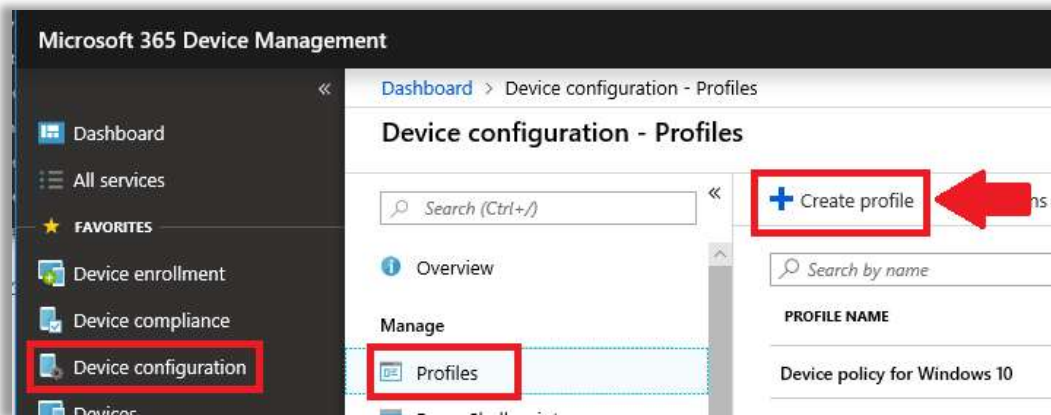


Configure device configuration profiles

If you are going down the MDM path (rather than MAM-only for BYOD devices) then you will likely want to create device configuration profiles as well. These provide much more granular control over various device options, and allow you to push things like Wi-Fi, email, and VPN settings. If you are requiring a managed email profile in your compliance policy, this is where you would tell devices to install said profile.

These are *not* the same as compliance policies, which can only evaluate the devices against the conditions that you set in the policy. In the case of *device configuration profiles*, the settings will be administratively set and are not capable of being changed or altered by the end-user; they are also not evaluated as part of a compliance check.

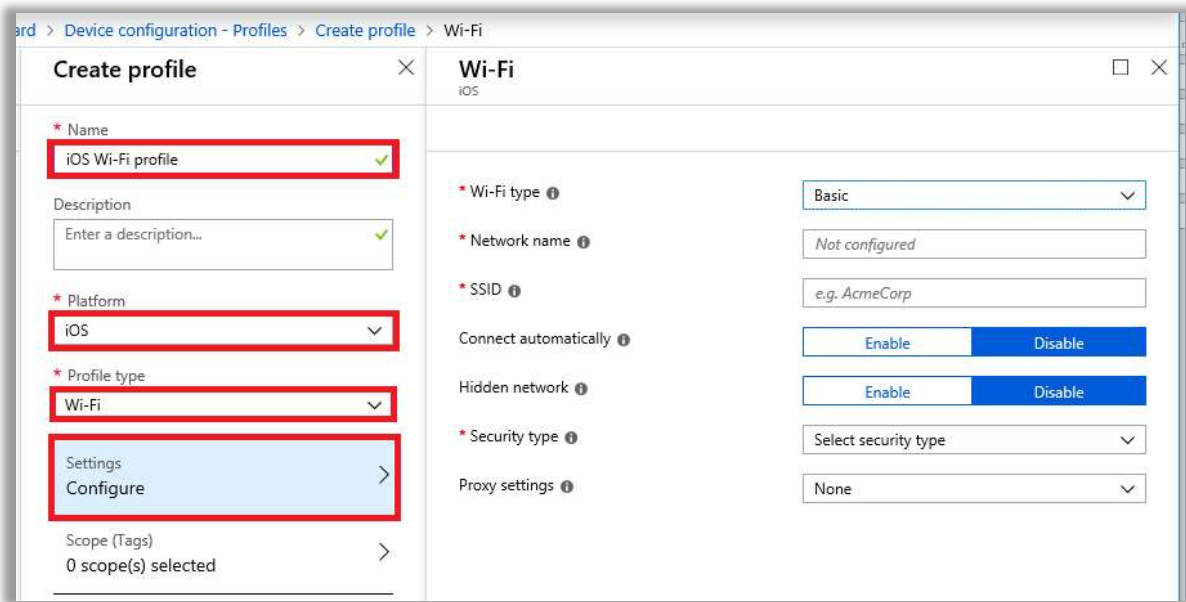
To create a new device configuration profile, navigate within the device management portal to: **Device configuration > Profiles > Create profile.**



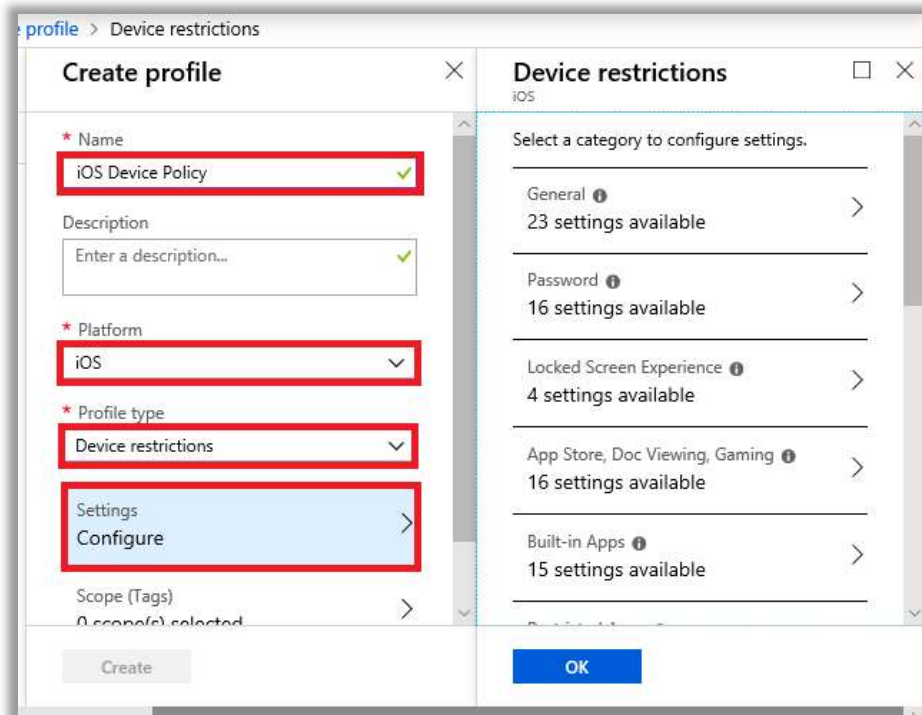
Give it a descriptive **Name** such as *iOS Managed Email profile*. Choose **iOS** as the **Platform** and **Email** as the **Profile Type**. For mailboxes hosted in Office 365, the **Email server** name is **outlook.office365.com**. You can use the **User Principal Name** for both **Username** and **Email address**. Specify **Username and password** as the **Authentication method**.

A screenshot of the 'Create profile' form in the Microsoft 365 Device Management portal. The form is divided into two columns. The left column contains fields for 'Name' (iOS Managed Email profile), 'Description' (Enter a description...), 'Platform' (iOS), and 'Profile type' (Email). The right column contains fields for 'Email server' (outlook.office365.com), 'Account name' (ITProMentor Corp), 'Username attribute from AAD' (User Principal Name), 'Email address attribute from AAD' (User Principal Name), and 'Authentication method' (Username and password). There are also 'Save', 'Discard', and 'SSL' options, and 'Enable' and 'Disable' buttons at the bottom right.

Optionally, it is possible to create an additional iOS policy that pushes a Wi-Fi profile to the device, if you have a corporate Wi-Fi that you wanted to pre-configure for auto-connection, for example.

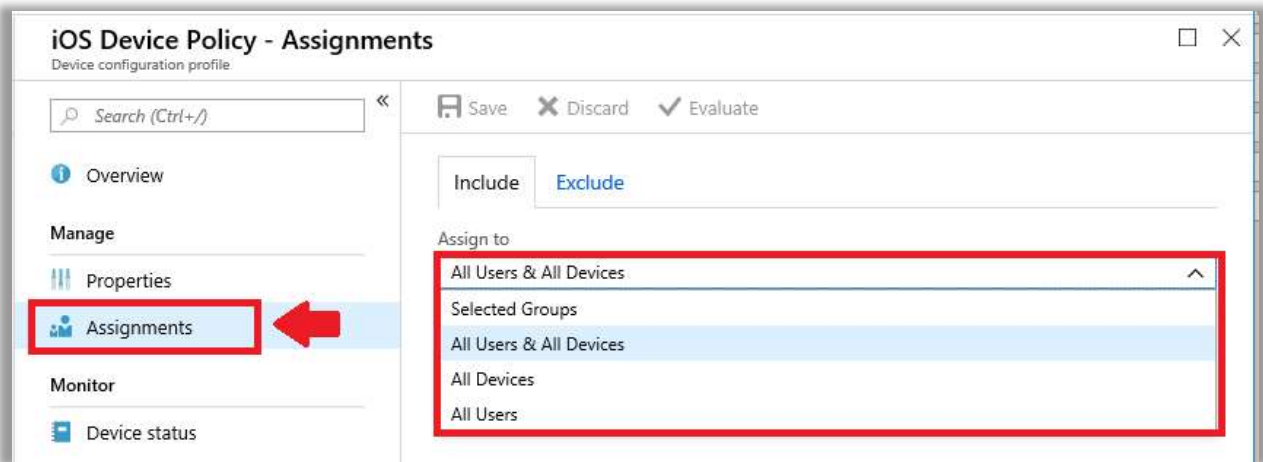


Optionally, you can also create another policy selecting **Device restrictions** as the **Profile type**. This allows you to control a great many other settings.



Again, the specific options will look different depending on the platform you select.

Once you have made all your selections for any given policy, under **Assignments**, you can assign the policy to either **Selected Groups** or alternately, **All Users and/or All Devices**.

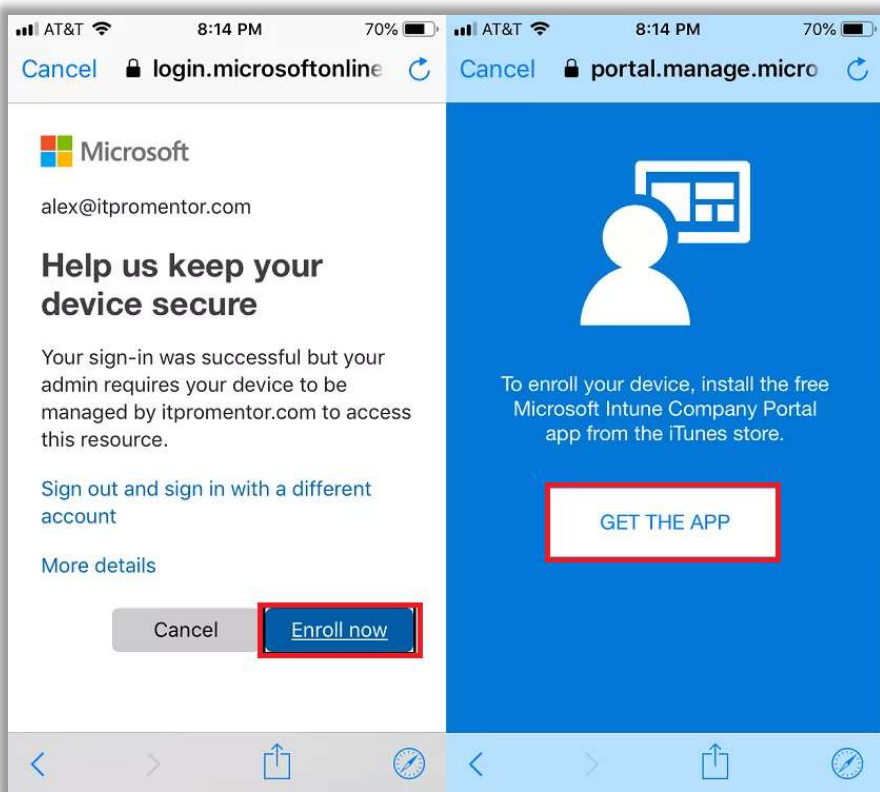


This makes it possible to configure multiple policies, scoped to different groups, or even have more than one policy scoped to the same groups.

Note: When two policies are in conflict, the more restrictive setting wins.

Enrolling a mobile device

If you have in place a proper Conditional Access policy (again: requires Azure AD Premium), then users will receive a prompt as they attempt to add an email profile to the device, which will in turn direct them to download the **Intune Company Portal** app from the app store, to complete the enrollment.



Note: If multi-factor is enabled, then the end-user will also need to have the Microsoft authenticator app handy.

Of course, even without Conditional Access, you can also *manually* enroll each device through the same steps—obtaining the Intune Company Portal app via the app store and going from there on your own.

A fair warning: there are a good number of screens that the user must step through to enroll the device, selecting options in the affirmative such as *Continue, Trust, Enroll, Accept, Check compliance*, blah, blah, blah...they seems to go on forever. I won't cover them here. In fact, the enrollment hassle associated with MDM is one reason why many small businesses choose to stick with MAM.

Use Conditional Access to require MDM instead of MAM (or in addition to it)

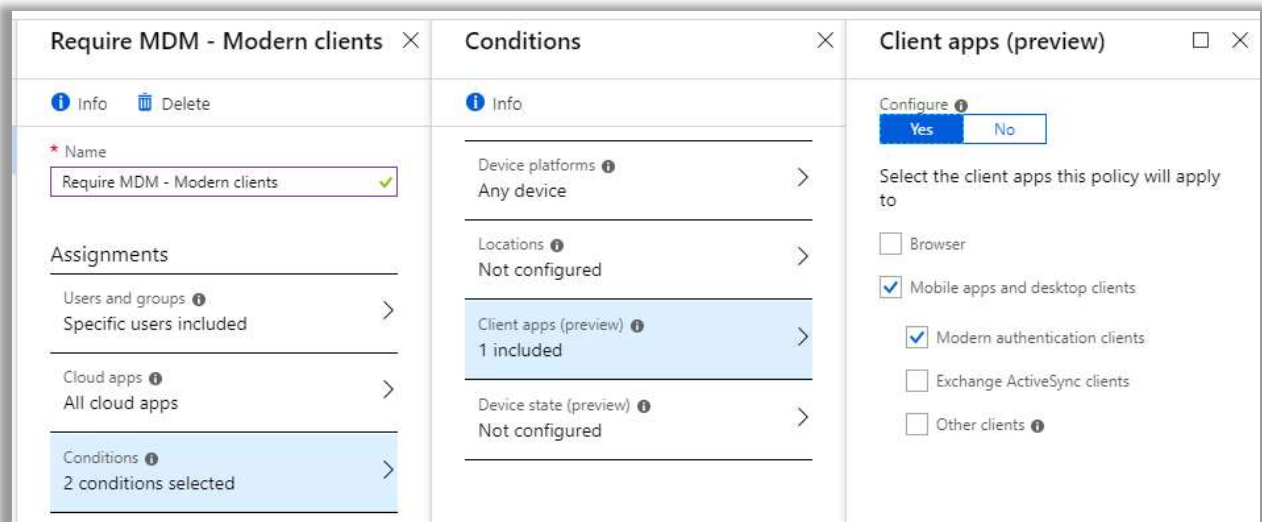
Similar to how we enforce MAM using Conditional Access for BYOD devices, you can design a policy that enforces MDM instead, if that is your requirement. And you have a lot of options here, too. Some organizations prefer to enforce both MDM *and* MAM with a single set of policies. Or, a policy set that supports either option.

I will cover three policy sets (for each, note that you will still need one targeted to EAS clients and another to modern clients).

- Configure a policy set that requires MDM only
- Configure a policy set that requires MDM *or* MAM
- Configure a policy set that requires MDM *and* MAM

Policy Set Option #1: Require MDM only

To require MDM enrollment, create a new Conditional Access policy from the **device management portal > Conditional access**. Name the policy something descriptive such as *Require MDM – Modern clients*.



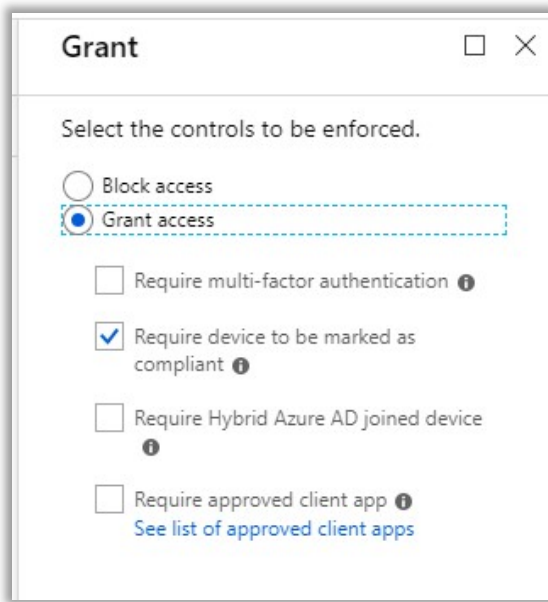
Under **Assignments**, select the **Users and groups** to whom the policy will be applied.

For **Cloud apps**, you can certainly choose **All cloud apps** to protect apps across the board, including Exchange Online, SharePoint/OneDrive, Teams, etc., or, select specific cloud apps such as Exchange Online, if, for instance, you only want to require MDM for access to email.

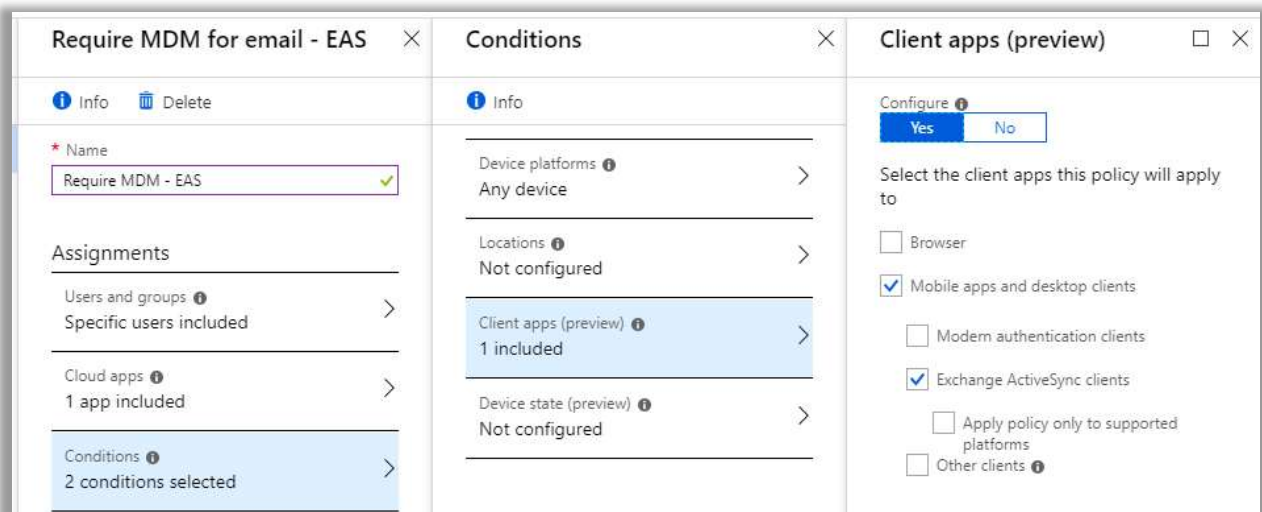
Under **Conditions > Device platforms**, select **iOS** and **Android**. Optionally, you can choose **All devices** if you intend to require enrollment of all Windows and Mac clients, also.

Finally, under **Client apps** select only **Mobile apps and desktop clients > Modern authentication clients**.

Saving all those selections, scroll down to the **Access controls** blade and pick **Grant access** with the option: **Require device to marked as compliant**.



Save all your selections and **Enable** the policy. Now you need to create the same policy again, but for EAS clients. The only difference with targeting EAS clients, is that you cannot choose any other conditions besides the **Client apps** condition, and you may specify no other cloud applications besides **Office 365 Exchange Online** (so **All cloud apps** doesn't mean anything to EAS).

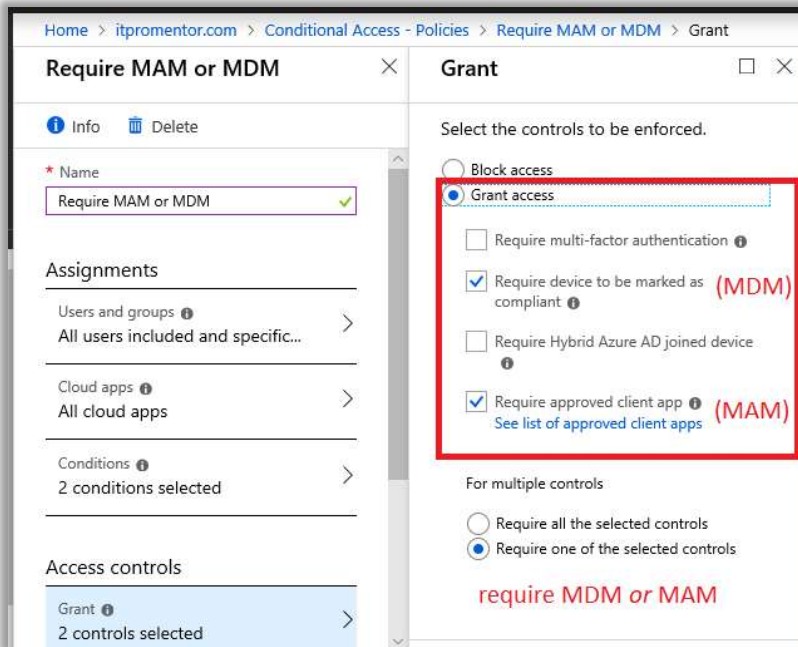


Just target **Mobile apps and desktop clients** > **Exchange ActiveSync clients**. Require the same access control as before to enforce compliance with Intune, then save and **Enable** the policy.

Policy Set Option #2: Require either MAM or MDM

This is my favorite option to implement for customers, because it gives them both options. Some end-users just cannot give up their native iOS mail app, and refuse to use Outlook. And, some organizations prefer to issue mobile devices to groups with special needs such as Sales, but not others, e.g. in Admin or otherwise. Therefore, there is often a split between the groups' needs.

One way to accomplish this bifurcation in management approach is simply to use security groups to scope the two different policy sets to either group of users—making some MAM users and some MDM users. However, you can also create a set of policies that defines *both* access controls at once, with the requirement to meet only one of them. This is the most flexible, since some users may have a managed phone and personal tablet, for example, that can be treated differently but with just one policy set.



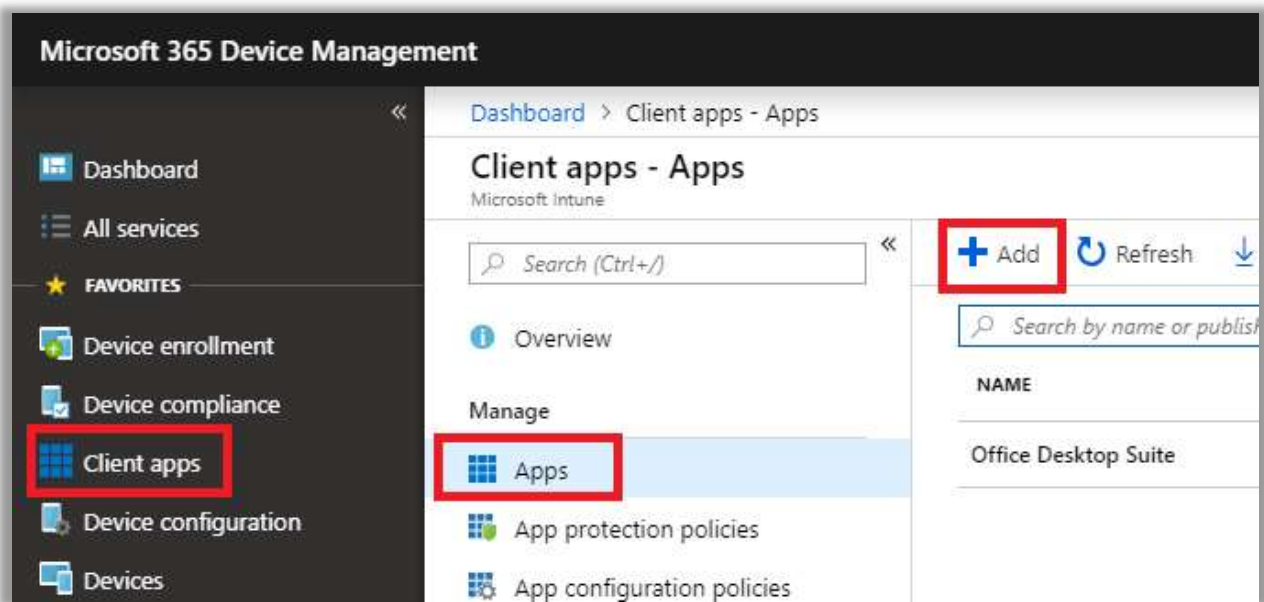
On the very last **Access Controls** page, simply use the selection to **Require device to be marked as compliant** as well as **Require approved client app**. Then only **Require one of the selected controls**.

Don't forget to create the EAS version of this policy also.

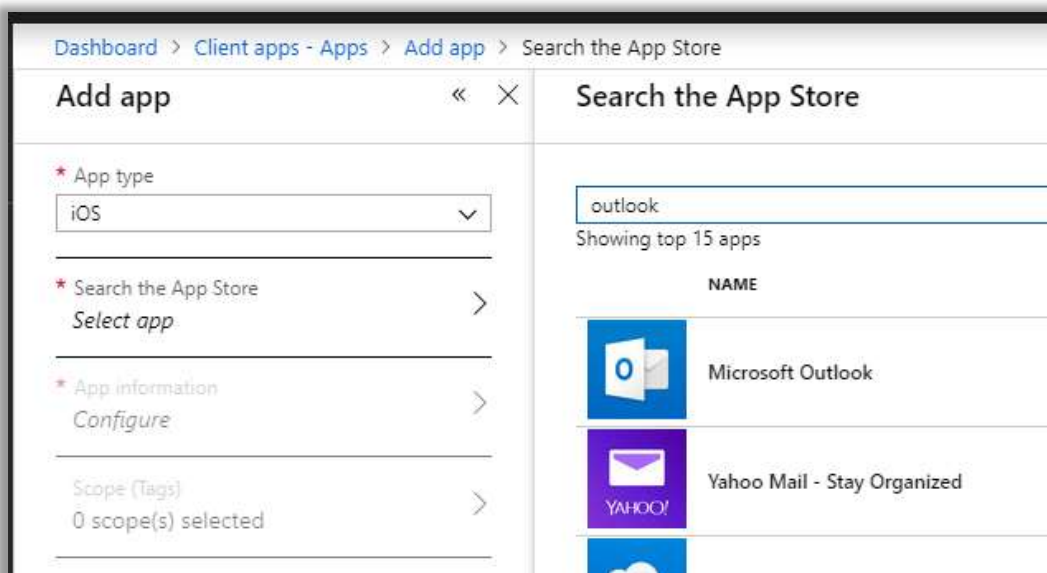
Policy Set Option #3: Require *both* MAM and MDM

As you can probably guess, the way to require both MAM and MDM is to **Require all the selected controls**, rather than just one, as we saw above. And you would be correct.

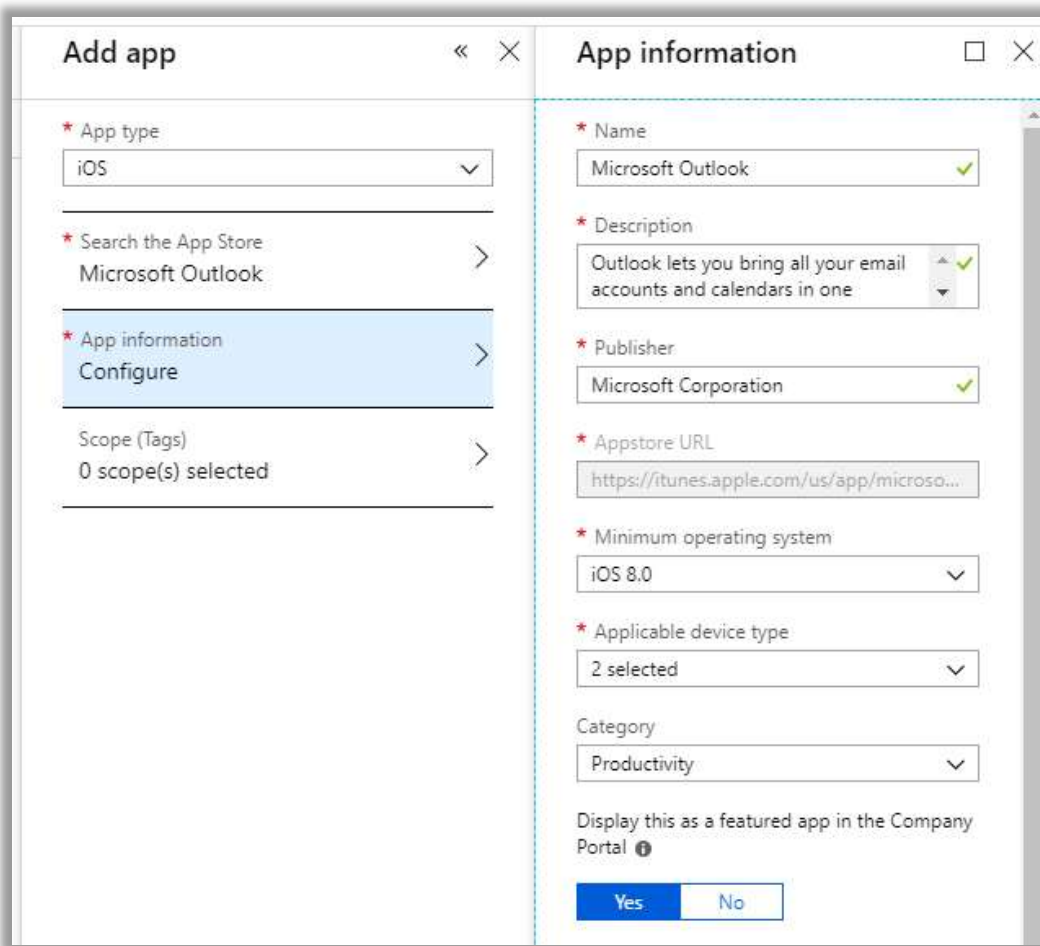
But since you are enrolling the devices for full MDM, and will have additional management capabilities at your fingertips, you should know that it is also possible to “go the extra mile” for your users, and assign the supported apps for automatic installation on their devices.



Go to **Client apps > Apps** and click **Add**. Select **iOS. Search the App Store** and find **Outlook**. Pick the **Microsoft Outlook** tile.

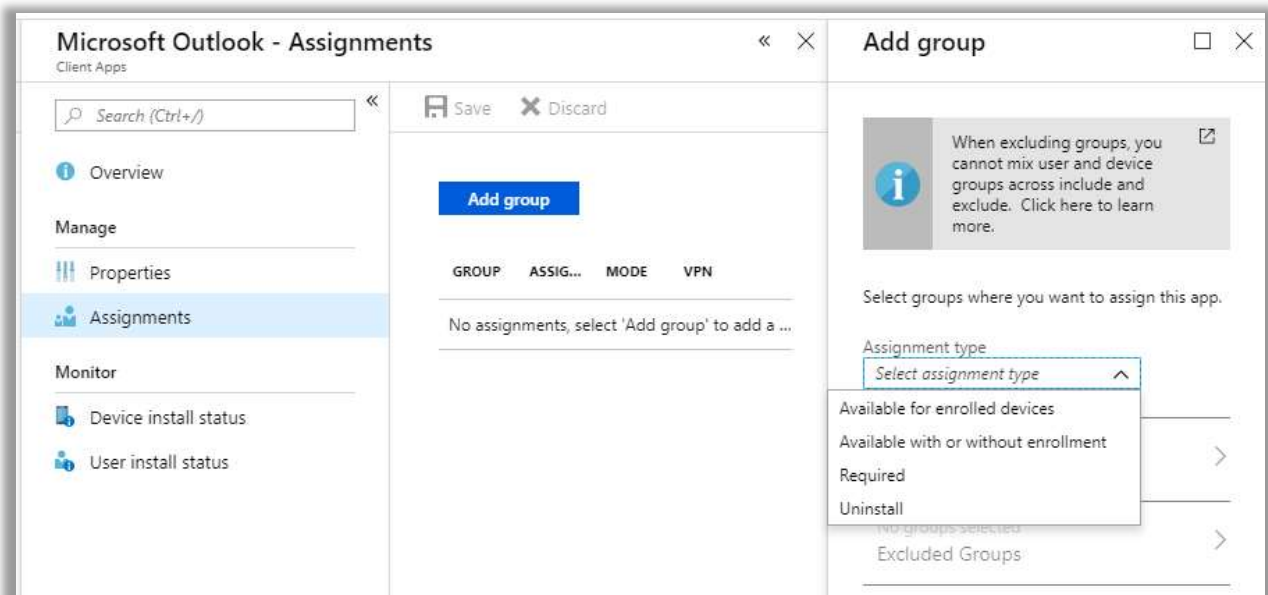


Under **Configure**, you can optionally specify a **Category** and choose to **Display this app as a featured app in the Company Portal**.

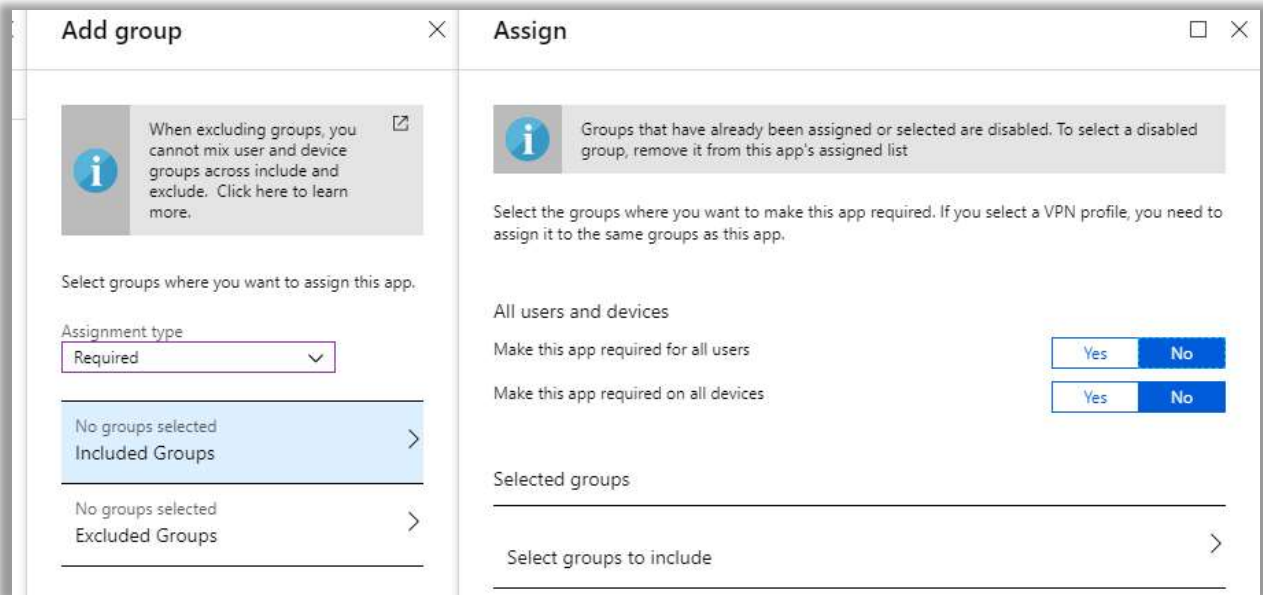


Click **OK** then **Add**.

As always, we need to assign the app to a group. Click **Assignments > Add group**. From the Assignment type drop down, if you want to have the app automatically deployed to the device upon enrollment, click **Required**.

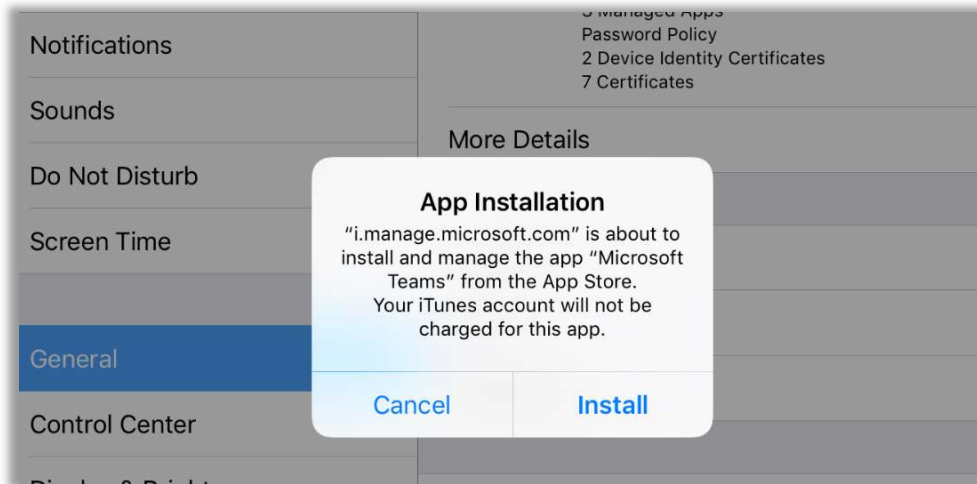


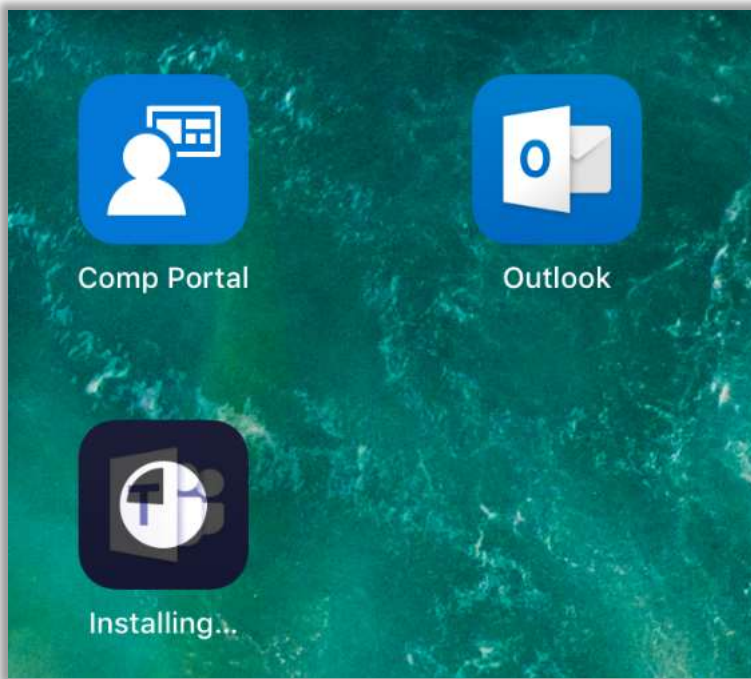
You can make the app required for a specific group or target all users or all devices.



After you save all your selections, you can repeat this process for any other platforms and apps that you want, including non-Microsoft apps, if you like. I'll just add Teams as well as Outlook for now.

Enroll a device to see the result.





Manage devices in the Microsoft 365 admin center

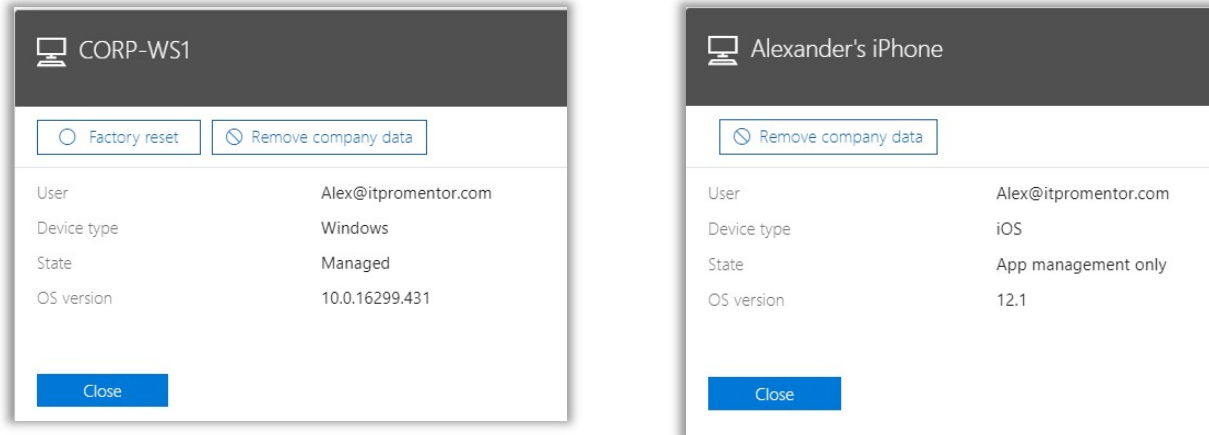
You can, of course, use the Intune Device management portal to manage the devices and perform certain actions against them, but you will find that the inventory of devices also shows up right in the Microsoft 365 admin center, as well. Go to **Devices > Manage**.

| Devices | User | Device type | State |
|---------------------------------------------|----------------------|-------------|---------------------|
| <input type="checkbox"/> Devices: 4 | | | |
| <input type="checkbox"/> CORP-WS1 | Alex@itpromentor.com | Windows | Managed |
| <input type="checkbox"/> Elizabeth's iPad | Alex@itpromentor.com | iOS | Managed |
| <input type="checkbox"/> Alexander's iPhone | Alex@itpromentor.com | iOS | App management only |

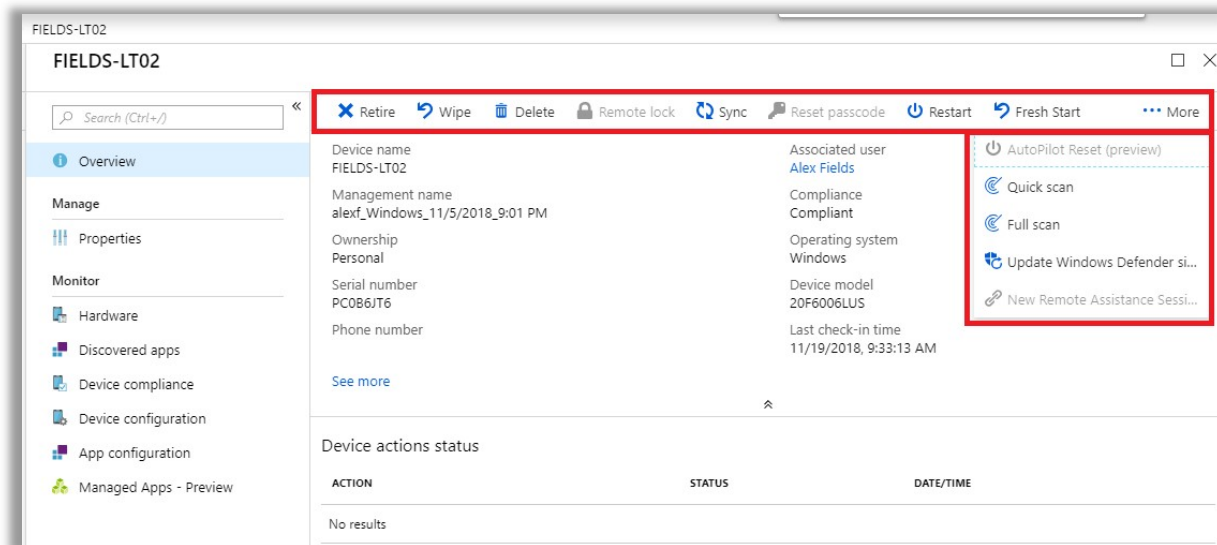
If you are using Conditional Access to require devices to become protected by your MDM and/or MAM policies, then you should see a complete list of corporate-issued and BYOD devices here. You can see the device name, the **User** it is associated with, as well as the **Device type**. Under the **State** column, you can see that it will tell you at what level you are managing the device:

- **Managed** = MDM (enrolled and managed at the *device* level)
- **App management only** = MAM (managed at the *application* level, device is not enrolled)

In either case, we can remotely wipe the corporate data.



Fully managed devices can also be factory reset. You can find additional controls and levers over the *managed* devices from **Devices** in the **Device management portal**.



This concludes the chapter on device management.

Part 3. App & Data Protections

The features we will discuss in this next chapter are meant to be distinguished from the management of identities and devices, which we covered in previous chapters. But it's important to realize that all these technologies are working together to provide layers that were just not previously available to us back in the on-premises days of yore.

The Microsoft 365 bundle includes several subscriptions which are considered "add-ons" to Office 365 Business Premium or to any other standalone Office 365 product. The benefits afforded by these add-ons are generally applied at the application layer, and their purpose is to provide certain protections for every user, on any device: whether company-owned or not, and whether behind a company firewall or not.

- **Azure Information Protection** (AIP) – Provides us with the ability to label (classify) and encrypt sensitive email messages and Office documents, wherever they travel
- **Exchange Online Archiving** – Add an online archive mailbox for long-term storage of important emails; deploy retention tags and policies that preserve and/or expire data
- **Data Loss Prevention** (DLP) – Enable rules to detect when sensitive information is being shared externally, and take automatic action to block, encrypt or notify users
- **Advanced Threat Protection** (ATP) – Suite of tools to help protect users from malicious threats, including zero-day malware, compromised websites or bad hyperlinks, and phishing, whaling or spear-phishing emails

At the time of this writing, the Security & Compliance Center (<https://protection.office.com>) is the admin portal through which we will configure many of these add-on products. However, the Security & Compliance center will be broken apart into the Compliance admin center (<https://compliance.microsoft.com>), and the Security admin center (<https://security.microsoft.com>), respectively.

Be aware that changes like this are not unusual in the cloud—but the core products and feature sets should basically remain intact, even if they morph and the feature-set is expanded over time.

Configure Azure Information Protection

Azure Information Protection serves two important functions that we will discuss in turn:

1. Encrypting outgoing email messages (called Office Message Encryption or OME)
2. Labeling or classifying documents, applying encryption, watermarks, restrictions, etc. (e.g. Personal, Public, General, Confidential, Highly Confidential)

Enabling email encryption (OME)

In the olden days, a lot of PowerShell was required to get the Email encryption features enabled within the tenant. These days, most of it is already enabled for us, right out of the box. However, there may be additional customization that you want to make before configuring your mail flow rules, and this will still require the use of PowerShell.

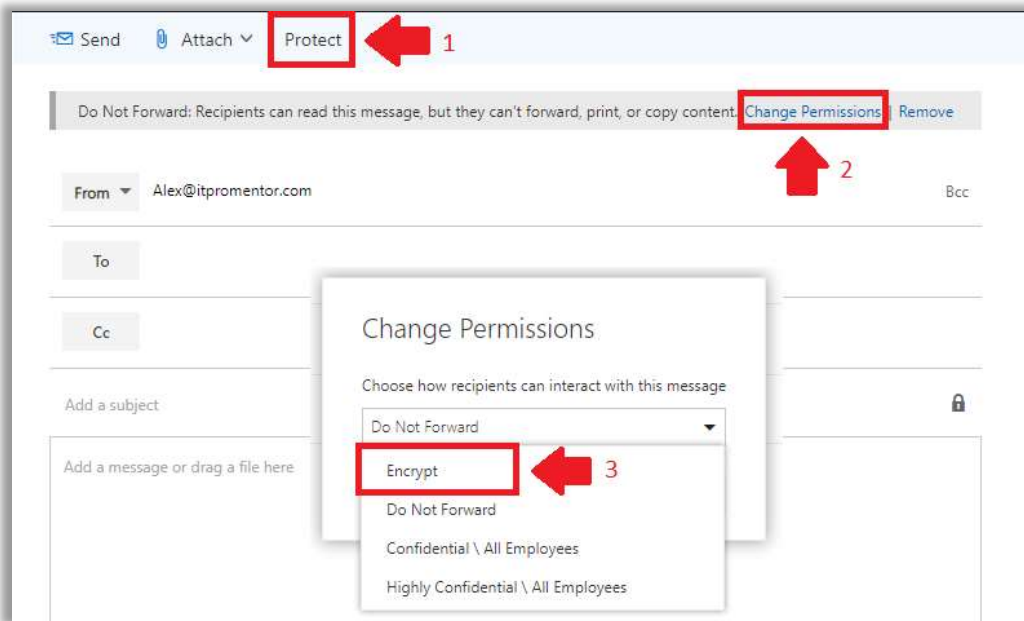
To begin, connect to Exchange Online using PowerShell:

```
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -
Authentication Basic -AllowRedirection
Import-PSSession $Session
```

The first option that you will probably want to configure, is the option to display a “Protect” button in Outlook Web Access. By default, this value is set to \$false, and we just need to flip it to \$true.

```
Set-IRMConfiguration -SimplifiedClientAccessEnabled $true
```


Once a user clicks on **Protect**, the default template that is applied is *Do Not Forward*. To change this to another template, such as *Encrypt*, click **Change Permissions**.

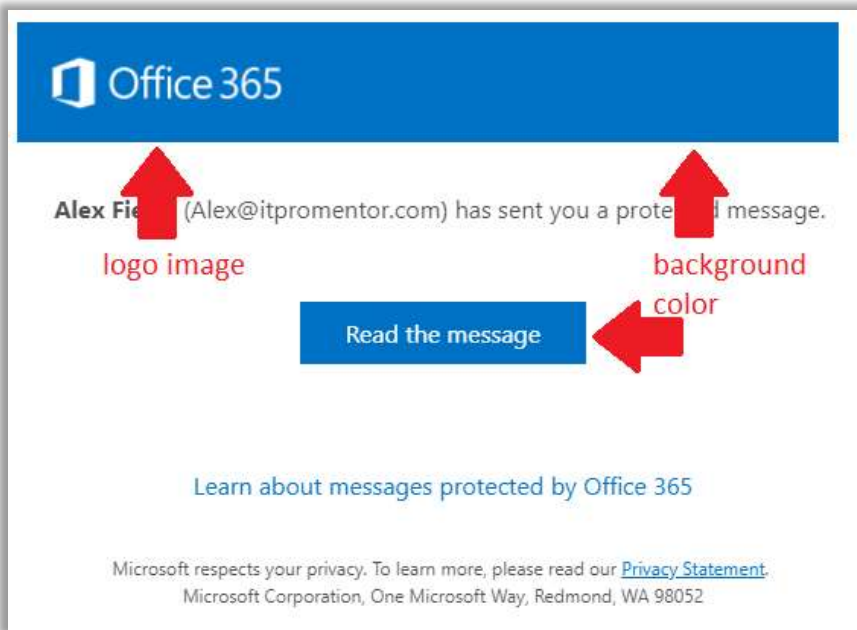


We find four default permissions templates available for sending email messages. They are:

- **Encrypt** – Use this template *only* to encrypt; no other special restrictions will be applied. This is the most popular template for sending encrypted email messages. External recipients are allowed with this template.
- **Do Not Forward** – Recipients of a message marked with *Do Not Forward* permissions will not be able to share, print or copy the message or document. External recipients are allowed with this template.
- **Confidential\All Employees** – Recipients of a message marked with *Confidential\All Employees* permissions can reply to and forward the content within the organization only. It is not possible to share with external users.
- **Highly Confidential\All Employees** – Similar to the above, *Highly Confidential* messages can only be shared within an organization, however, the content is accessible only to the specific individuals with whom the content has been shared. Forwarding to other users either internally or externally is not possible.

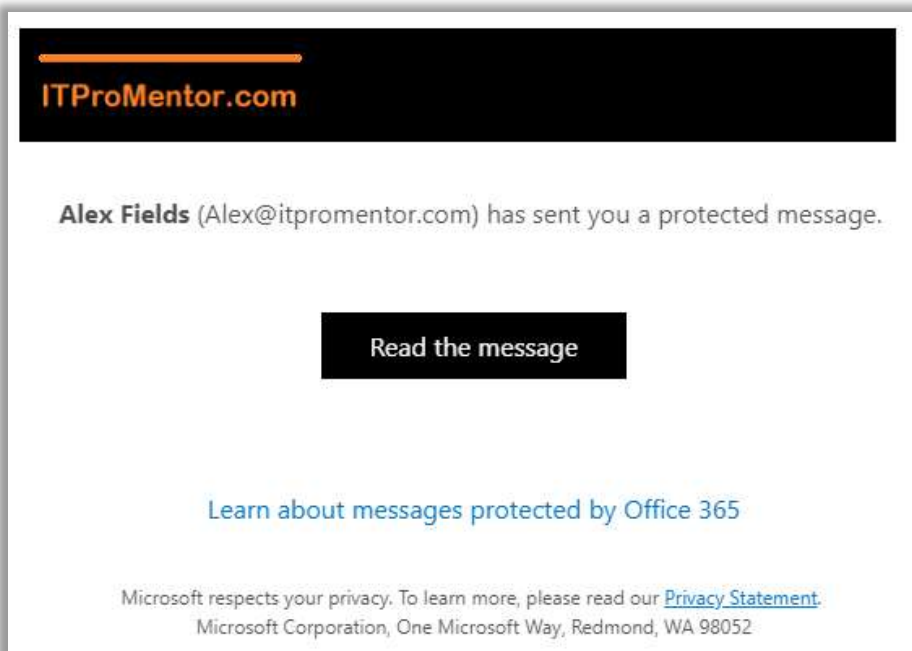
Configure branding for encrypted email messages

Second, you may want to customize the recipient experience by applying your logo to the default encryption messages and portal. You will need a copy of your company's logo in .png, .jpg, .bmp, or .tiff format. It should be less than 40 KB, with an optimal size of 170x70 pixels (but it doesn't have to be exactly that ratio).



Still connected via PowerShell to Exchange Online? Good. Then you can customize both the logo image, as well as the background color (which is blue by default). In my example, the color is set to black.

```
Set-OMEConfiguration -Identity "OME configuration" -Image (Get-Content "C:\Temp\logo.png" -Encoding byte) -BackgroundColor "#000000"
```



After the customization is applied, we can see the result in a test message sent to an external user (e.g. a Gmail account). There are also other parameters you can customize, such as the default text displayed on the message, and in the online portal. To see them, simply run:

```
Get-OMEConfiguration | fl
```

```
PS C:\WINDOWS\system32> Get-OMEConfiguration | fl
RunspaceId           : 
TemplateName         : OME configuration
Image                : {137, 80, 78, 71...}
ImageUrl             : https://e4eomev2branding.blob.core.windows.net/6
EmailText            : 
PortalText           : 
DisclaimerText       : 
BackgroundColor      : #000000
IntroductionText     : 
ReadButtonText       : 
OIPEnabled           : True
SocialIdSignIn       : True
ClientEncryptionEnabled : True
ExpirationOptionEnabled : True
Identity             : OME configuration
IsValid              : True
ObjectState          : Unchanged
```

Configure how downloaded attachments are treated

Next, most users who receive an encrypted email are not expecting the attachments to be “locked down” with encryption themselves. However, that is in fact the default behavior of Office Message Encryption. If that’s what you want, great—feel free to skip this section.



However, it is also possible to automatically decrypt any attached documents when they are downloaded from the portal. Many organizations opt to have this setting enabled:

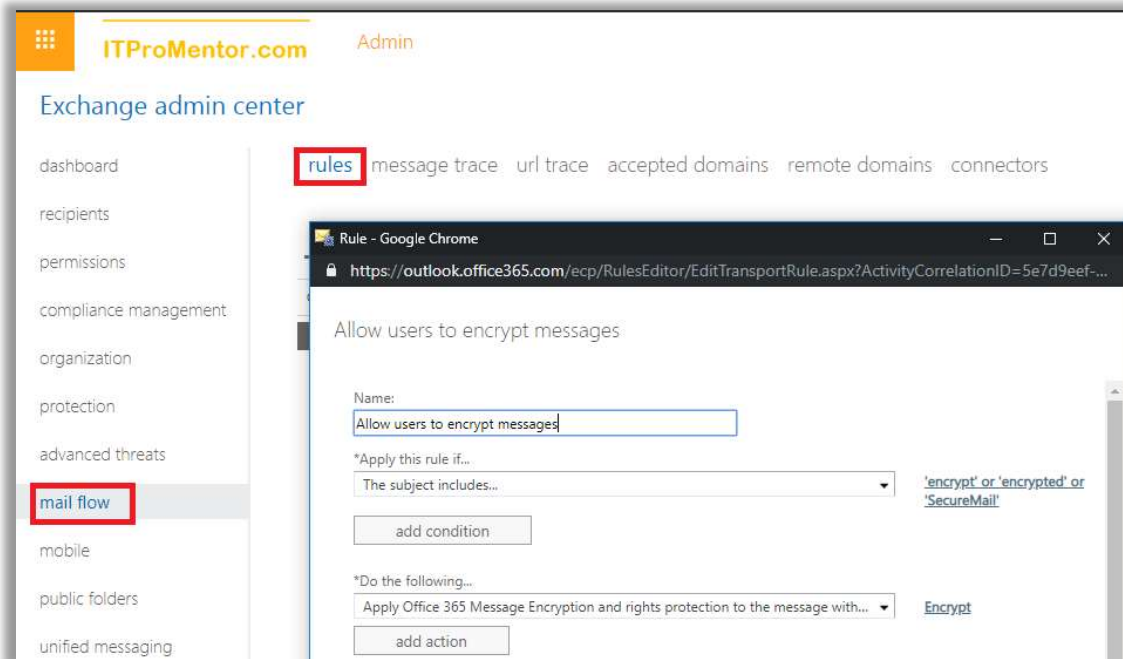
```
Set-IRMConfiguration -DecryptAttachmentForEncryptOnly $true
```

Configure mail flow rules to encrypt emails

The *Protect* button is only available in Outlook on the Web at the time of this writing. Use of Outlook will most likely trigger encryption using a subject line or body tag in the email message itself. Therefore, you need to set up a transport rule to allow for this. The easiest way to accomplish this is in PowerShell.

```
New-TransportRule -Name "Allow users to encrypt messages" -SubjectContainswords "SecureMail" -Priority 0 -ApplyRightsProtectionTemplate Encrypt
```

In this example, the transport rule will apply OME encryption to any message with a subject line that contains the text SecureMail. You can customize this to your own liking. The transport rule also can be edited via the Exchange Online admin center GUI, by navigating to **mail flow > rules**.



You can create mail flow rules which take advantage of any of the other default templates, as well.

Azure Information Protection labels

Azure Information Protection (AIP) uses “labels” to classify and protect data. Labels are published to end-users for eventual consumption and use through a “policy.”

In the olden days, applying permissions and restricting access to files was more rudimentary—again, it was based on the concept of the “four walls.” We would erect digital boundaries that simply mimicked familiar physical boundaries. The idea, which seems silly now, is that you could protect your files *inside* a file server much in the same way you would protect physical files that were locked up in a file cabinet somewhere, inside an office building. A file server is a container, protected by an access control list (ACL), exactly like a building or cabinet is protected by lock and key. With the right credentials (or the right key) you get to enter the server (or building/cabinet).

But these sloppy old structures are just no longer adequate in a world where so much of our data has become mobile and *slippery*—moving easily from one device to another, one file system to another, one cloud to another.

Therefore, Azure Information Protection (built on its predecessor Azure AD RMS), allows us to stamp permissions and encryption onto individual files themselves—an ACL is applied, and the access is controlled no matter where that file travels during its lifetime.

For the purposes of covering basics here, we are just going to work mostly within the default labels and the Global policy that is provided with AIP out of the box. But you must understand that preceding any actual implementation of AIP labels and policies is data classification.

Planning for data classification

Data classification is a formal exercise that must be completed with the key decision-makers and stakeholders in the business. Before you can begin to actually classify and protect data, you must first define what your “labels” or “classifications” are going to be:

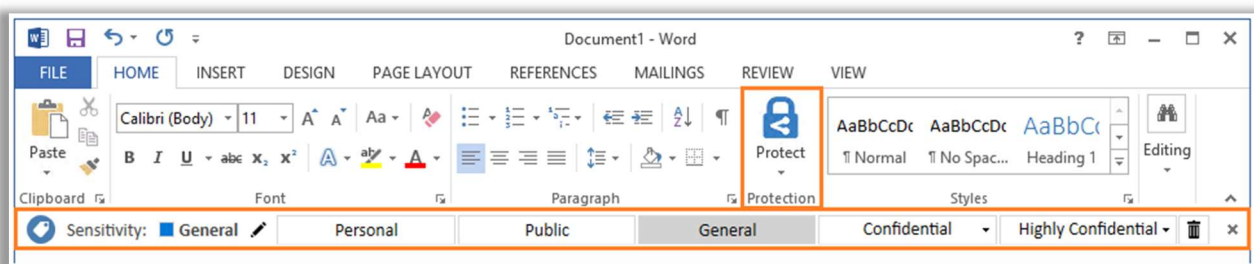
- What will they be called?
- How will they be described to end-users?
- What will they do to a document?
 - Label it with header, footer, watermark?
 - Protect and apply encryption?
 - Apply specific permissions or restrictions?
- Who has access to apply which labels?

It will be easier for you to complete this planning exercise if you first understand what your capabilities are. To that end, we will review the basics of both labels *and* policies, and finally move onto Office 365 “Sensitivity labels,” a similar technology which you can now use in conjunction with AIP labels, so that you do not have to re-create any labels moving between the two.

Note: Office 365 Sensitivity labels are in fact a distinct and separate technology, even though you can now “marry” your labels; there remain some crucial differences, and we’ll be sure to cover them.

AIP Client and basic end-user experience

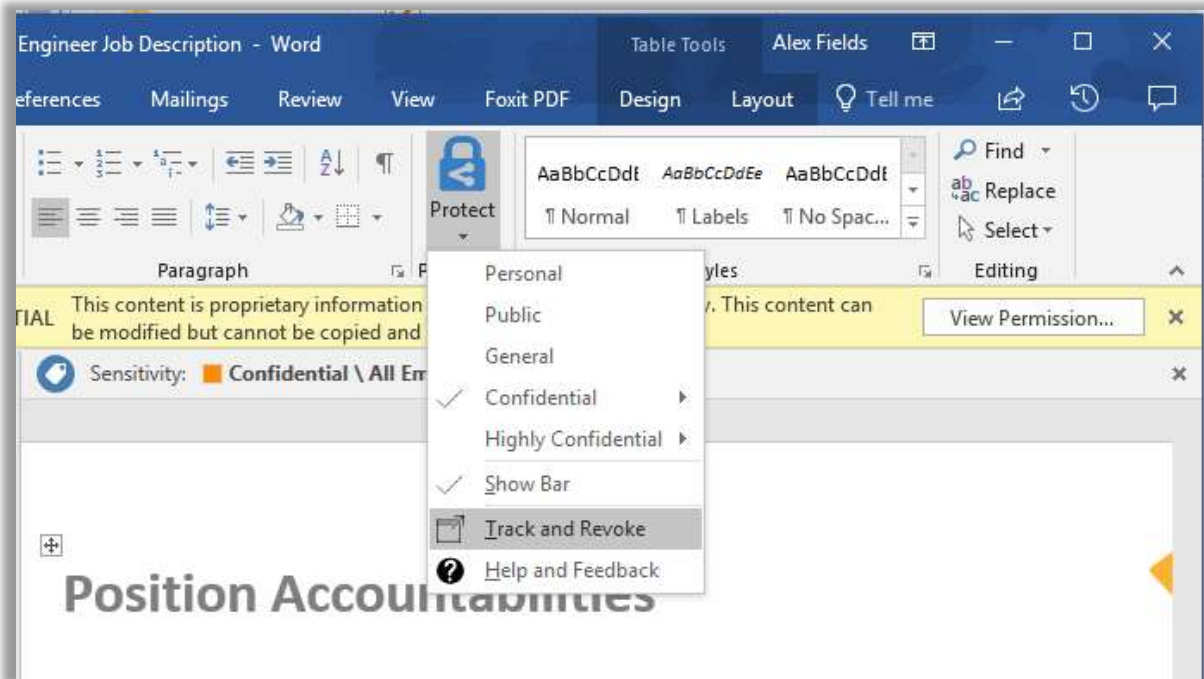
Today, if you want users to be able to access and apply labels from AIP, they will need to have the [AIP client installed](#) on their devices, so that the labels are available via the various applications. When you install the client, it shows up on the Office ribbon (it says **Protect** and looks like a blue lock—see the image below).



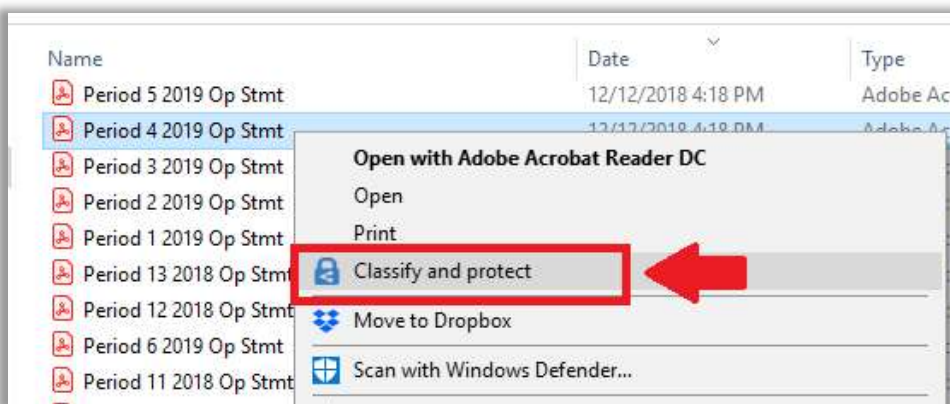
From the end-user perspective they are just classifying documents according to these labels, but behind the scenes there is quite a bit of technological magic happening, in some cases applying

encryption to the document with embedded permissions—think of it as an access control list (ACL) that travels with the file, wherever it goes.

Whenever this protection is enabled, a yellow bar with the label's description and permissions is displayed above the document, and the user will also have the ability to track and revoke any access that has previously been granted.



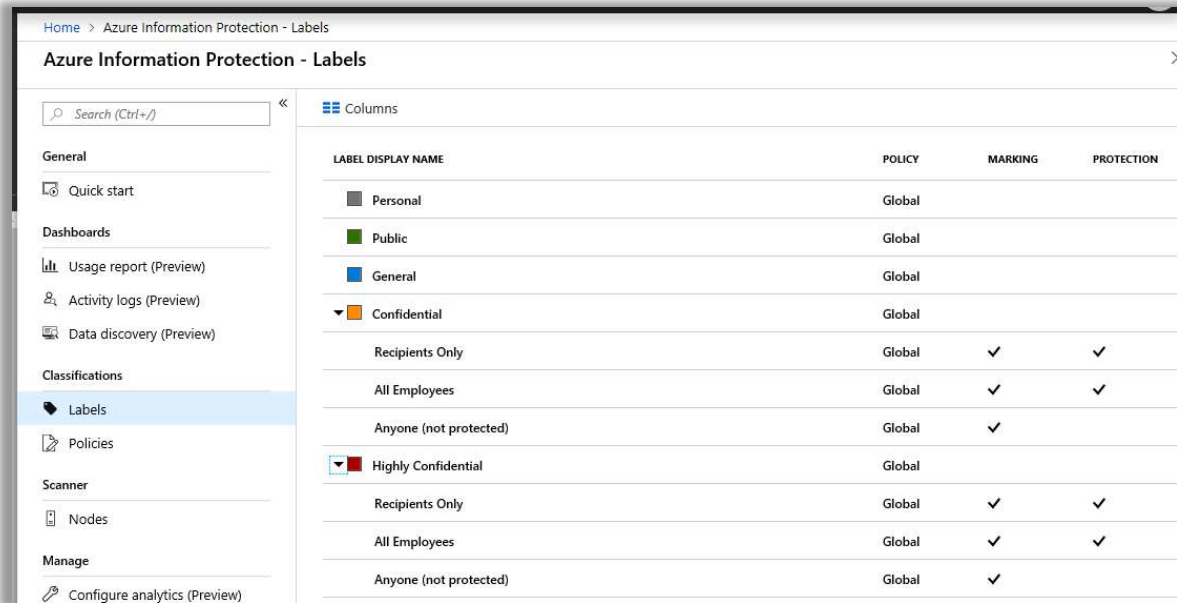
Users with the AIP client installed will also get the ability to classify and protect documents right within the native File Explorer for Windows.



A simple but powerful tool. However, before you throw it out there to users, you should work on your data classification and building your labels, and then publishing them with a policy.

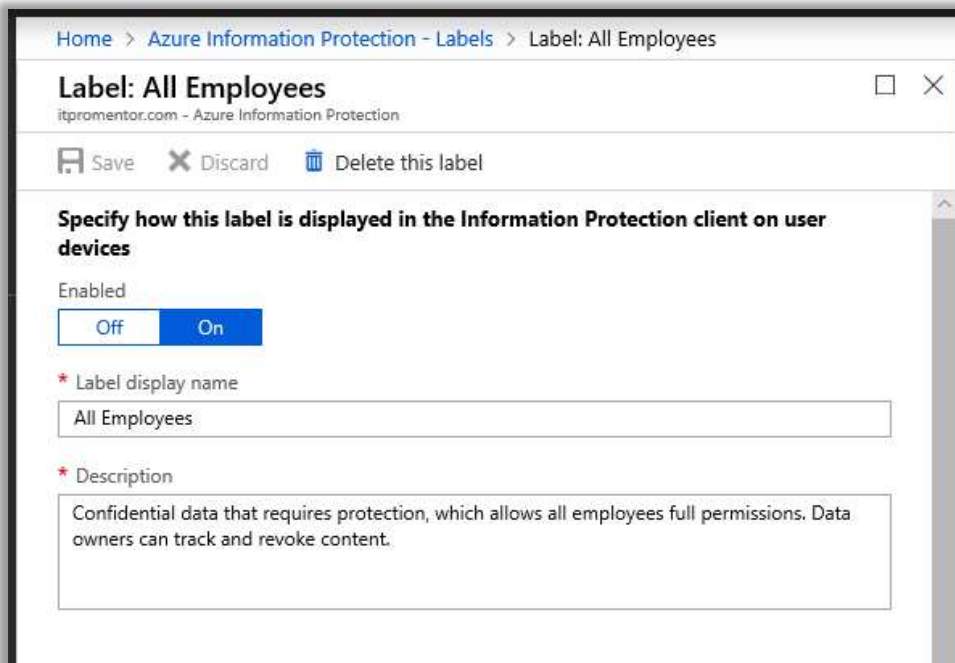
Configure AIP labels

Labels are managed and accessed via the [Azure Portal](#), on the **Azure Information Protection > Labels** blade. To begin exploring, check out the already existing *Confidential/All Employees* sub-label.



| LABEL DISPLAY NAME | POLICY | MARKING | PROTECTION |
|------------------------|--------|---------|------------|
| Personal | Global | | |
| Public | Global | | |
| General | Global | | |
| Confidential | Global | | |
| Recipients Only | Global | ✓ | ✓ |
| All Employees | Global | ✓ | ✓ |
| Anyone (not protected) | Global | ✓ | |
| Highly Confidential | Global | | |
| Recipients Only | Global | ✓ | ✓ |
| All Employees | Global | ✓ | ✓ |
| Anyone (not protected) | Global | ✓ | |

You will notice that all labels allow you to display the label in the AIP client, or not. This one is set to **Enabled > On**. Therefore, we expect to see it in the AIP client (and we do).



Home > Azure Information Protection - Labels > Label: All Employees

Label: All Employees

itpromentor.com - Azure Information Protection

Save Discard Delete this label

Specify how this label is displayed in the Information Protection client on user devices

Enabled

Off On

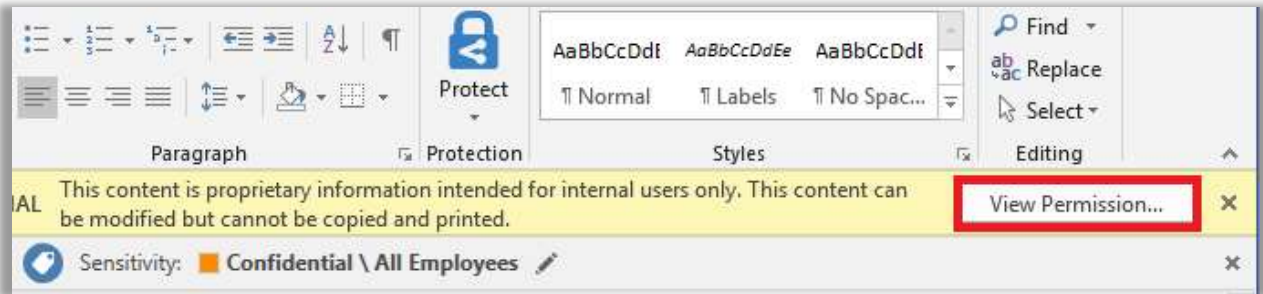
* Label display name

All Employees

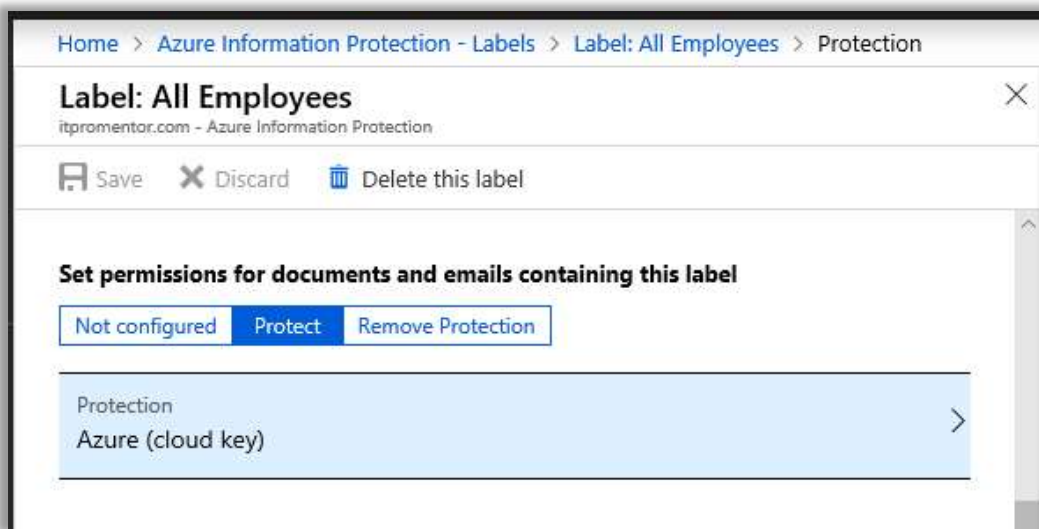
* Description

Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.

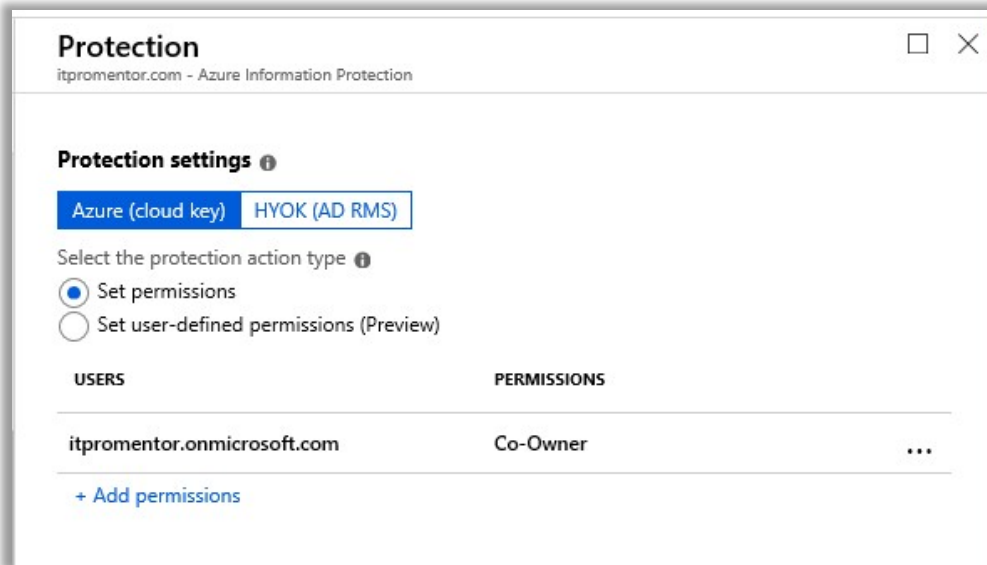
The name and description of the label shows up in a yellow bar at the top of the content, when end-users open a classified document. The bar also gives them the option to *View Permission* where they can look at any restrictions imposed for them.



Scrolling down further on the *Label: All Employees* blade, we find the settings for *Protection* (that is, encryption). Confidential / All employees are indeed encrypted documents by default. Click the **Protection** button to open a new blade, which allows us to review the access list and the permissions assigned.

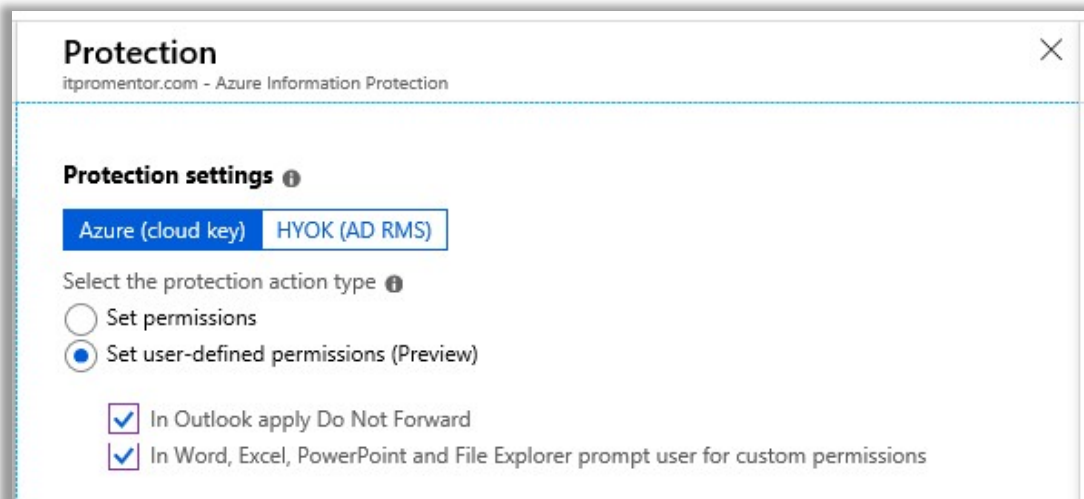


Focusing just on the first section here, we have controls for adding groups of users and assigning permissions. We can see that all users of my tenant are given *Co-Owner* permissions, using the default *Azure (cloud key)*—as opposed to using a key that you bring from an on-premises deployment of AD RMS. Using the Microsoft 365 Business SKU, we will always just use the Azure cloud key. Hold your own key (HYOK) requires Azure Info Protection P2, which is bundled in the E5 subscription.



Notice the toggle to either **Set permissions** explicitly, or to **Set user-defined permissions**.

Selecting the **Set user-defined permissions** radio button exposes two more options—the first one specific to sending email messages in Outlook—and it will apply the *Do Not Forward* permissions, which I previously described. The second option allows the user to apply their own permissions ad-hoc in Word, Excel, PowerPoint, and File Explorer.

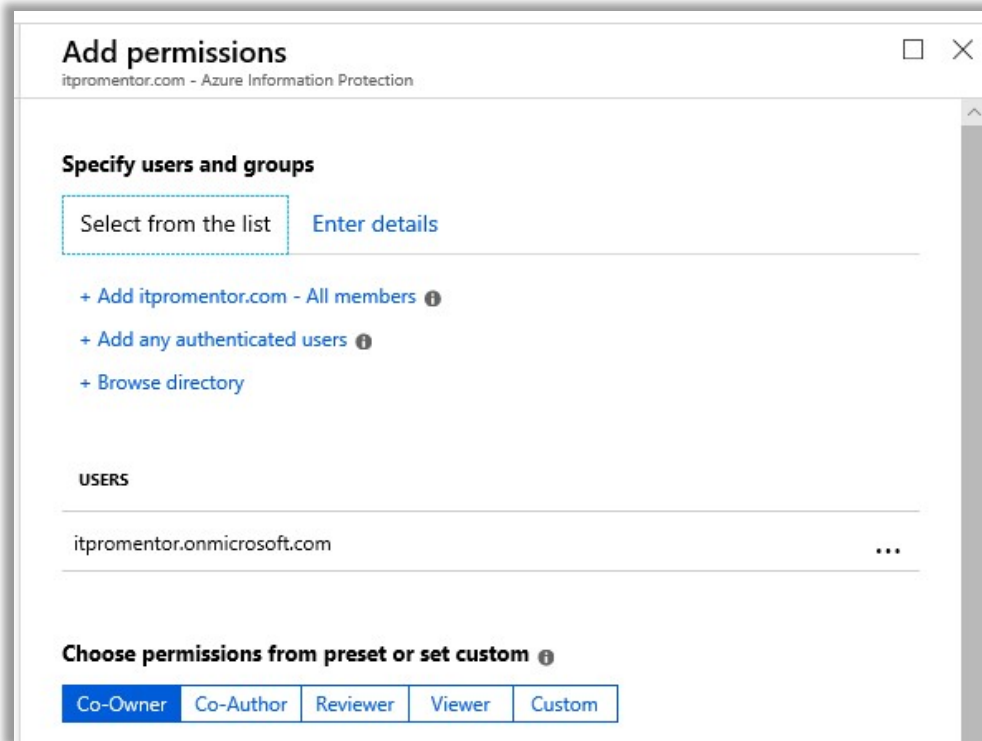


Back to assigning explicit permissions in **Set permissions**; let's take a closer look at the options there. When you select the option to **Add permissions**, you have a few options:

- **Add <tenantname> - All members** – Adds everyone in the organization to the access control list. This is the default selection for the *All employees* sub-label
- **Add any authenticated users** – This option does not specify anyone in particular, and so allows you to share the content with anyone (who has a Microsoft account) to access

the content, while still giving you the option to restrict permission (and revoke access if needed). Microsoft has some [additional notes](#) about this option, which we will discuss later.

- **Browse directory** – Here you can enter your own selection of individuals or security groups from your organization to the ACL
- **Enter details tab** – Go here to add external email addresses or domain names to the ACL



Once you have specified a user or group, you can then assign a permission from: *Co-Owner*, *Co-Author*, *Reviewer*, *Viewer*, or *Custom*. Each selection will display for you below which permissions are granted on the content. Custom, of course, means you can make your own selections.

| Permission | Co-Owner | Co-Author | Reviewer | Viewer |
|-------------------------|----------|-----------|----------|--------|
| View, open, read | Yes | Yes | Yes | Yes |
| View rights | Yes | Yes | Yes | Yes |
| Edit content | Yes | Yes | Yes | No |
| Save | Yes | Yes | Yes | No |
| Print | Yes | Yes | No | No |
| Copy | Yes | Yes | No | No |
| Reply | Yes | Yes | Yes | No |
| Reply All | Yes | Yes | Yes | No |
| Forward | Yes | Yes | Yes | No |
| Change rights | Yes | No | No | No |

| | | | | |
|-----------------------|-----|-----|-----|-----|
| Save As/Export | Yes | No | No | No |
| Allow Macros | Yes | Yes | Yes | Yes |
| Full Control | Yes | No | No | No |

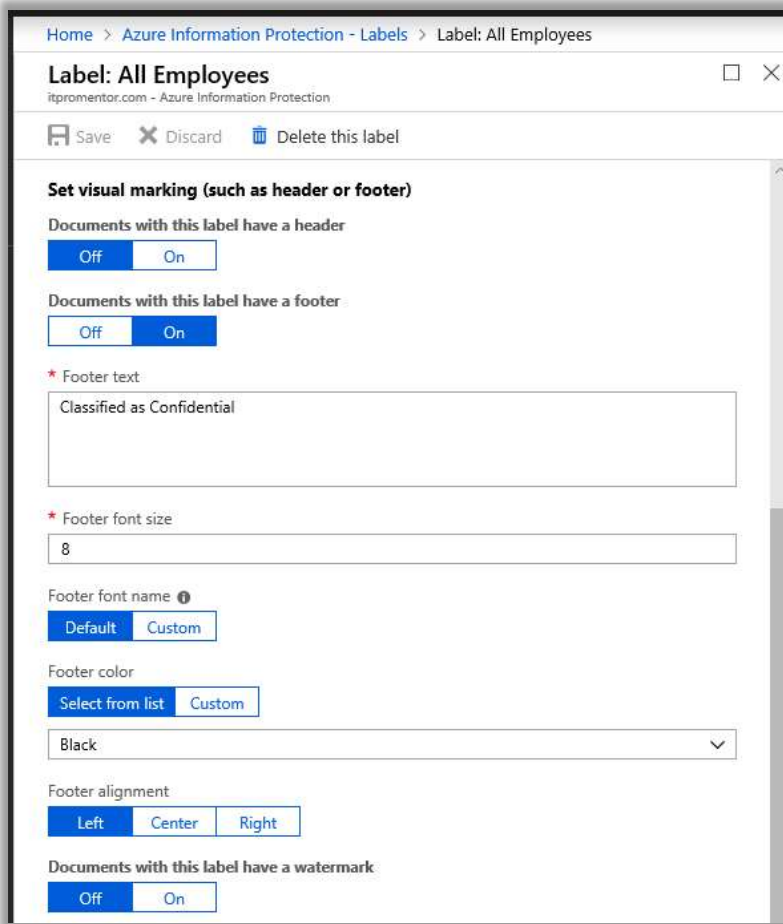
You can exit the blade without saving your changes. Back on the *Protection* blade, you can also find **Content expiration** and **Allow offline access**. What is pictured are the defaults for the *All employees* sub-label.

The screenshot shows two settings sections. The first section, 'Content expiration', has three buttons: 'Never', 'By date', and 'By days'. The second section, 'Allow offline access', has a description: 'Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)'. Below this are three buttons: 'Always', 'Never', and 'By days'. At the bottom, there is a text input field labeled 'Number of days the content is available without an Internet connection' with the value '30' and a green checkmark icon to its right.

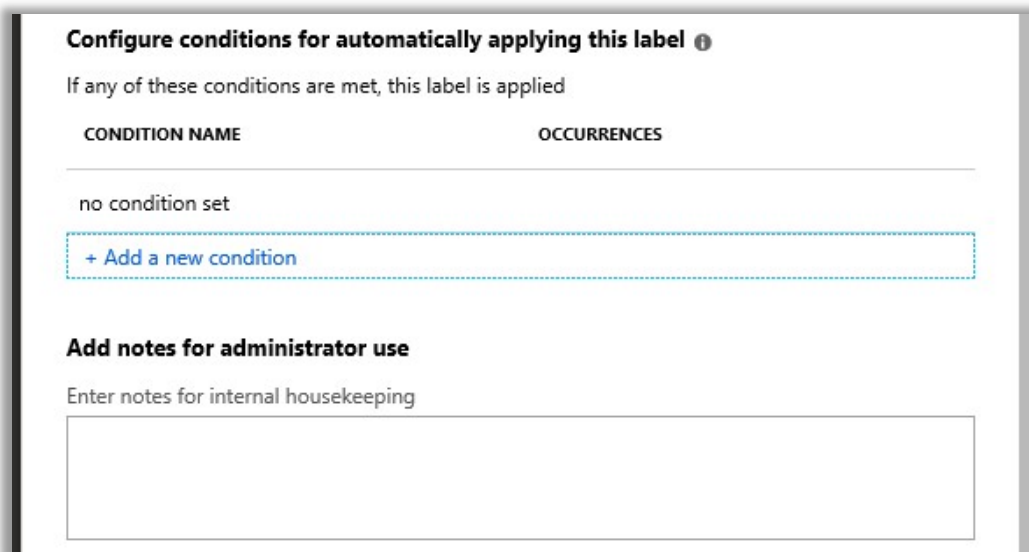
In the case of *Content expiration*, this just means that access can be scheduled to expire. Either on a specific date, or a certain number of days after the content is initially shared.

Allow offline access is a setting which enables a recipient to authenticate to gain their access and unlock the encrypted file, but then be able to continue opening the file without re-authenticating again for a certain number of days (or indefinitely). Obviously you would want to use this option with caution—especially for content that is able to be shared externally.

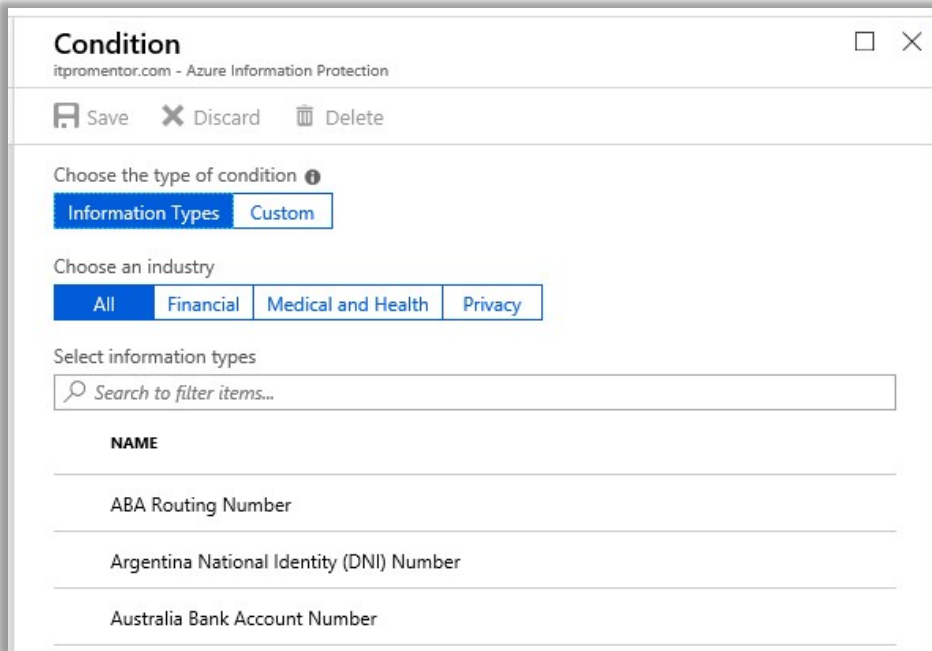
Exit this blade without saving any changes. On the label blade, scrolling down further we see that it is possible to configure headers, footers, and watermarks—all pretty self-explanatory.



And last, we find an option to classify documents based on conditions. Click **Add a new condition**.



This option allows you to give the user a prompt in the AIP client, to recommend this label for classifying the document, if a specific type of information is detected within the document (e.g. a credit card number or similar). This would require the P2 subscription (found in E5), and is therefore not applicable to the Microsoft 365 Business subscription.



Exit the *Condition* blade. Exit the *All Employees label* blade.

Default label templates in AIP

Below is a summary of the default labels that are included with AIP out of the box. Most of them are not applying any kind of encryption or marking, and therefore are not distinguishable except by label name (honor system). Anything with protection applied is enforcing a permissions list (ACL).

| Label | Encryption Settings | Content Marking |
|-------------------------------|----------------------------------------------------------------------------------------|-----------------|
| Personal | None | None |
| Public | None | None |
| General | None | None |
| Confidential | None | None |
| Recipients Only | User defined permissions In Outlook apply Do Not Forward | Footer |
| All Employees | Set permissions Add all tenant members, Co-Owner rights Offline access = 30 days | Footer |
| Anyone (no protection) | None | Footer |
| Highly Confidential | None | None |
| Recipients Only | User defined permissions | Footer |

| | | |
|-------------------------------|-----------------------------------------------------------------------------------------|--------|
| | In Outlook apply Do Not Forward | |
| All Employees | Set permissions Add all tenant members, Co-Author rights Offline access = 30 days | Footer |
| Anyone (no protection) | None | Footer |

Perhaps you would want to modify these defaults, for example it would be possible to add encryption even to *General* documents. Or add a watermark and tighten the permissions on *Confidential* and *Highly Confidential* a bit further. Or, you may want to abandon the defaults and create completely different labels depending on the environment and requirements.

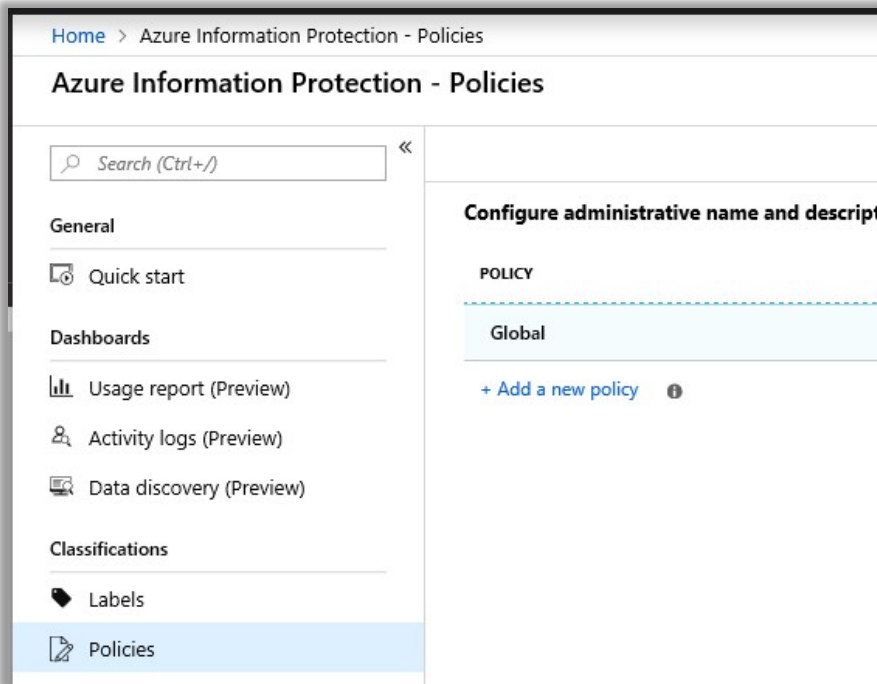
When planning your own classifications, content markings are usually easy decisions to make, but people tend to have trouble with protection. Think of the protection features this way:

- Some content is okay to share freely outside the organization with no encryption (e.g. Public)
 - No need to enable protection
- Some content is okay to share outside the organization, but you still want the ability to restrict permissions or revoke access to the content (e.g. Private, Privileged or Restricted)
 - Use either: User-defined permissions (custom/ad-hoc) or
 - Add any authenticated user (to define the permissions globally) or
 - Add specific outside email addresses and domains with permissions selections for each
- Some content should not leave the organization (e.g. Confidential, Highly Confidential)
 - Add all tenant members and choose permission levels
- Some content may not even leave a specific department or group (e.g. Finance or Management)
 - These can be sub-labels under something like Confidential or Highly Confidential
 - Add specific groups or individuals and apply permissions to each accordingly

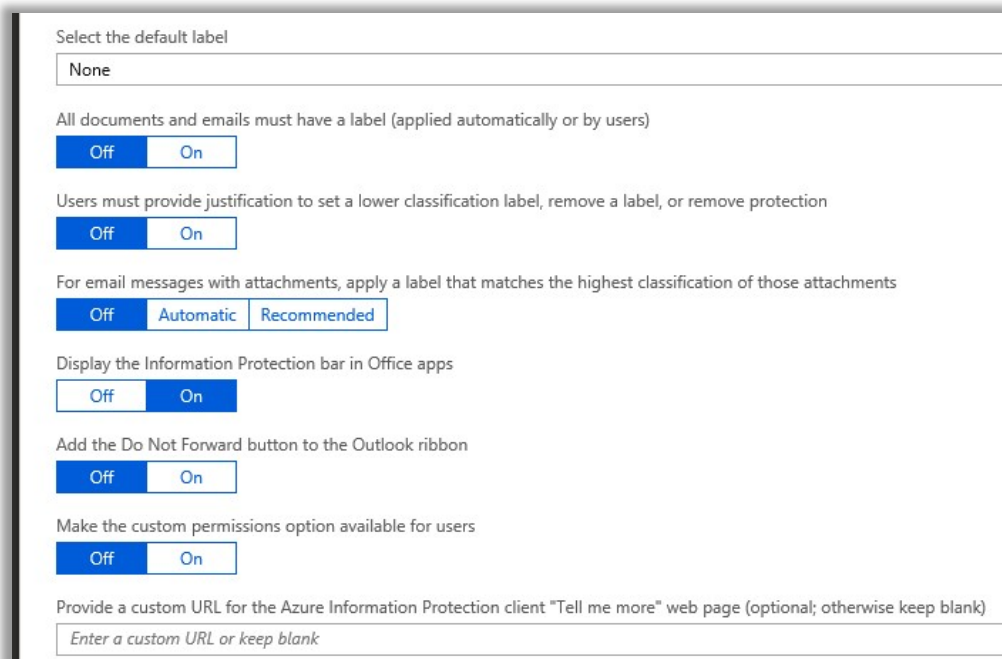
This can be a good kick-start to thinking through the data classification exercise, but there are so many iterations/variations to this, it would be impossible to cover them all—every organization is different, and some will surely surprise you with their requests.

Default global policy

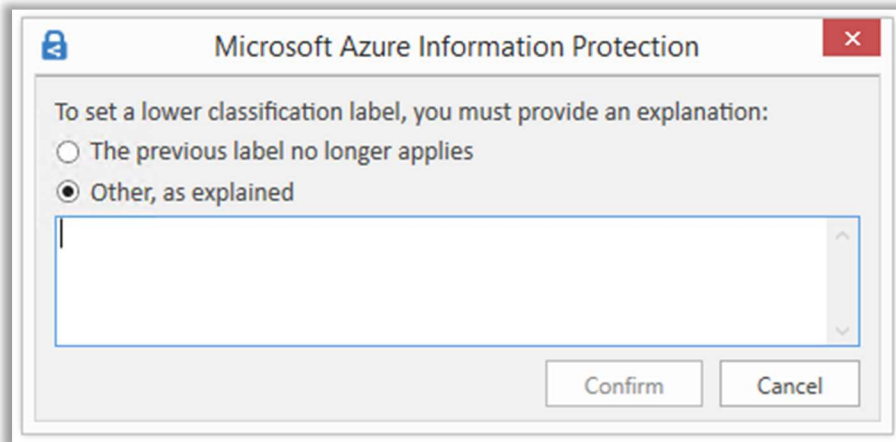
All the default labels are published via a default label policy called *Global*. Find it on the **Policies** blade.



The purpose of a policy is basically to assign a certain set of labels to a certain group of users. So beyond a name and description, that's the majority of what you see in the first section of this blade. At the bottom, we have options which can customize the experience of end-users who interface with the AIP client in the Office apps, and Windows Explorer.



Most of these are unconfigured, or “off,” by default. But it is common for SMBs to want to require users to provide justifications for “downgrading” or removing a label, as well as the option to enable the *Do Not Forward* button in Outlook (which we previously covered), if nothing else.

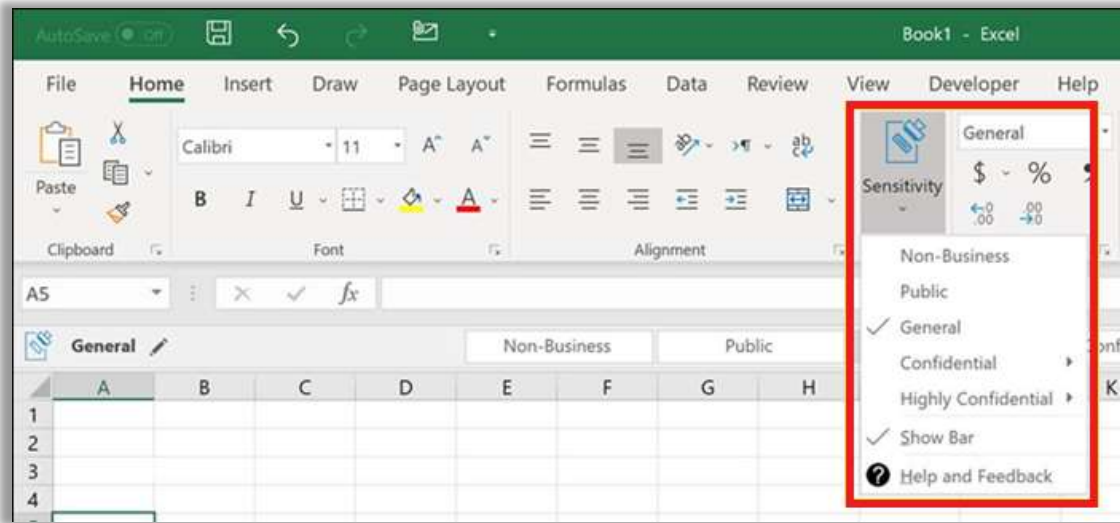


The other settings—like whether users **MUST** classify a document, or whether there is a “default” classification on new documents, etc.—those selections can be all over the place, and should also be discussed with the business stakeholders when implementing document classification.

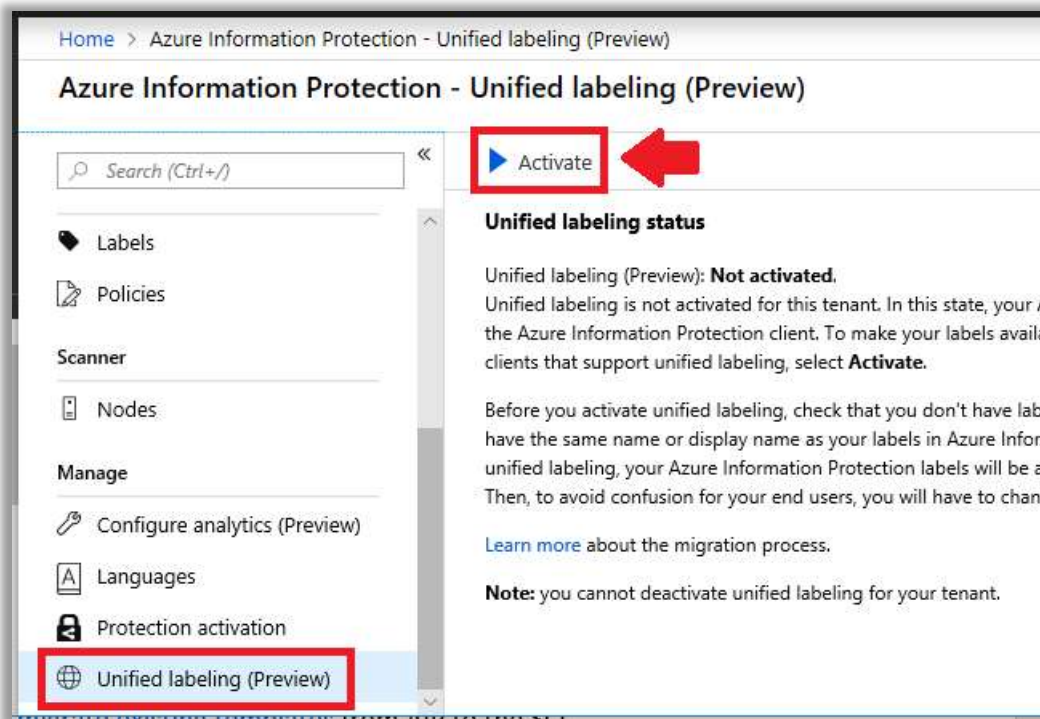
Office 365 Sensitivity labels

It is now possible to migrate AIP labels over to Office 365’s new **Sensitivity Labels** which are managed through the Office 365 [Security & Compliance Center](#) (SCC). Then, moving forward, you can manage labels via the 365 admin centers, and have any changes and additions reflected in AIP.

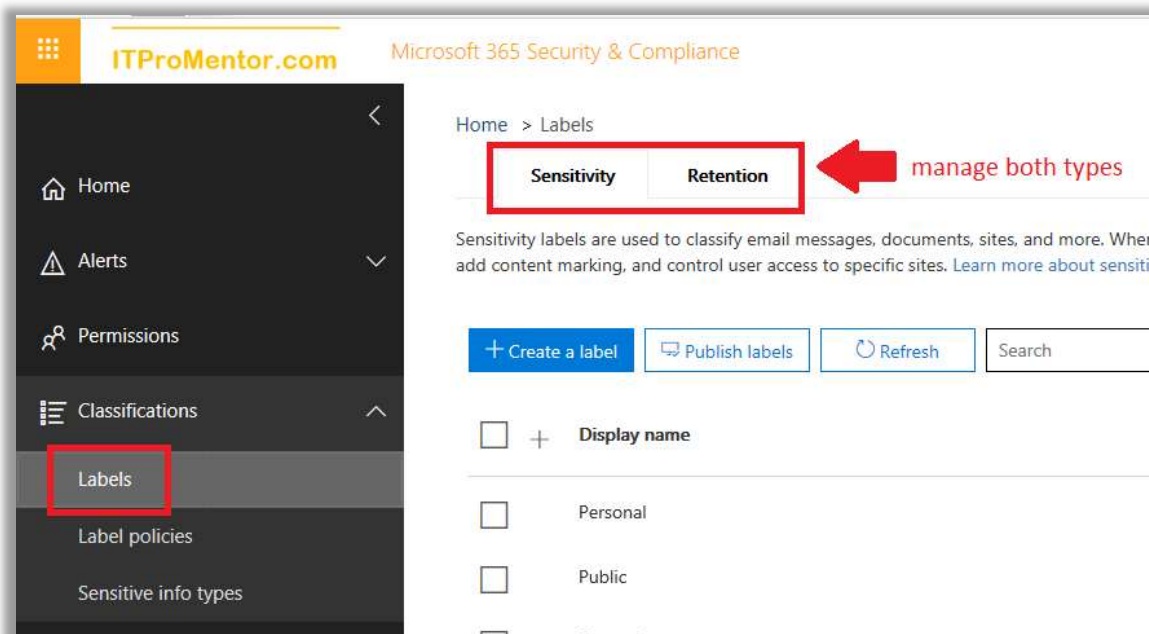
Note: If you make this move to “*Unified labeling*,” you still need to use the AIP client for the time being. But soon, it’s been promised that the Office applications will have *native* support for Sensitivity Labels, so that they will show up and be available *without* needing to install a separate client plugin (the button will say *Sensitivity* rather than *Protect*).



The label migration feature is still in preview at the time of this writing, but know that this process is also optional; there is no rush to move away from AIP, especially since the Sensitivity button is not available everywhere just yet. If you have configured no labels in either portal, then completing this migration process is painless, and involves literally one button (see below). Otherwise, see Microsoft's article describing how to [migrate existing labels](#) from AIP to the SCC, for some other guidance and caveats.



With that in mind, once you complete the migration to "Unified labeling" you are free to create your own labels in the Security & Compliance Center, and access them using the AIP client. To get started, navigate to: **Classifications > Labels**.



Through this new UI, you can manage both *Sensitivity* and *Retention* labels.

Sensitivity labels are used to apply encryption and protect content from being overshared. For example, you may want to label an email or document as *Confidential* and prevent accidental sharing with recipients external to the organization.

Retention labels by contrast are used in situations where you want to preserve and/or delete content after a certain amount of time has passed (e.g. content expires and is removed after 7 years).

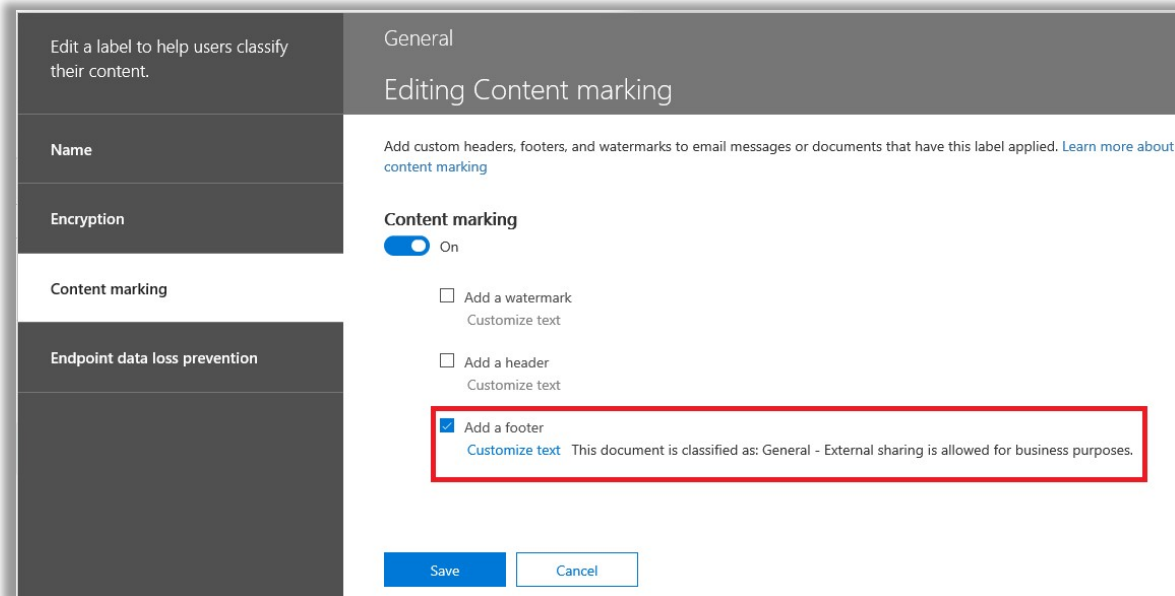
Planning data classification

Similar to what we talked about with AIP labels, planning your data classification with the stakeholders in the business is a crucial step, but often neglected. As an IT professional you should be transparent with the business owners and decision makers about your capabilities with this tool, and clearly define the meaning of each data classification label.

You have these options with Office 365 Sensitivity labels:

- **Encryption** – With the encryption option enabled, you can automatically expire access to shared content, allow or disallow offline access, and assign different permission levels to separate groups of users. Templates include *Co-Owner*, *Co-Author*, *Reviewer*, *Viewer*, or, create *Custom* permissions.
- **Content marking** – Apply headers and footers, and/or watermarks that clearly label the nature of the content on the document.
- **Endpoint Data Loss Prevention** – As of today, you would need a higher subscription level such as E5 to take advantage of this feature; [see pre-reqs here](#). We won't describe this in much detail except to say that when enabled, it signals to Windows endpoints that this data is extra sensitive, and cannot be copied or moved to, say, a USB device or other unsanctioned location.

In planning your labels, you may for example choose to enable *only* a footer on labels such as *General*. No other protections would be necessary, most likely.



However, for more sensitive content, such as *Confidential*, you may choose to use a watermark, *and* require encryption, limiting the permissions so that recipients cannot modify or redistribute content outside the organization. Note: the data owner always maintains full control permissions.

Confidential

Editing Encryption

Edit a label to help users classify their content.

Name Control who can access files and email messages that have this label applied. [Learn more](#)

Encryption ⚠️ Certain features (co-authoring, eDiscovery, and more) won't function correctly for OneDrive. [Which features are impacted?](#)

Content marking

Endpoint data loss prevention

Encryption On

Choose options that apply to
 Email messages and files

User access to content expires
 Never

Allow offline access
 Always

Grant permissions to specific users and groups *
[Assign permissions](#)

| Users and groups | Permissions |
|-----------------------------|-------------|
| itpromentor.onmicrosoft.com | Viewer |

Last note: the *order* in which these labels appear in the admin portal *does* matter (just like with AIP). Why they don't show some sort of sensitivity scale or something along the side is odd, but in fact, the top-most label on the list is the meant to be the *least* sensitive, while the labels down at the bottom of the list contain the most protection and the most restrictive settings.

Home > Labels

Sensitivity Retention

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user) the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

| <input type="checkbox"/> | + | Display name | Created by | Last modified | |
|--------------------------|---|---------------------|-------------|-----------------|-----|
| <input type="checkbox"/> | | Personal | Alex Fields | 1/2/19 8:41 PM | ... |
| <input type="checkbox"/> | | Public | Alex Fields | 1/2/19 8:41 PM | ... |
| <input type="checkbox"/> | | General | Alex Fields | 1/7/19 11:20 PM | ... |
| <input type="checkbox"/> | + | Confidential | Alex Fields | 1/2/19 9:51 PM | ... |
| <input type="checkbox"/> | + | Highly Confidential | Alex Fields | 1/2/19 8:41 PM | ... |

- + Add a sub label
- ↑ Move up
- ↓ Move down

Creating your own label

Let's just say that you are going to create your own labels. I have migrated the default labels from AIP, but maybe I want to add an even more restrictive "Top Secret" label to the tail end of the labels list... because I have so much Top Secret data that I work with, and I'm feeling all Top Secret today. Like my life is a *Mission Impossible* movie level of Top Secret.

Let's step through this process, by way of example. Click + **Create a label** to get started.

New sensitivity label

Name your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, and documents. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to your device.

● Name & description

● Encryption

● Content marking

● Endpoint data loss prevention

● Review your settings

Label name * ⓘ

Top Secret

Tooltip * ⓘ

This content is highly sensitive information intended for the recipient's eyes only.

Description ⓘ

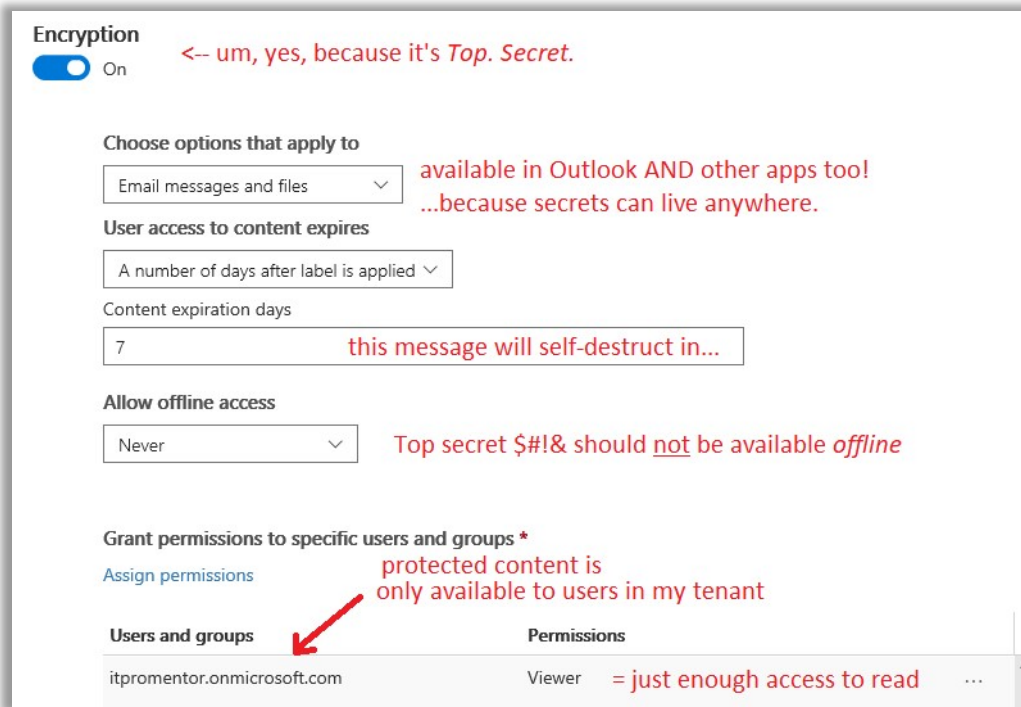
Enter a description that's helpful for admins who will manage this label

Next Cancel

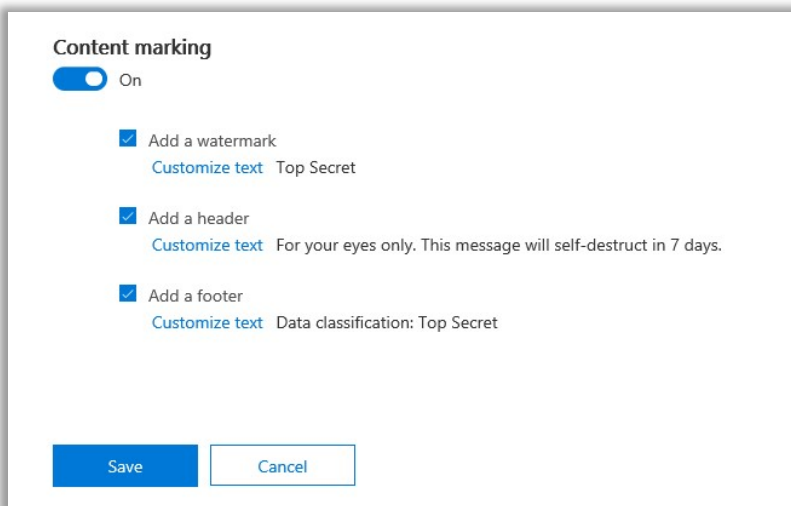
It is required to provide just two things here—a **Name**, and a “**Tooltip**” which is the short description that shows up on the bar or banner at the top of a document or email message when the label has been applied. **Next**.

On the **Encryption** page, we need to make some choices.

- First of all, yes—we want this turned **ON**. It's *Top Secret*, after all.
- Second, **User access to content expires**: We can force the content to expire after a period of time has passed, or not. I think, since we're talking about *Mission Impossible* here, that a self-destruction option feels best.
- The **Allow offline access** bit sounds scary to me. There is some black magic going on here which allows a user to authenticate once and then keep the token locally to re-open the document for a certain number of days without also re-authenticating, even if the endpoint goes offline, but I like the scenario where *this is not allowed not happen* much more. Given the top-secret nature of my data and all.
- Last, click **Assign permissions** to assign various users, groups, domains, outside email addresses, etc. various permissions levels. For this example, I am allowing recipients who belong to my organization /tenant the *Viewer* permissions, which contain just enough access to read the content, but do nothing substantial with it—edit, export, copy, print, etc.—all those actions are disabled.

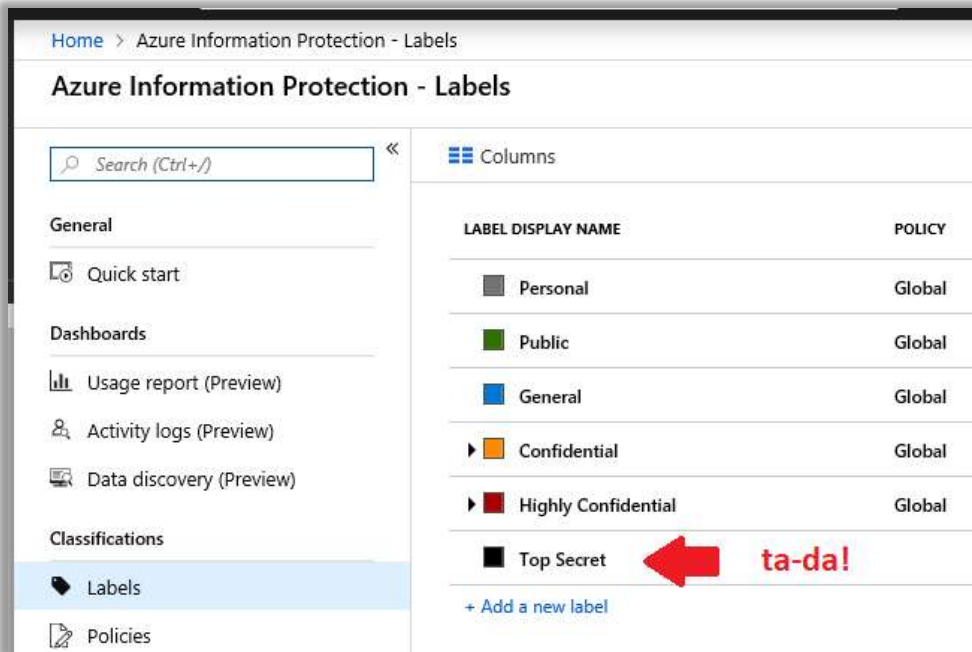


On the **Content marking** page, I am going to mark the crap out of this thing. Watermark? Check. Header? You bet, in **Red** text no less. Footer? Why not? One more reminder about the sensitivity of a document never hurt anyone when it came to TOP SECRET information.



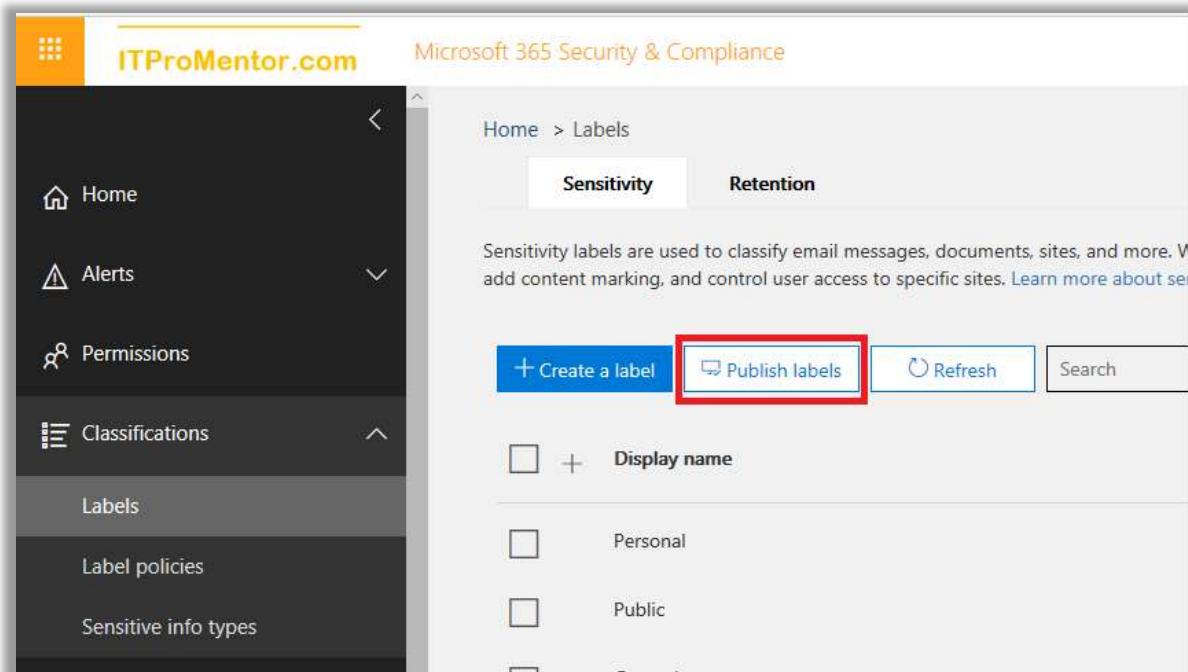
Now, Endpoint Data Loss Prevention. As I mentioned, this would not apply to the Microsoft 365 Business subscription, at least today. Maybe things will change in the future, but right now this would require Windows Information Protection (WIP) and Windows Defender ATP—which are available only at the Enterprise E5 level. So do not configure this option and just **Save** and **Close** after reviewing your selections.

Next, if you want to verify that the marriage between your AIP labels and the Office 365 labels is working correctly, go check out the Azure portal.

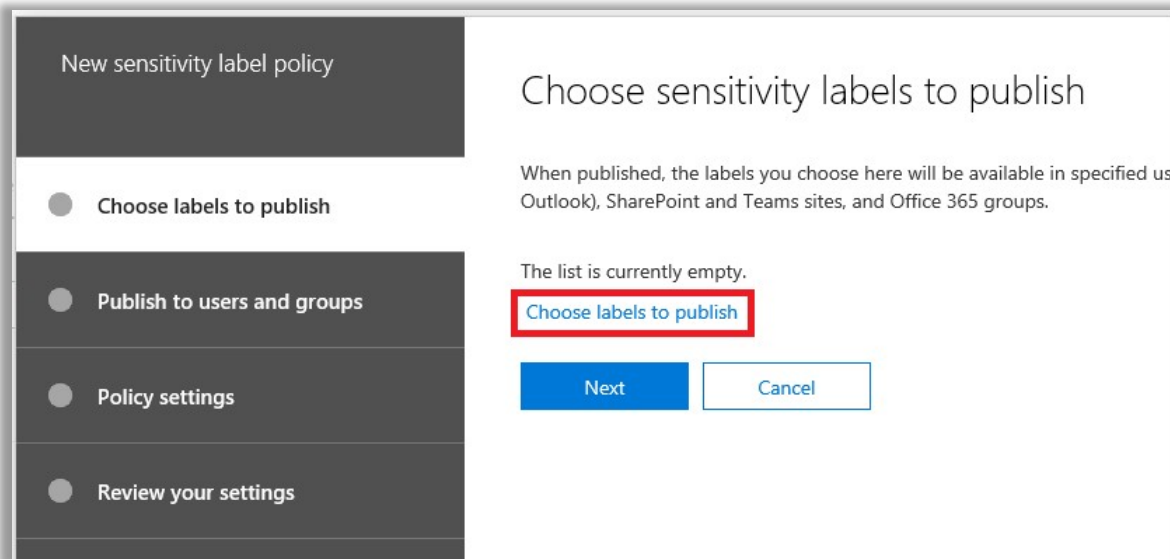


Publishing the labels

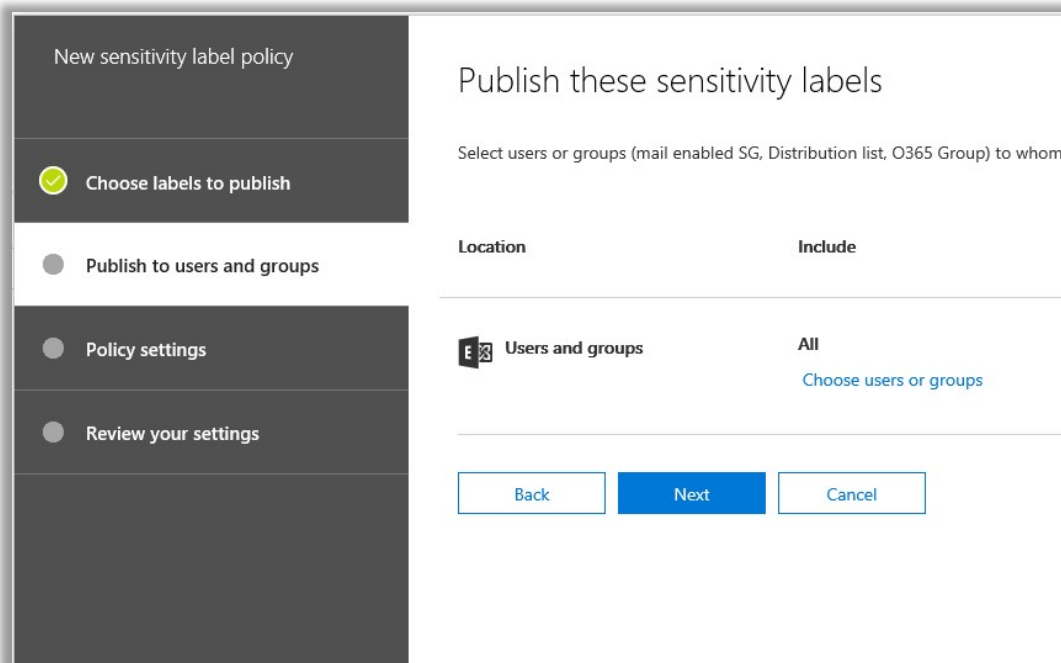
Once you have your labels all defined, you will want to publish them to your end-users. It is possible to publish different sets of labels to different people, but many small businesses will simply publish all the available labels to everyone. Click **Publish labels** to get started.



Click the link to **Choose labels to publish**. Select all the labels you want to publish and click **Add. Next**.



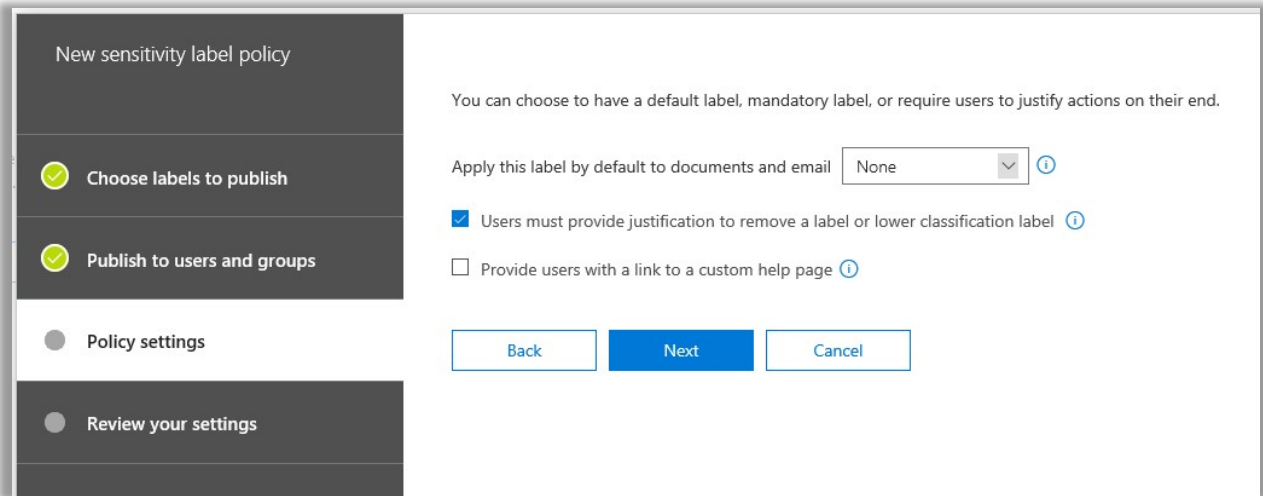
Choose users or groups to whom these labels will become available.



Next, on the **Policy settings** page, we find that it is possible to choose a default label which is applied to new documents or messages (or leave it set to **None** in case you do not want this behavior).

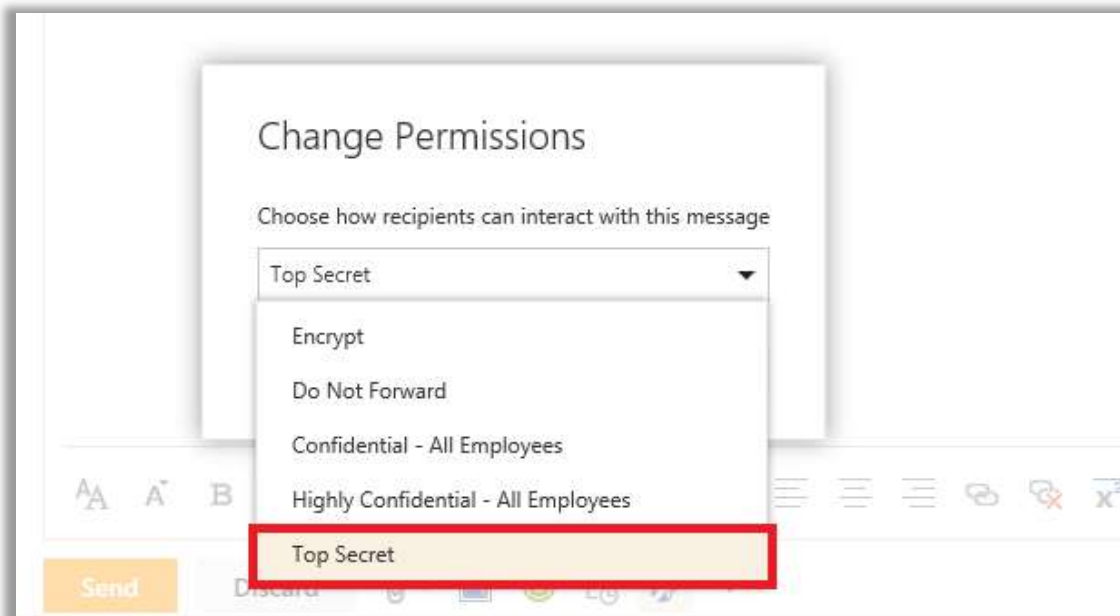
As well, we can require users to provide justification when removing or “downgrading” a classification. I would certainly recommend this setting.

Last, I don’t know that many small businesses would take the time to develop a custom help page for sensitivity labels, but maybe (calling IT providers...) this might be a cool thing to develop for your customers.

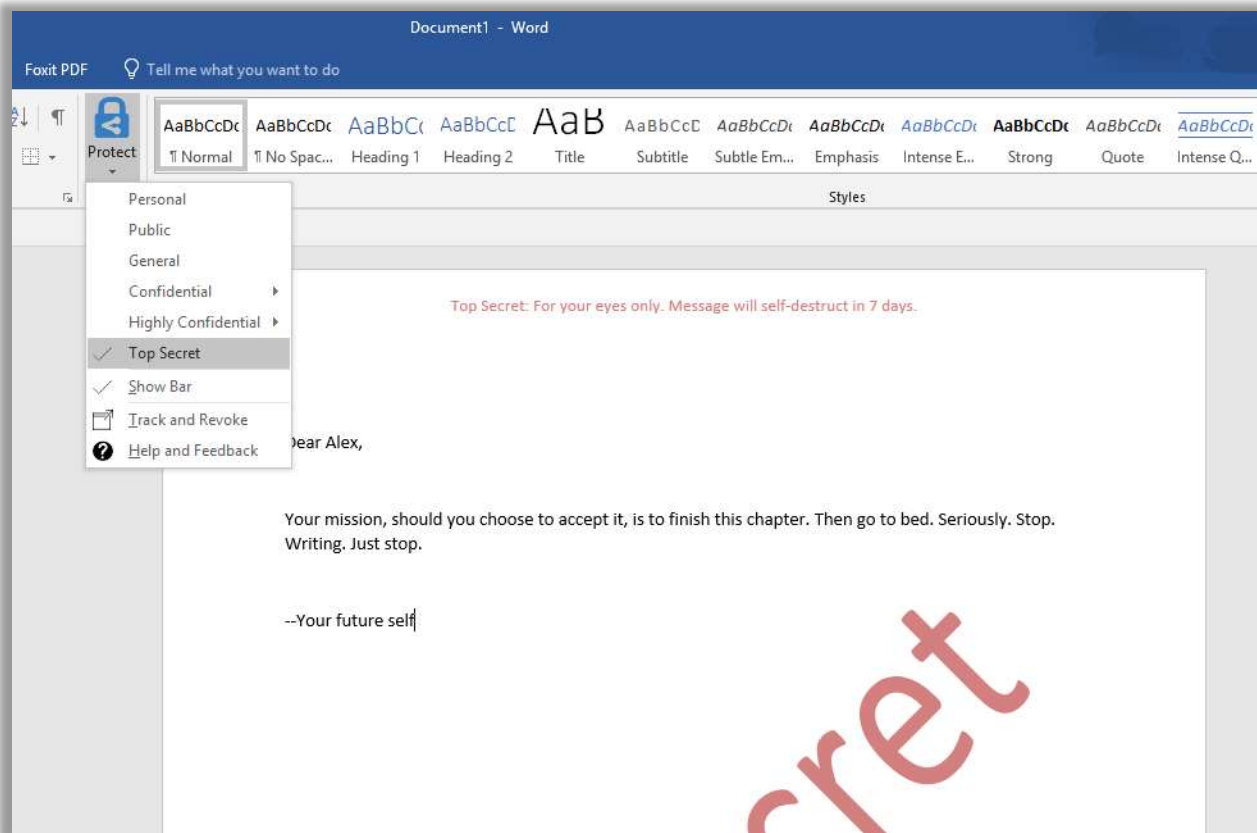


Working with labels in Office

Now, if you have previously configured the *Protect* button in Outlook using PowerShell, then you will find that your new sensitivity label is already available to use in Outlook on the Web.



As mentioned previously, to label content in the other Office apps will require the Azure Information Protection client to be installed on the workstation, for now. The AIP client is available from [Microsoft downloads](#). And yes, there is an MSI that you can deploy administratively.

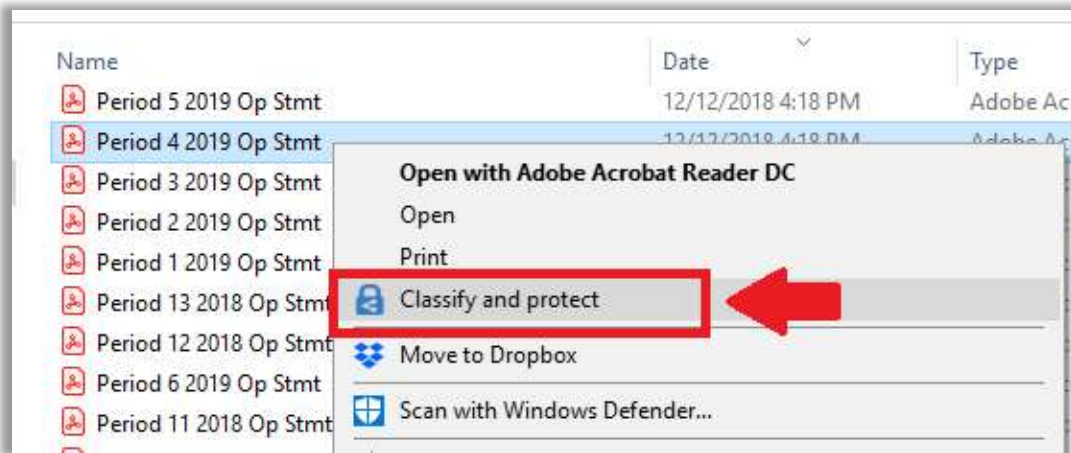


Once installed, the next time you open your Office application, you should see the *Protect* button. When I label my document as Top Secret, the watermarking and permissions I expect are applied.

AIP labels vs. Sensitivity labels

If you decide to stick with AIP for now—that’s totally cool. But even though you can “unify” the two disparate label sets, it is important to remember that they are not the same. Azure Information Protection is a more advanced subscription with more capabilities than what exists using the Office 365 Security & Compliance Center’s “Sensitivity labels”—again, for now.

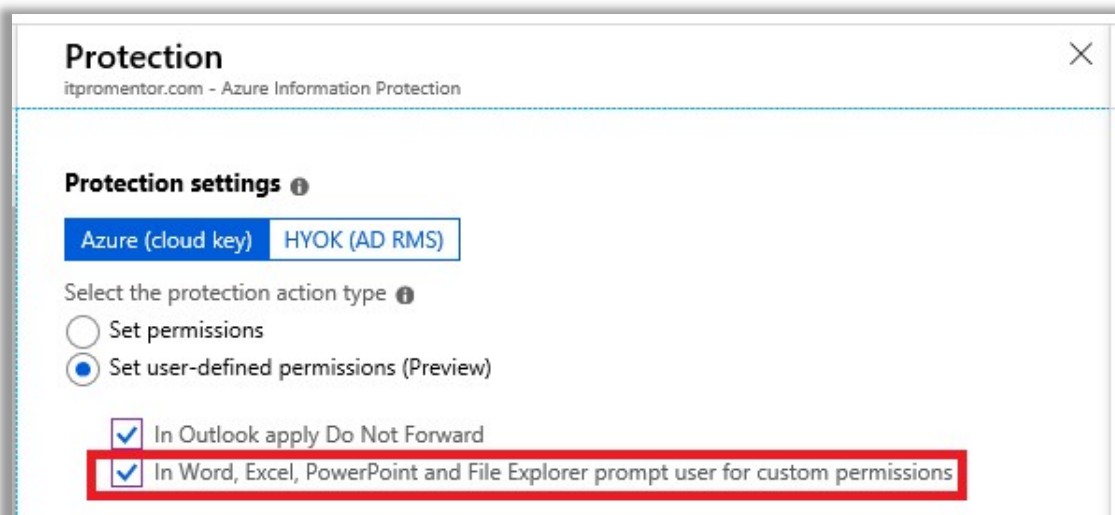
The main difference to note is that AIP is better suited to hybrid environments. You can use AIP to encrypt all types of documents (including PDF) on a traditional file server, for example, right in Windows Explorer.



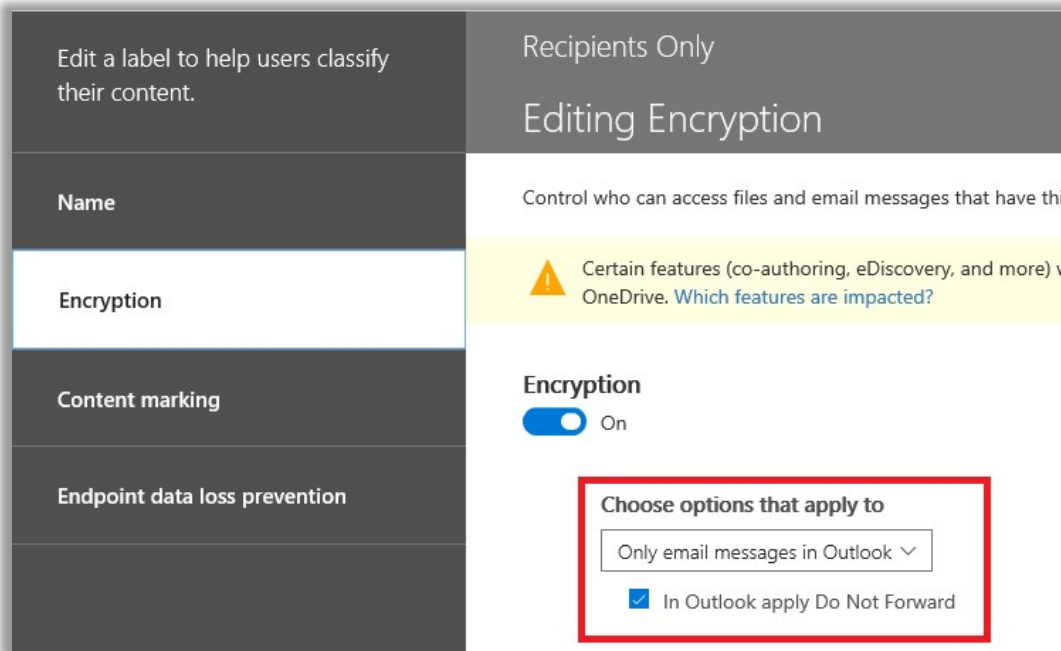
Therefore, AIP works whether you have Office 365 or not—you could even buy it as a standalone subscription and use it with any content, on any on-premises server, or any cloud, and so on.

These are not features that exist with Sensitivity labels, which are specifically tied to Office 365. For a cloud-first business with all of its document storage and transacting in 365, the additional features of AIP might not be necessary at all, but since you have access to this capability in Microsoft 365 Business, it's worth discussing with the business stakeholders.

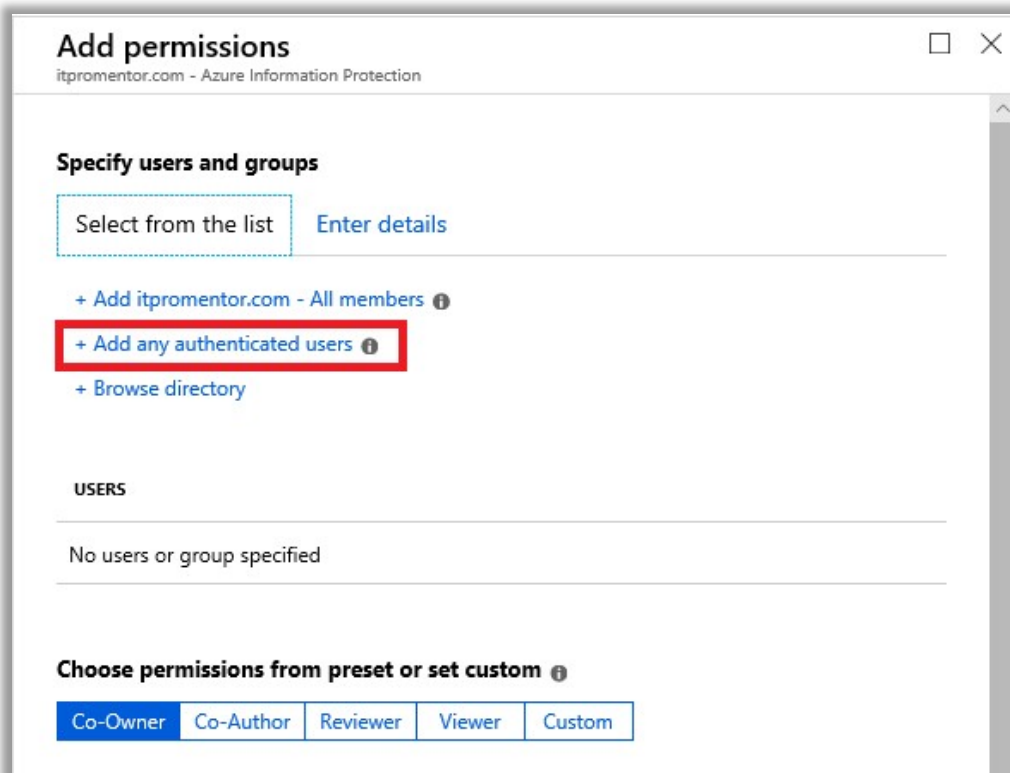
Another notable difference: as we go to configure protection settings on a label in AIP, we will find an option to either **Set permissions** administratively, or, to **Set user-defined permissions**. There is no equivalent to the second option in the SCC: *In Word, Excel, PowerPoint and File Explorer prompt user for custom permissions*. The native Office 365 Sensitivity labels do not appear, at this time, to support user-defined "Custom" permissions, as the AIP client does.



Now if you were to choose ONLY the first checkmark box above: *In Outlook apply Do Not Forward*, then that would be the equivalent of choosing the *Only email message in Outlook* option with the corresponding checkmark box for the Do Not Forward button in the SCC wizard.



If you assign permissions administratively, then in specifying users and groups for the recipients of a labeled document we find this: **Add any authenticated users**—people who might be *outside* of your tenant.



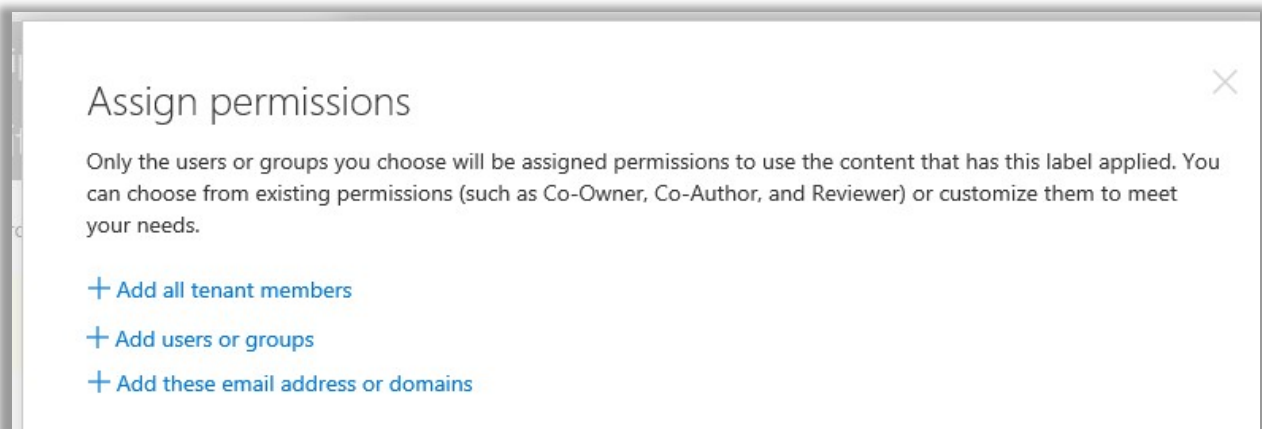
[From Microsoft](#): "This setting doesn't restrict who can access the content that the label protects, while still encrypting the content and providing you with options to restrict how the content can be used (permissions), and accessed (expiry and offline access).

However, the application opening the protected content must be able to support the authentication being used. For this reason, federated social providers such as Google, and onetime passcode authentication should be used for email only, and only when you use Exchange Online and the new capabilities from Office 365 Message Encryption. Microsoft accounts can be used with the Azure Information Protection viewer and Office 2016 Click-to-Run.

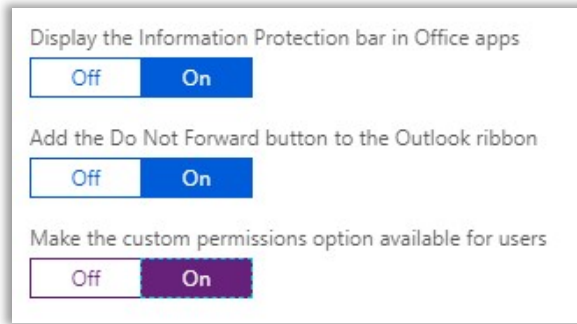
Some typical scenarios for the any authenticated users setting:

- You don't mind who views the content, but you want to restrict how it is used. For example, you do not want the content to be edited, copied, or printed.
- You don't need to restrict who accesses the content, but you want to be able to track who opens it and potentially, revoke it.
- You have a requirement that the content must be encrypted at rest and in transit, but it doesn't require access controls."

Again, there is no equivalent to this in the SCC. You *can* add external email addresses or domains (and this same capability is present under the *Enter details* tab in the AIP blades), but the lack of the "Any authenticated user" option means that you, the administrator, would need to know in advance any potential external users that would fall under the scope of this label. Handy for sharing with known partner organizations, but not very helpful for allowing users to distribute protected content to *anyone* (well, anyone with a Microsoft account and AIP viewer, anyway).



Last, as we go to publish our labels via a policy, in the SCC we will **not** find the toggles to control extra buttons that show up in the ribbon, including the *Do Not Forward* button or the option for users to apply their own custom permissions.

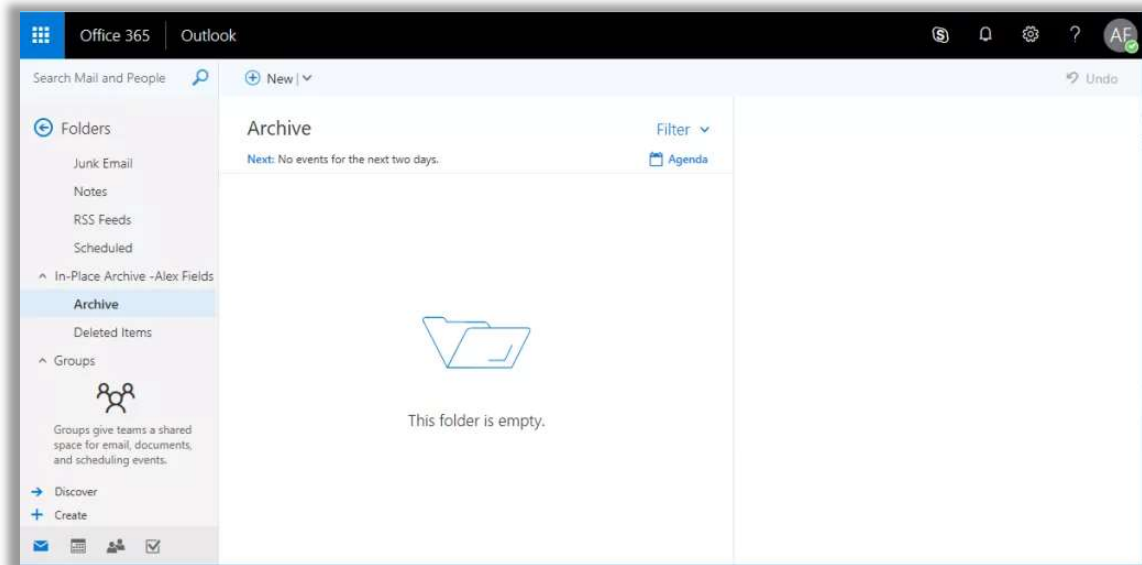


This makes sense since, again, the SCC interface would not contain settings for the AIP client. Time will tell if the built-in Sensitivity functions will include support for extra buttons such as *Do Not Forward* (or *Encrypt?*) in the future.

And there are other differences. For example, in the P2 subscription of AIP (e.g. available in E5), you get access to auto-classifications. There is also an on-premises scanner which can find and classify content on traditional file servers. But as pertains to the Microsoft 365 Business subscription, I think I've identified most of the significant differences between the two.

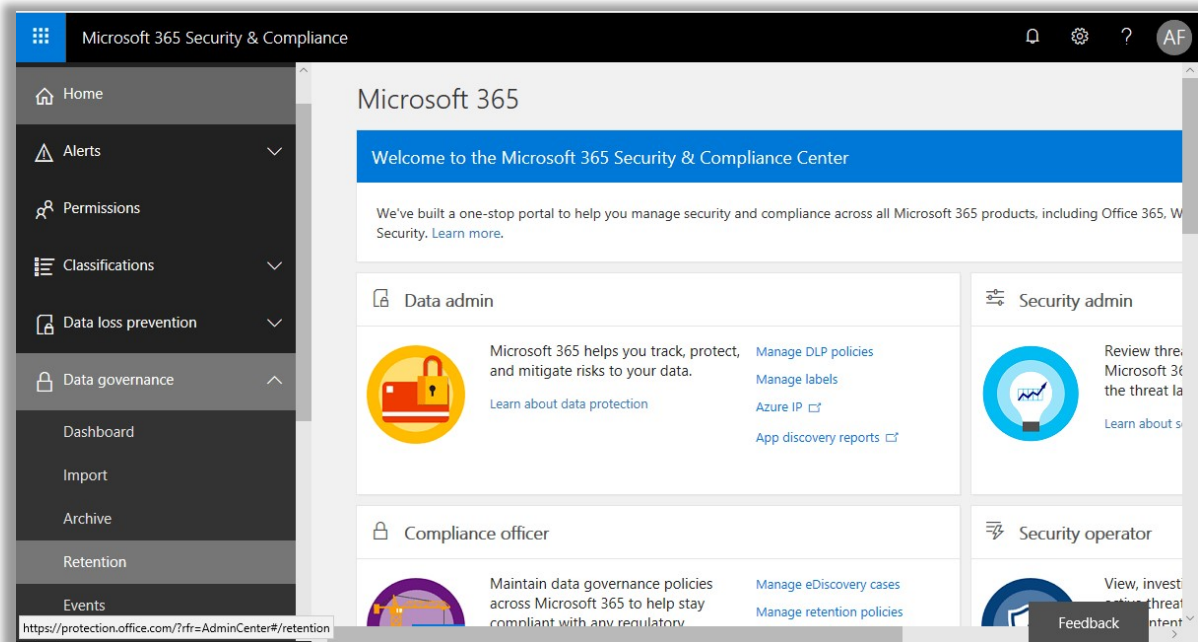
Data Governance: Archive and retention

Under the *Data governance* area in the Security & Compliance Center, we will find both *Archive* and *Retention*. The first of these allows you to enable an archive mailbox for each user, which is available because the Microsoft 365 Business bundle includes the Exchange Online Archiving subscription.



The *archive mailbox* is like a long-term storage container which appears in Outlook, underneath the user's primary mailbox. By default, a canned policy will automatically sweep data older than two years into this archive mailbox. However, users can move items into it at any time, and, as an administrator, you can adjust the default auto-archive policy.

Note that archiving items into this mailbox is not the same as *preserving* email records via a retention policy. For example, you could delete data out of an archive mailbox, and without a hold or retention policy in place to protect that data, you would have a limited amount of time (30 days) to recover that data, but eventually it would be gone forever.



Retention in the Security & Compliance Center is used for two purposes:

1. *To Preserve* data, keeping it safe and accessible (e.g. via eDiscovery searches)
2. *To Delete* data when it reaches a certain age

As administrators, we can apply retention policies broadly across Office 365 content locations, and, we can also publish individual labels that provide users with another option to self-categorize content.

A crucial point to remember is that whenever two policies or labels are in conflict, preservation always wins. For example, if you have an organization-wide policy which deletes email data after five years, but a user has applied a seven-year retention label to an email message, then preservation will win and the content won't be deleted until the seven-year retention period has passed.

Retention policies in Office 365 also meet the requirements for SEC rule 17a-4 (sometimes known as WORM or Write-Once-Read-Many—meaning that once written, the data is

unalterable in its preserved state). In the United States, this is helpful in the financial services industry, to demonstrate compliance with certain laws and regulations. Microsoft has even [published a whitepaper](#) on it.

Enable the Archive mailbox

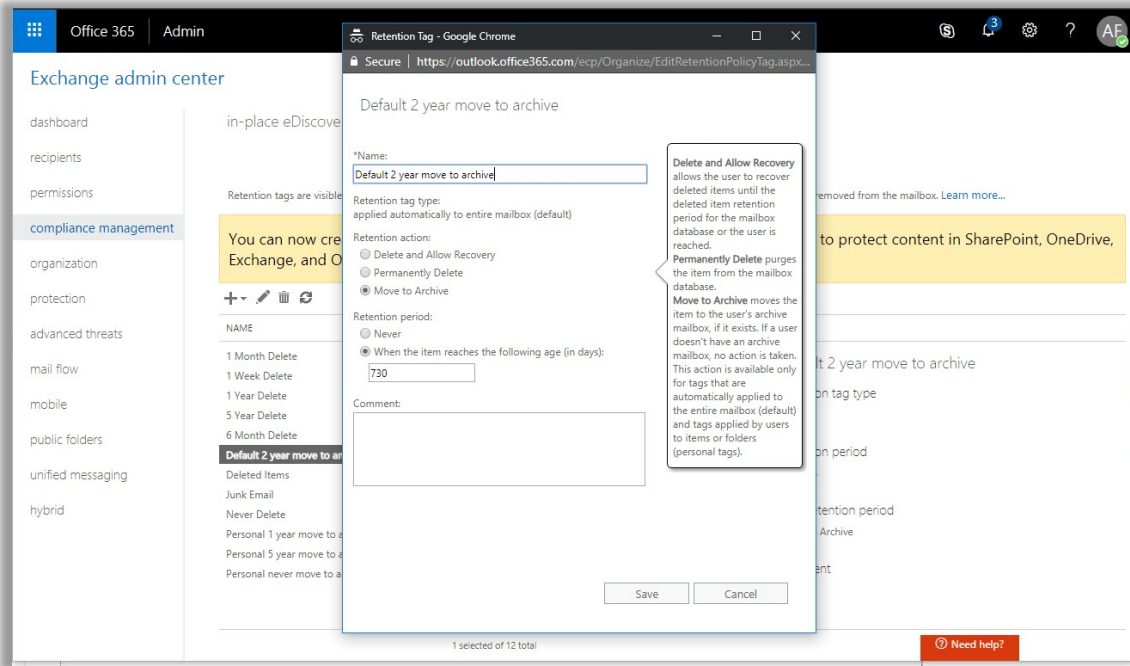
Enabling this mailbox for users is very easy, but pay attention to what I'm about to tell you: *where* you enable it changes based on whether you are in a full-blown hybrid environment, or cloud-only. On any account being synchronized via Azure AD Connect, it is necessary to enable the archive mailbox on-premises and let that update sync to the cloud, where the archive mailbox will then become provisioned. Otherwise, this operation is performed in the cloud directly, for cloud-only accounts.

However, before we enable the archive mailbox, swing over to the **Exchange Admin center**.

You should know going in that you can find and modify default retention tags and policies, including the default policy which moves items older than two years into archive. These modifications are done in the cloud, regardless of whether you have a hybrid/Azure AD Connect environment or not. Go to **compliance management** on the left, and then **retention tags** at the top.

| NAME | TYPE | RETENTION PERIOD | RETENTION ACTION |
|---------------------------------------|----------------|------------------|------------------|
| 1 Month Delete | Personal | 30 days | Delete |
| 1 Week Delete | Personal | 7 days | Delete |
| 1 Year Delete | Personal | 365 days | Delete |
| 5 Year Delete | Personal | 1825 days | Delete |
| 6 Month Delete | Personal | 180 days | Delete |
| Default 2 year move to archive | Default | 730 days | Archive |
| Deleted Items | Deleted Items | 30 days | Delete |
| Junk Email | Junk Email | 30 days | Delete |
| Never Delete | Personal | Unlimited | Delete |
| Personal 1 year move to archive | Personal | 365 days | Archive |
| Personal 5 year move to archive | Personal | 1825 days | Archive |
| Personal never move to archive | Personal | Unlimited | Archive |

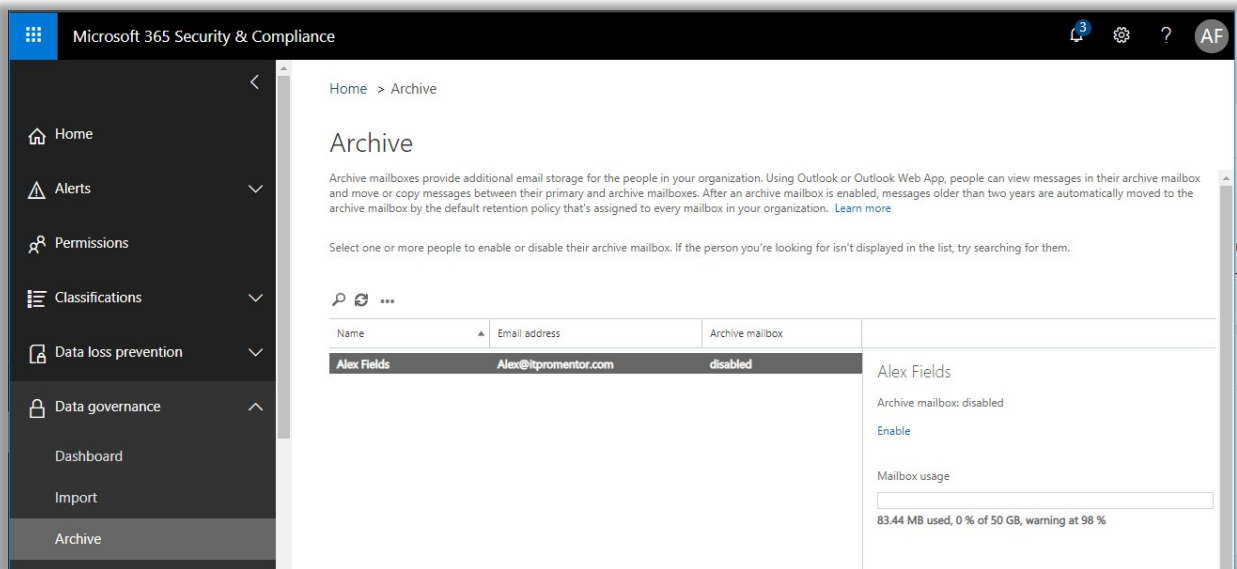
Open the **Default 2 year move to archive** tag, and from here you can rename the tag, and change the retention period to whatever value suits your environment. Click **Save**.



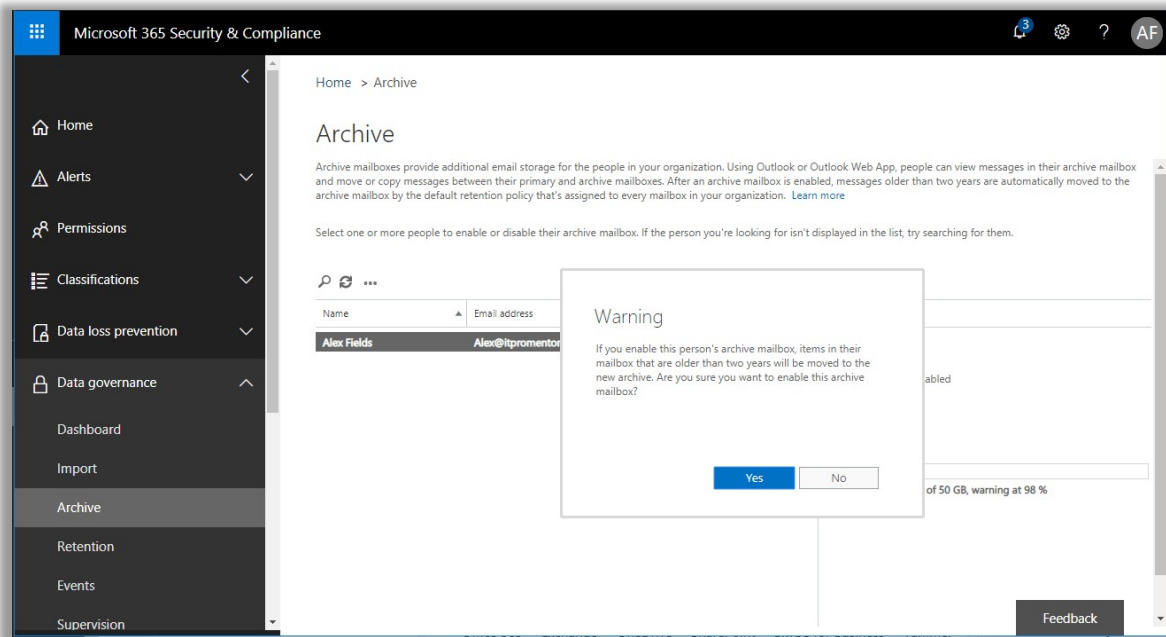
You might choose one year, or three years, or some other value, depending on your own requirements/preference.

Enable archive mailbox for cloud-only accounts

From the **Exchange admin center** > **recipients** > **mailboxes** — just select a user's mailbox to enable the archive from the right-hand pane. You can also find this same option from the **Security & Compliance Center**. Click on **Data governance** > **Archive** from the left menu, pick a user, and select **Enable** from the right pane.



When you do this, it will present a warning regarding that default policy we talked about—any items older than two years will automatically be moved here. Say **Yes** to continue.



Enable archive mailbox for hybrid users

On-premises, you should be able to locate the user in the Exchange admin center, just as you would in Exchange online, and then enable the archive mailbox, just like you do when it's in the cloud. You can also use a PowerShell command in the Exchange management shell, which is even easier:

- Enable-RemoteMailbox *USERNAME* -Archive

If you do not have an Exchange server installed but are using Azure AD Connect, it will be necessary to modify the Exchange attributes via ADSI edit to enable the archive mailbox.

Two values need to be modified:

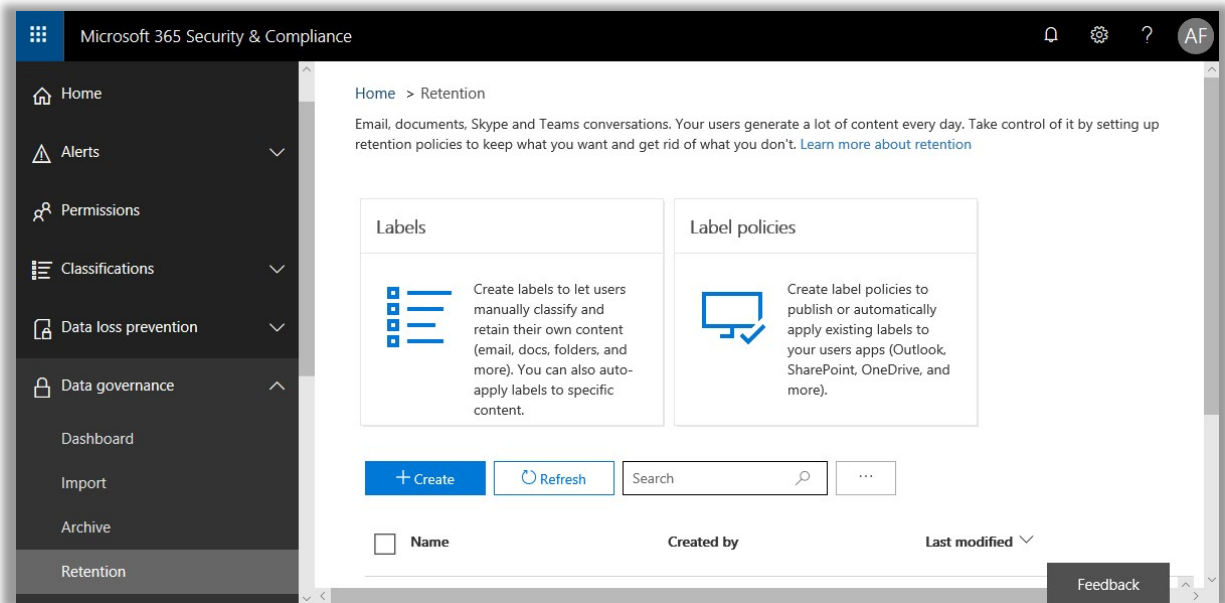
- **msExchArchiveName** = (give this any name like "**Personal Archive – Username**")
- **msExchRemoteRecipientType** = (change the value to **3**)

Once you have made these modifications on the user object's attributes in ADSIedit, or via the View > Advanced settings/Attributes tab within ADUC, when the next Azure AD Connect sync cycle runs, you will see the Archive mailbox show up in the cloud.

Remember: enabling a personal archive can be a useful tool for managing mailbox sizes and clutter-creep, but it is not a great tool for managing compliance requirements or retention of data on its own, without further configuration of retention policies and tags.

Configure retention policies

Under **Data governance**, pick **Retention**. Simply choose **Create**. You will start by giving it a name and proceeding. By way of example only, we will build an example policy that retains content for five years from the date it was last modified, then deletes it thereafter. Keep in mind that your own circumstances could require a completely different policy.



Now, you can begin to build your new policy. Notice, for example, that while you can set up to *retain*, *retain and delete*, or to just *delete* content older than a certain time frame. Be sure you understand your own organization's requirements before implementing your options.

Create a policy to retain what you want and get rid of what you don't.

- ✔ Name your policy
- Settings
- Choose locations
- Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 5 years

Retain the content based on when it was last modified ⓘ

Do you want us to delete it after this time? ⓘ

Yes No

No, just delete content that's older than ⓘ

1 years

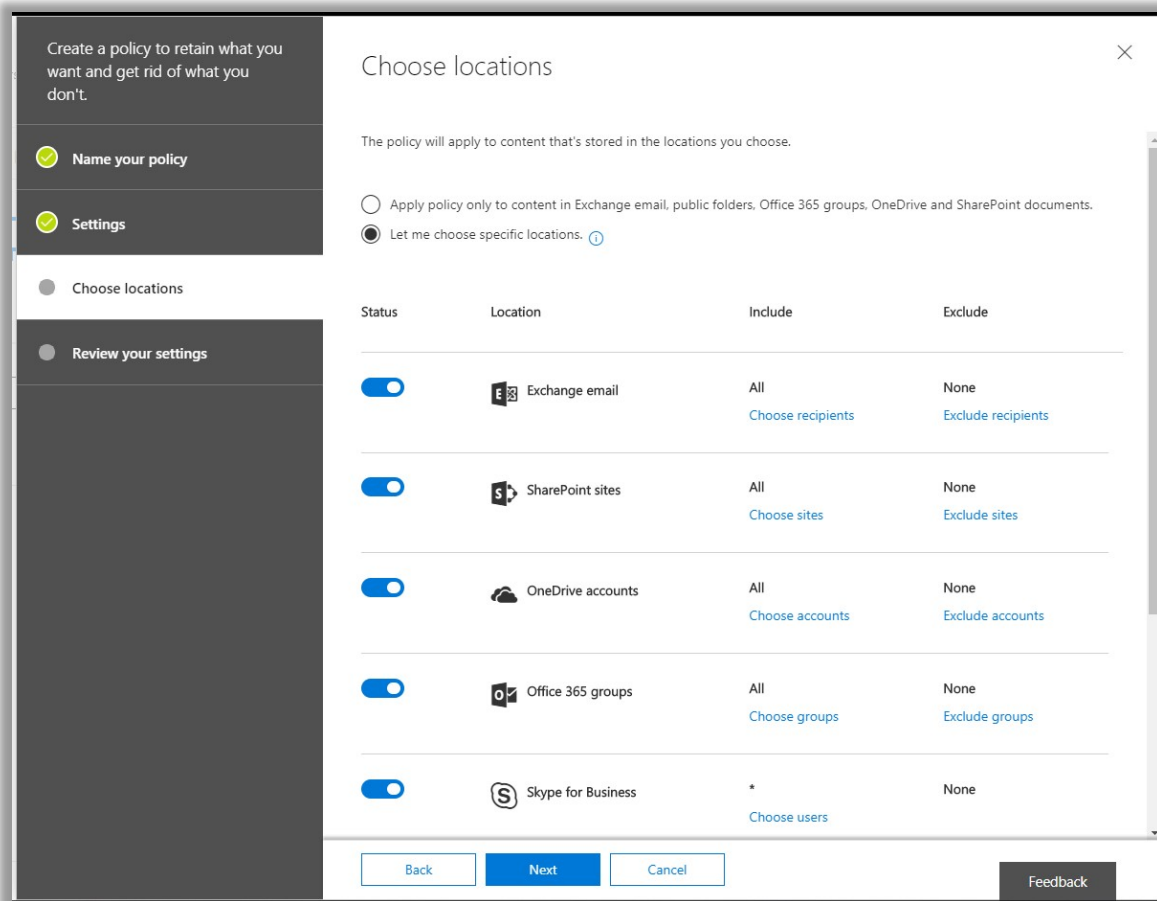
Need more options?

Use advanced retention settings ⓘ

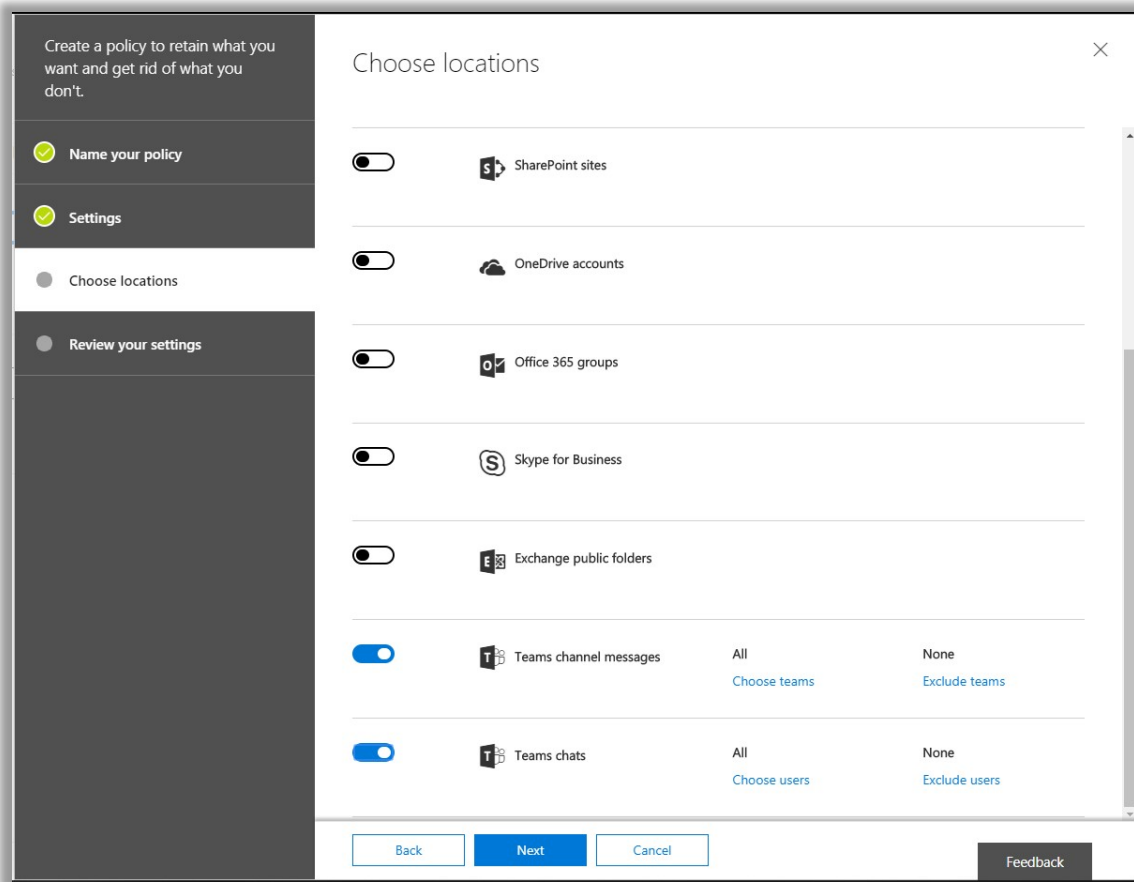
Back Next Cancel

Feedback

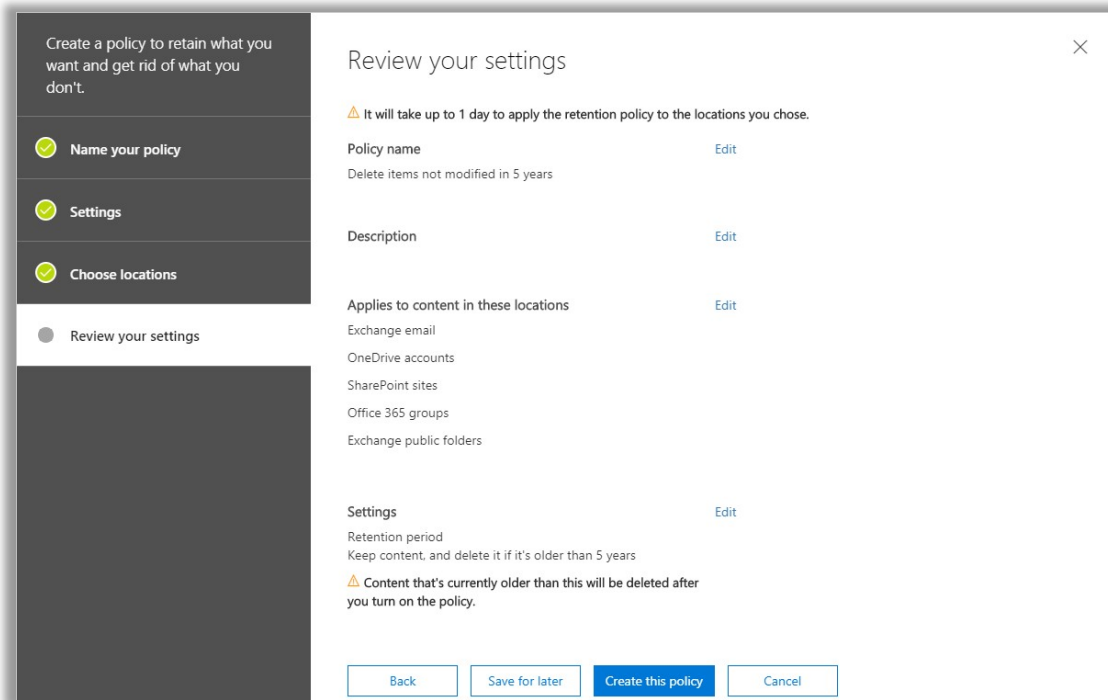
Next you can choose specific locations to which this policy applies—notice that it can be configured against just *one* or across *many* of the services within Office 365.



However, it should be noted that at the time of this writing, it's not possible to create a policy that will *also* apply to content in Teams. For whatever reason, when you select Teams channels and chats, it will automatically deselect all other locations for you. Therefore, it may be necessary to build Teams-specific policies alongside your other services, at least for now.



Finally, review the policy settings one more time before you **Create this policy**.



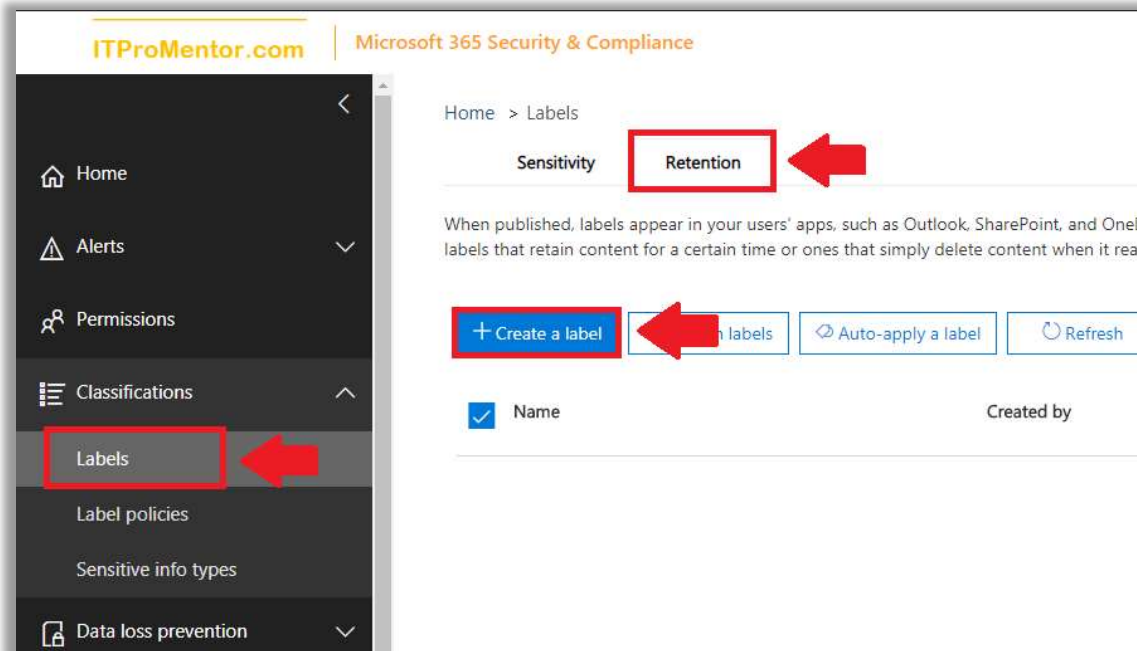
This is a very basic example, but it demonstrates what is possible: you can quickly deploy rules which preserve and/or delete data, as needed, from this central interface.

Creating custom retention labels

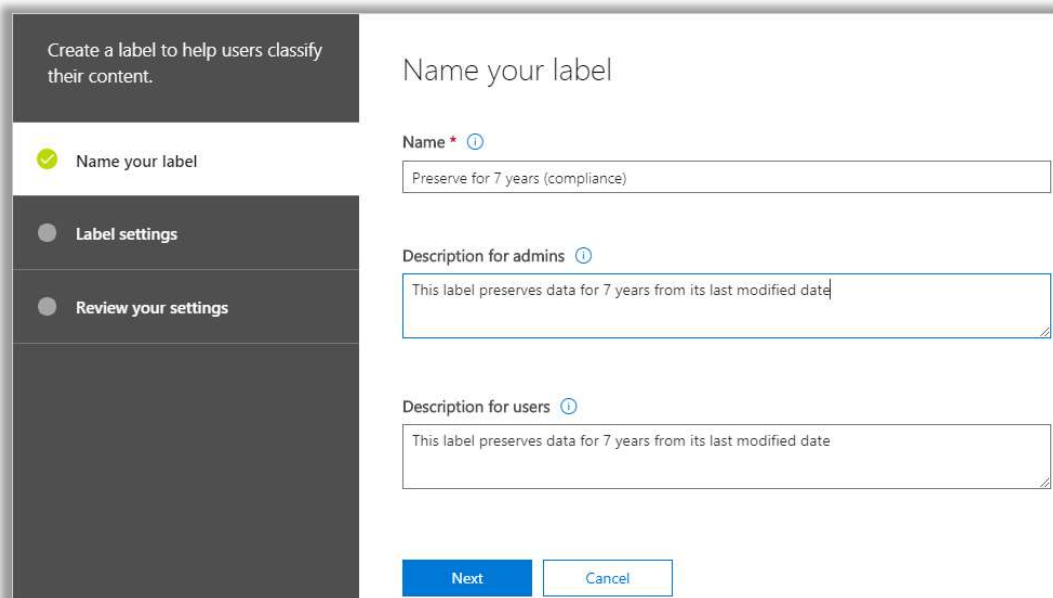
Now assume that you have a global policy that calls for retaining data and then deleting it after a specified date has elapsed. However, it is sometimes necessary to keep certain emails or documents beyond this period. For this, we will require more granular retention labels, which can be applied by end-users to content they wish to protect or handle in a way beyond the administratively set policies.

Again, whenever two labels are in conflict, preservation always wins, so keep that in mind and educate the user base. This should go without saying, but know in advance what you want your labels to do, before you even begin this process.

From the **Security & Compliance Center**, find **Classifications > Labels**. Select **+Create a label**.



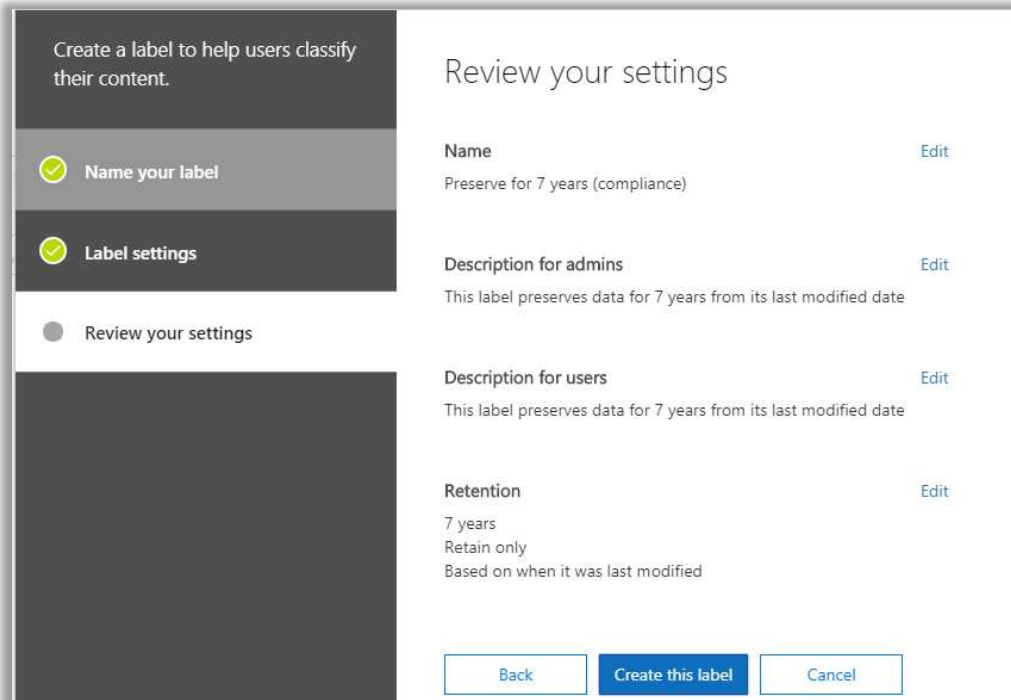
Give your label a name and description. **Next.**



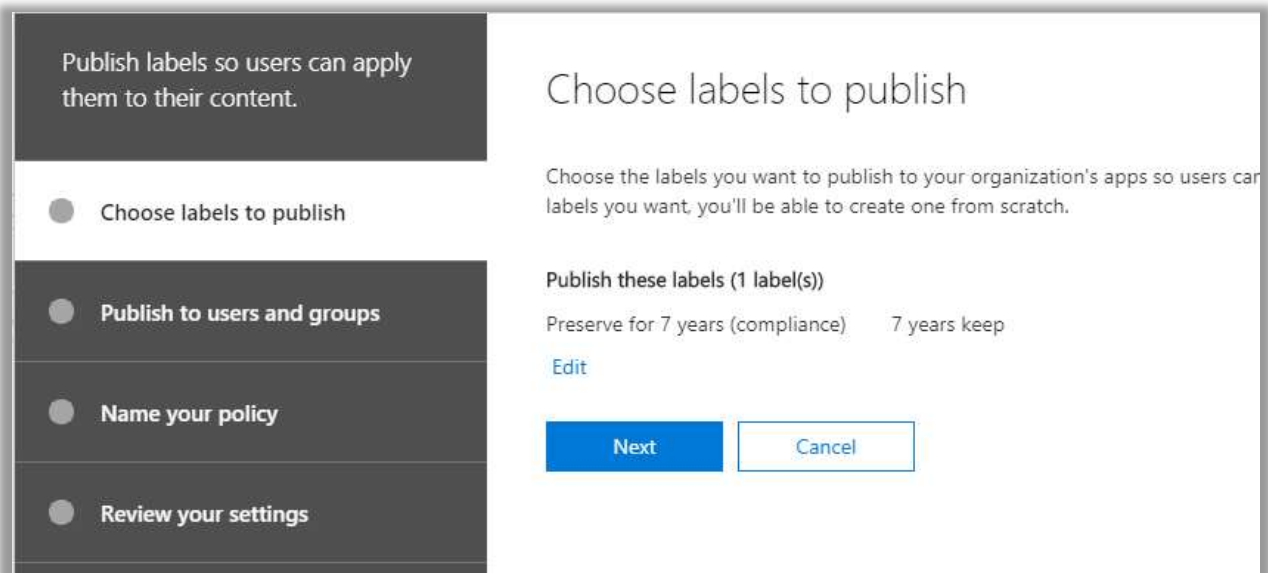
Turn **Retention** to **On**, and configure your settings. You can choose to apply the duration of the retention to *last modified date*, *creation date*, or *when it was labeled*. In this example we will use *last modified date*.

On this page you can also choose to label the content as a record, which makes it impossible for users to edit/change/delete the content, or to remove this label once it has been applied. Be careful when using this setting and labeling documents (I will leave it set to "off" in our example).

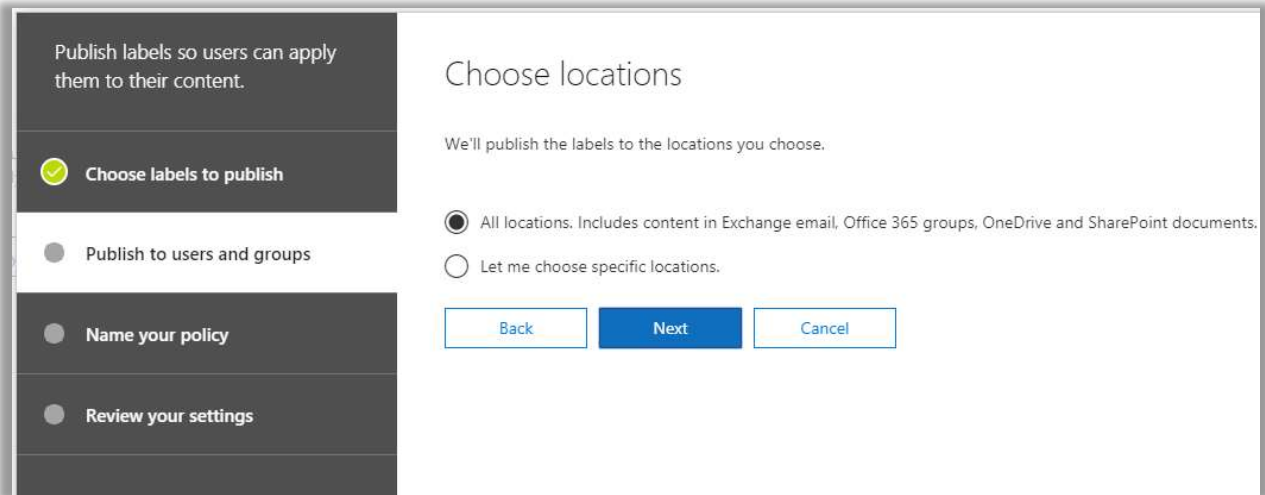
Now you can review and create the label.



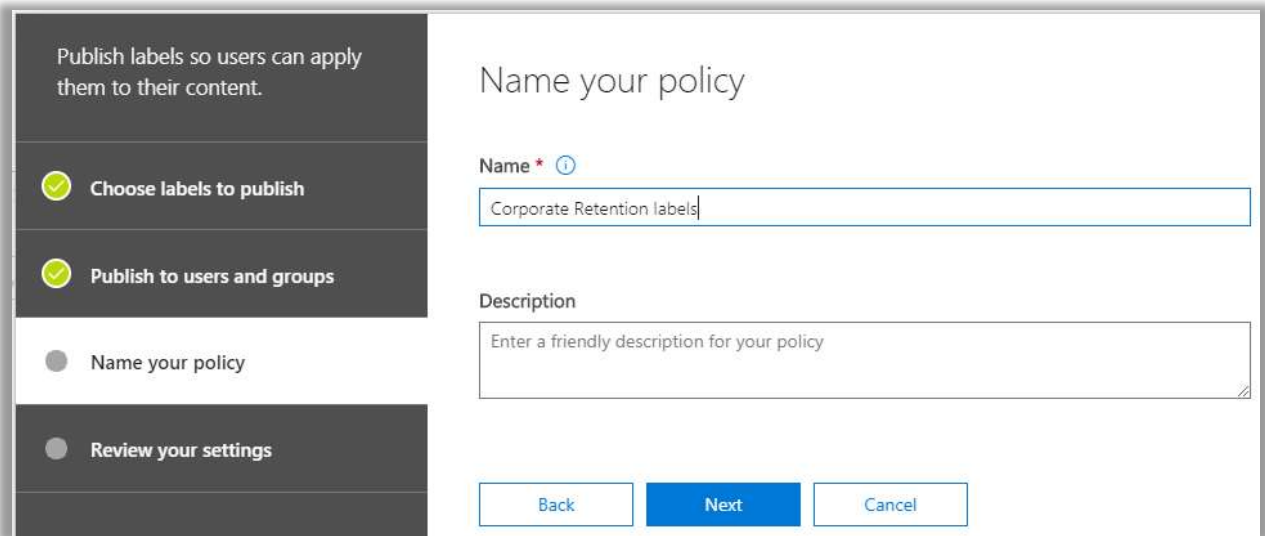
After all your labels are created, one more crucial step is *publishing*, which is the step that makes it possible for users to see the labels, and apply them.



You can have this label available everywhere in Office 365 or just specific apps such as Outlook.

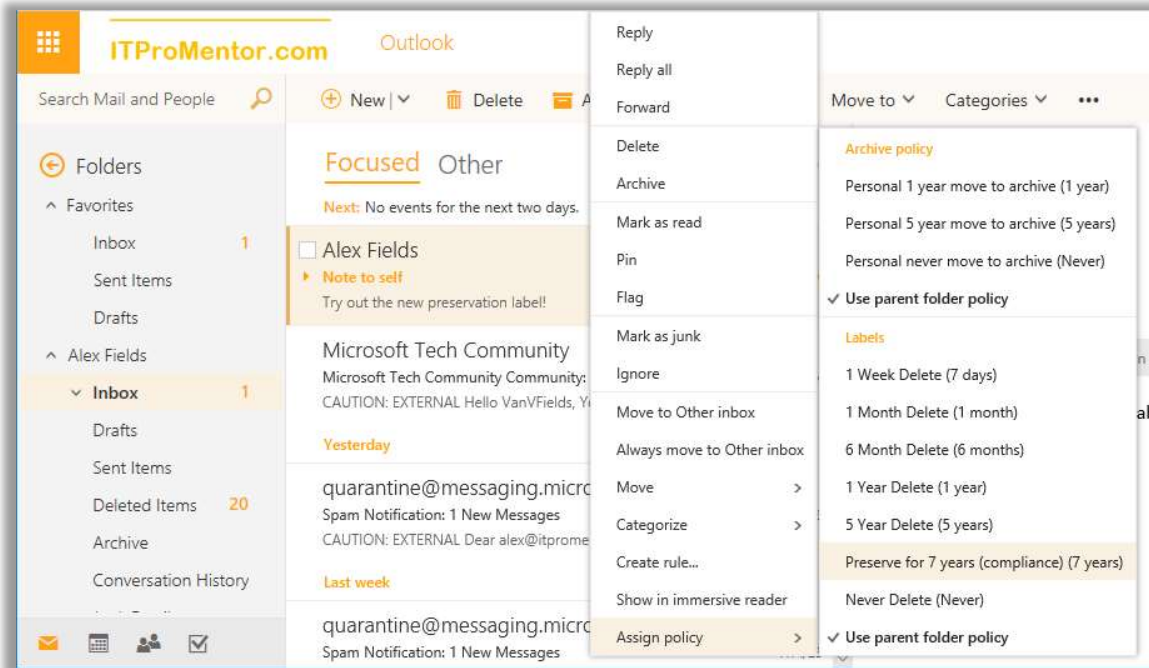


Name the label policy that you are publishing.



Go ahead and finish the wizard to publish the labels.

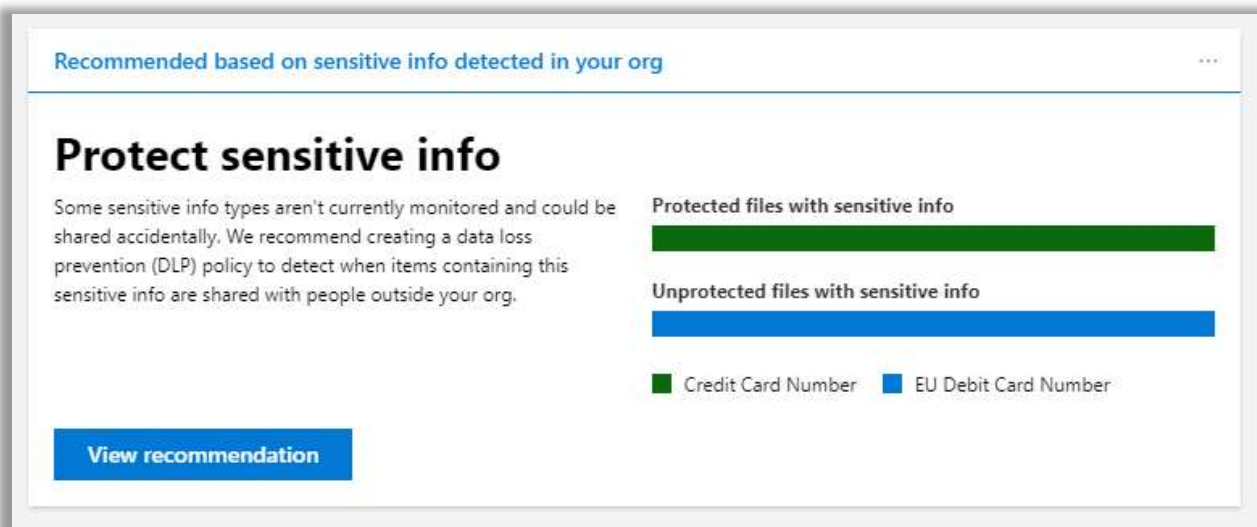
To see this label in action, let's check out an email message in Outlook.



My corporate retention *policy* will preserve and delete email data older than five years. But this *label* allows me to override the default, and apply preservation for seven years.

Configure Data Loss Prevention (DLP)

Data loss prevention (DLP) is a means for controlling sensitive data leakage, and/or recording incident reports when such leakage occurs. If your organization deals with certain types of data, like the Personally Identifiable Information (PII) prevalent in the health or financial services industry (social security numbers and the like), then the DLP templates would allow you to target data patterns that “look like” these sensitive information types.



Some capabilities that we have when sensitive information is detected is as follows:

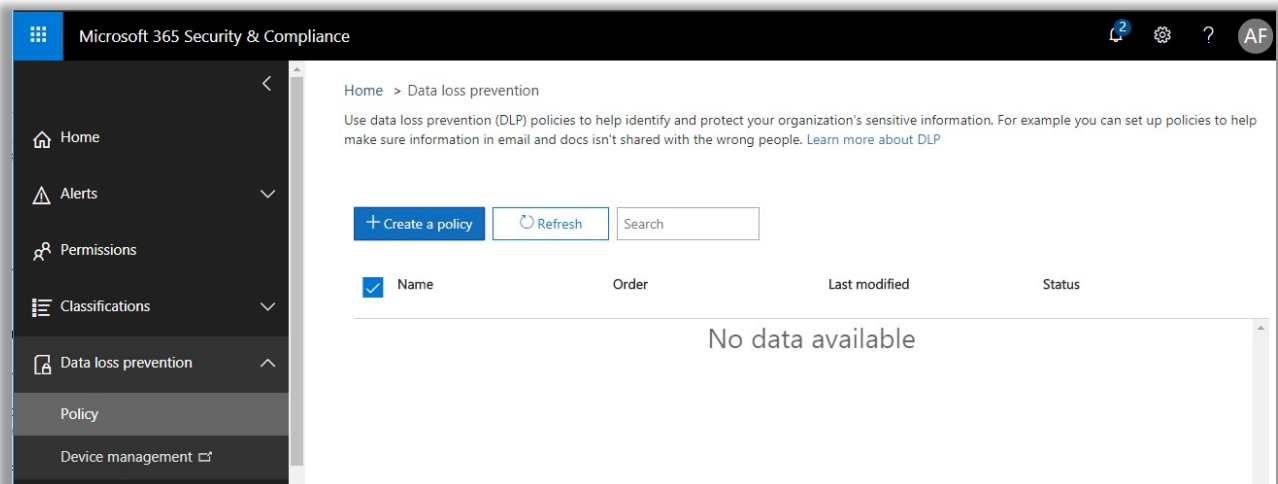
- **Encrypt** – automatically encrypt the content (applies to email messages only)
- **Block** – do not allow the content to be shared or sent externally
 - Optionally allow override of the policy with business justification
- **Notify** – Notify users and/or admins when something is being shared externally, using Policy Tips (informational banners that appear within the application) and email notifications
- **File an incident report** – email an incident report to another mailbox when sensitive content is shared externally
 - The incident report can optionally include the original content that was shared

You can choose any of these options individually (e.g. only file an incident report), or combine them—for instance, encrypt *and* file an incident report.

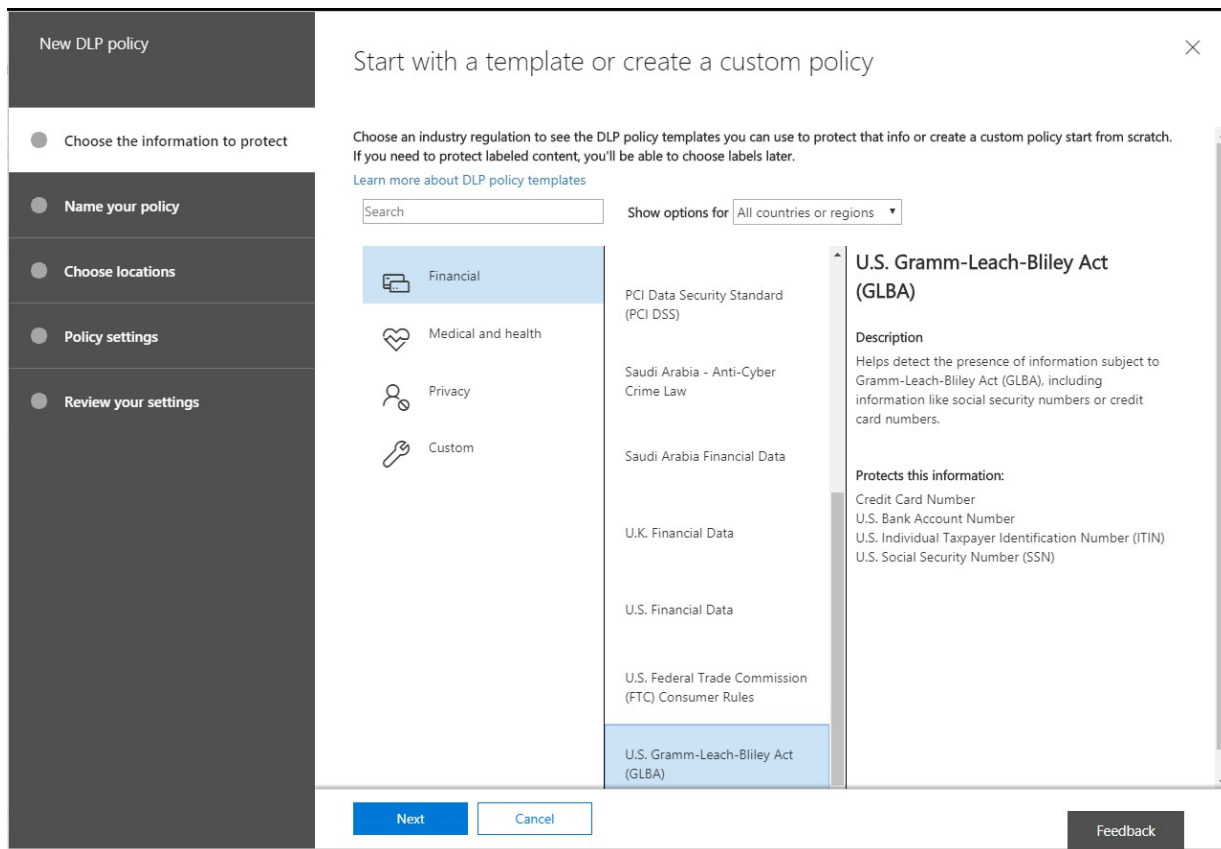
I am going to demonstrate some of these capabilities with examples that apply to data types which are specific to the U.S. (where I live), but Microsoft has templates for many different countries and regulations, including the European Union’s General Data Protection Regulation (GDPR).

Example 1. GLBA: Auto-encrypt email content

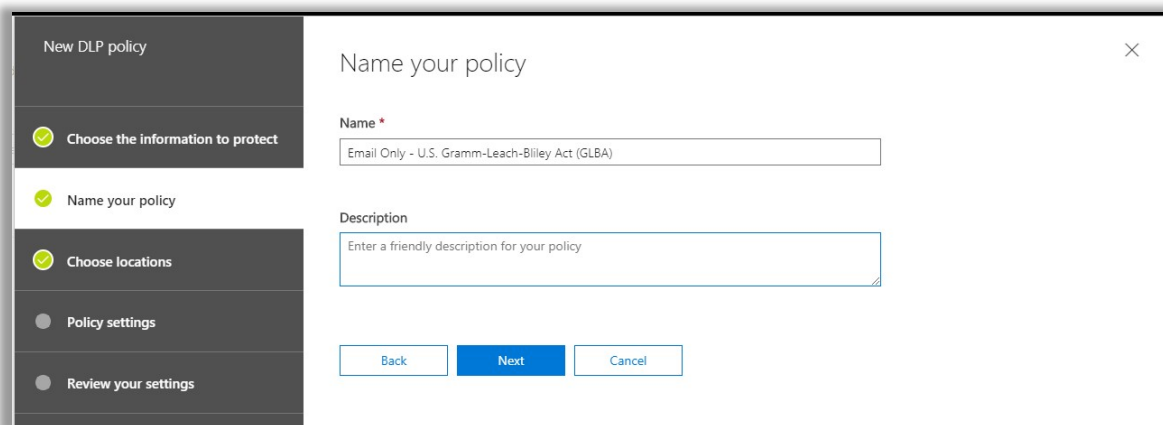
Under the **Data loss prevention** menu item on the left, choose **Policy**. Click **+ Create a policy**.



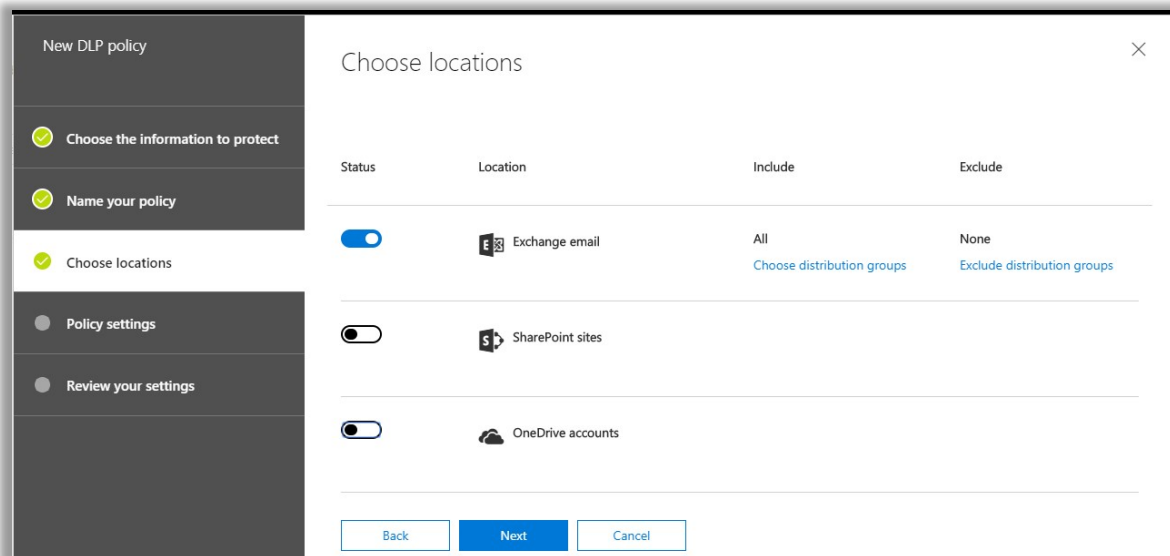
In this example, we will choose a policy template from the U.S. financial industry, called the U.S. Gramm-Leach-Bliley Act (GLBA). This policy template watches for credit card numbers, U.S. bank account numbers, and U.S. tax payer identification numbers, including ITIN and SSN.



Now I am going to name my policy. Note that I want this to be a descriptive name for what the policy does, or what it applies to. In this case, I plan to implement a policy which protects sharing this type of information, specifically over email communication. I'll name it *"Email Only – U.S. Gramm-Leach-Bliley Act."*



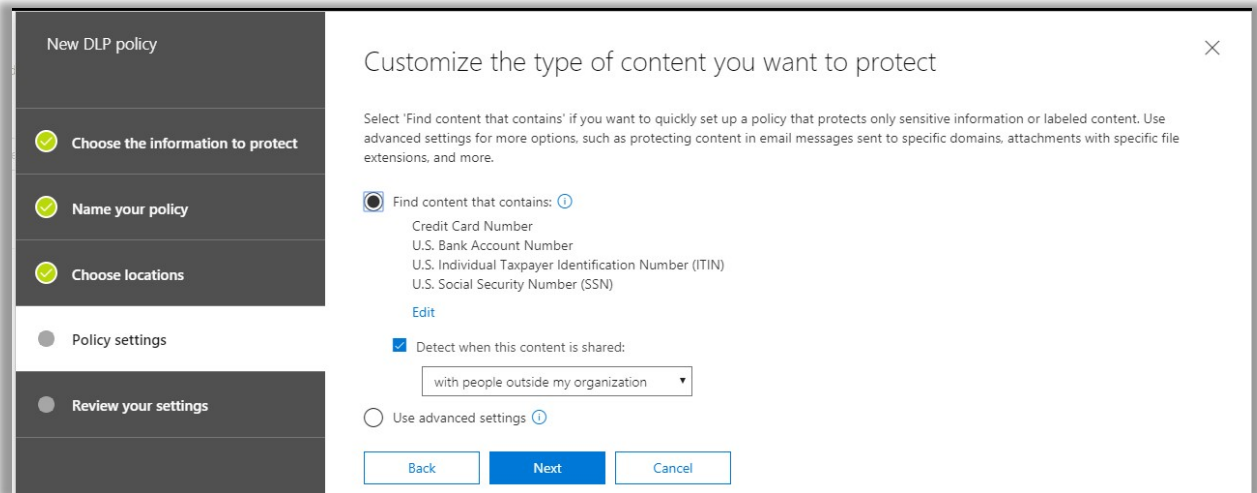
In choosing locations, I am going to select only **Exchange email**. As of now, this is the only location supported for auto-encryption with DLP.



Next to the first **Policy settings** page; here we begin to dial in the particulars—I will not use any advanced settings in this example. In this case I want to detect when the content is being shared **with people outside my organization**. DLP is usually targeted this way in the SMB, rather than sharing content internally.

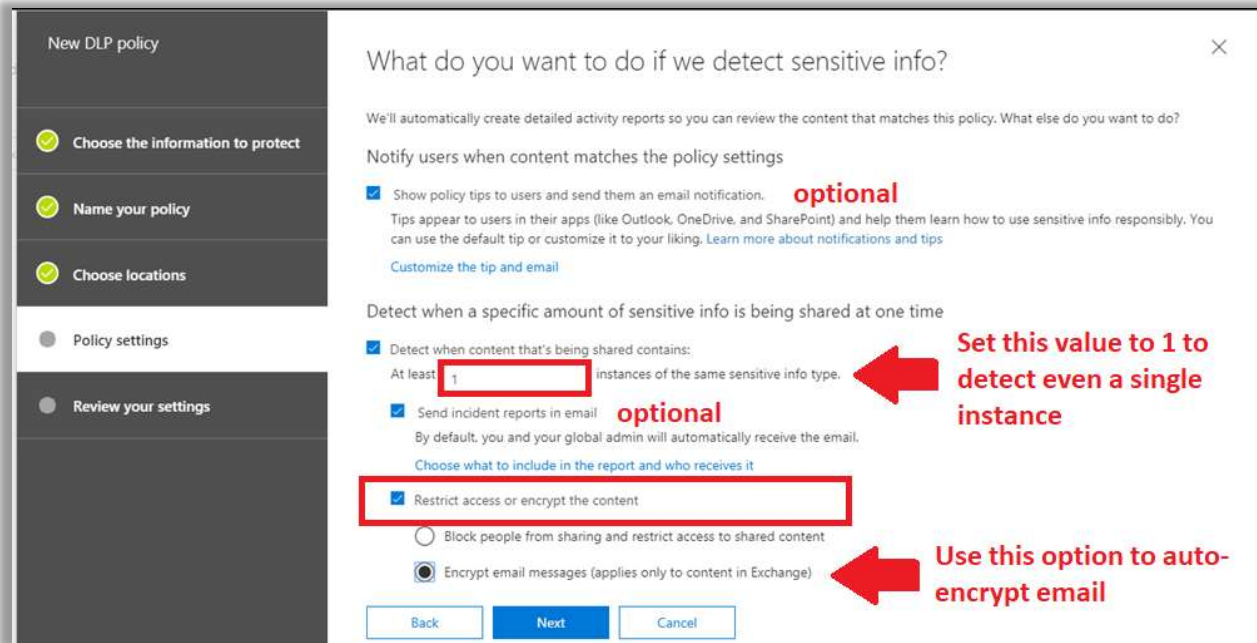
Since email communications within an organization never really leave the 365-hosted Exchange server, there aren't as many risks for data that is in-transit. Whereas, when the recipients are external to the organization, that content must be transported over the internet, which is a much riskier business, particularly if the recipient organization is still using SMTP over port 25 (unencrypted).

NOTE: by default, Office 365 will always attempt to send the mail via TLS on port 587 and fall back to port 25 if the recipient server does not support TLS. Email encryption however, will not transport the message externally at all—but rather require the recipient to sign-in at Microsoft, to view the message.



On the next **Policy settings** page, you can configure several options.

1. **Policy tips** and email notifications to end-users: I will include this option here (with some custom text) for demonstration purposes, but it is up to you whether or not to include.
2. Specify the **number of instances** of sensitive content that have to be detected before applying the policy actions. I usually always set this value to **1**, so that even a single instance of an SSN for example, would trigger the policy actions.
3. **Incident report** is also *optional—I will cover another example later, where we customize the policy a little further. I am going to use **Encrypt email messages**—meaning that content matching this information type will have Office Message Encryption automatically applied on its way out the door.
4. **Restrict access or encrypt the content** – this is the option you want to focus on here; in my example, our intention is not to block this communication, but rather *encrypt* it.



Notice that it is also possible to customize policy tips and email notifications, by selecting the link above to **Customize the tip and email**. Here you would also choose just exactly *who* is notified.

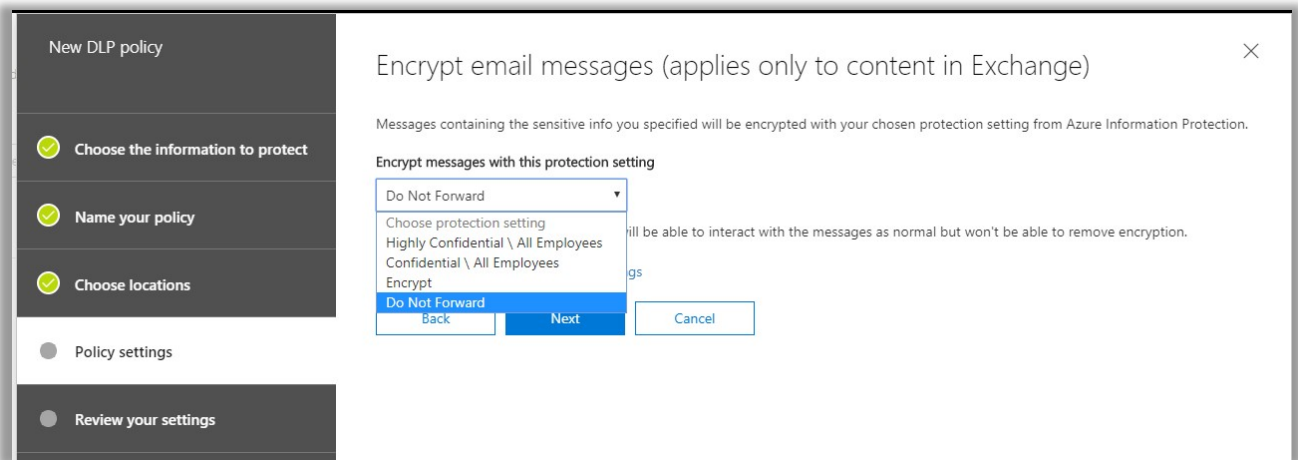
**Pro tip: I like to set up a compliance management mailbox in Exchange Online, so that it can collect a running record of incident reports. This can be as simple as a shared mailbox, with permissions assigned to whomever is the compliance officer within the organization. We'll cover this in more detail in the next example.*

Click **Next**. Remember that we were choosing to encrypt the email messages, so you have to choose which encryption template to apply. It is not possible to share encrypted content marked as *Confidential* or *Highly Confidential* with recipients outside of the organization. Therefore, you have two remaining options: *Encrypt* or *Do Not Forward*.

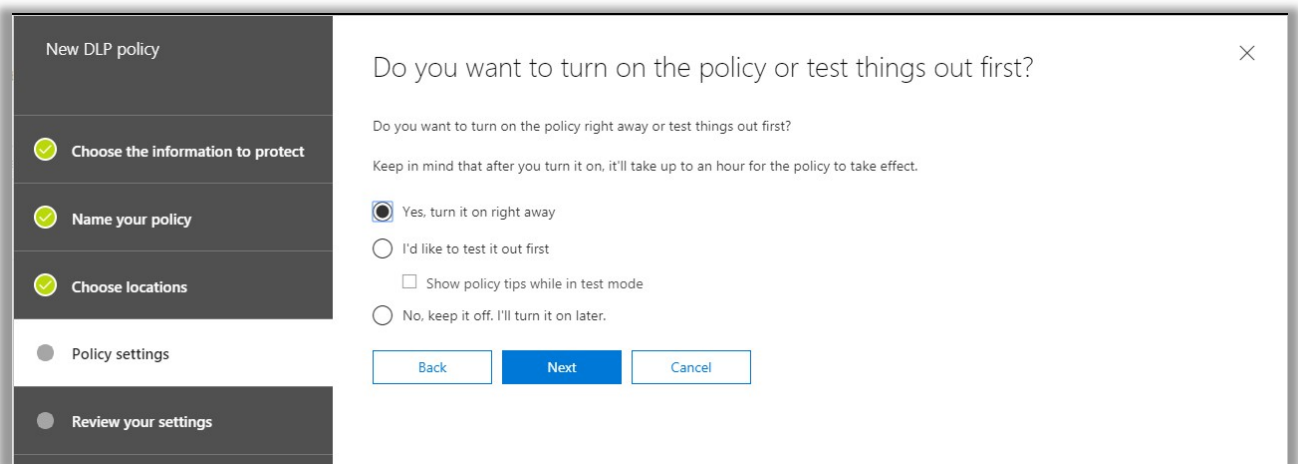
Encrypt: The *Encrypt* option is the weaker of these two—it will simply encrypt the message contents, meaning that a recipient will need to sign-in to view the email message via Outlook on the Web. In this case, it is still possible to forward and/or copy/export any content within the message.

Do Not Forward: The stronger encryption option is *Do Not Forward*. With this setting, you are saying, "I want to share this with you, but I don't want you to share it with anyone else."

Recipients will be able to sign in and view the message, but they will find it very difficult to get any of that information shared beyond themselves (however, they can still *reply* to the sender).

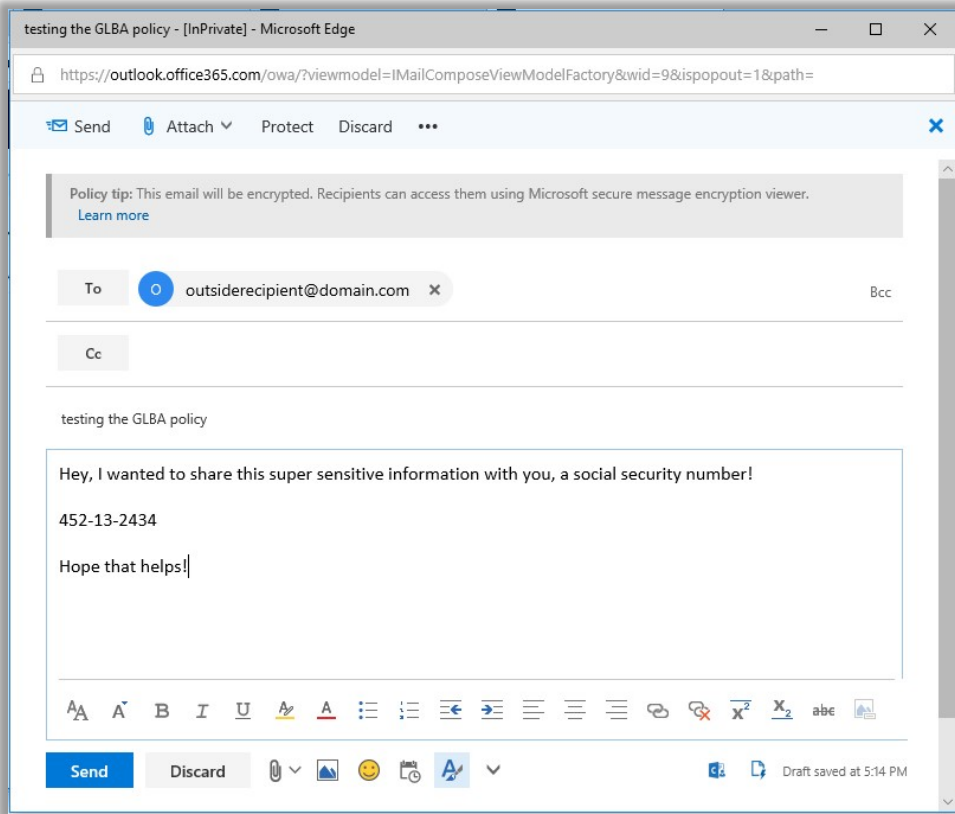


Proceeding to the last step, you will find that it is possible to test the policy first, and you can choose whether policy tips “show up” or not while doing this. Otherwise, it basically has the same effect as just turning it on (you just get the option to disable policy tips in test mode—that seems to be the only functional difference).

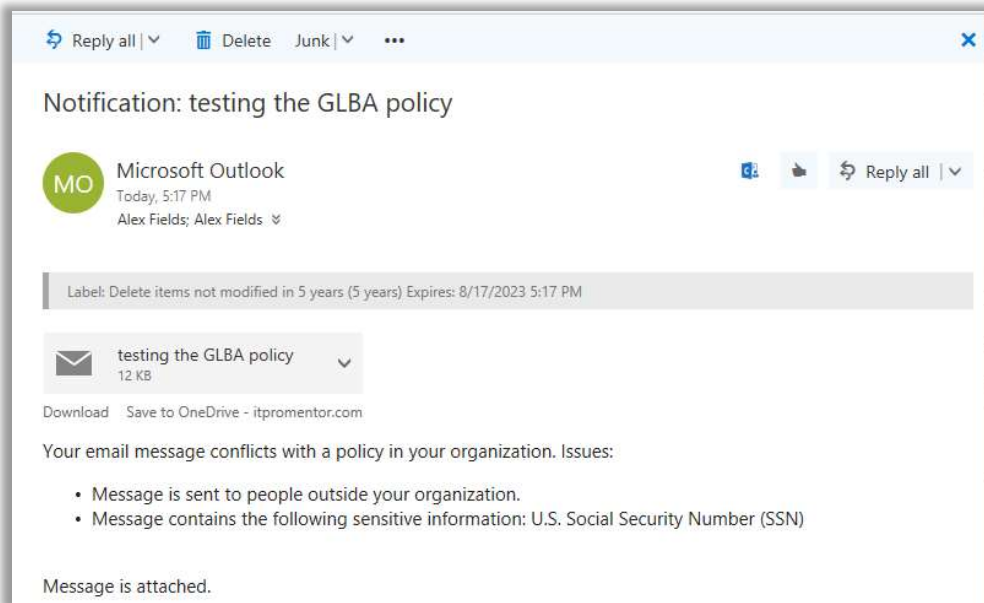


Finally, you can proceed to review your settings and **Create** the policy to finish.

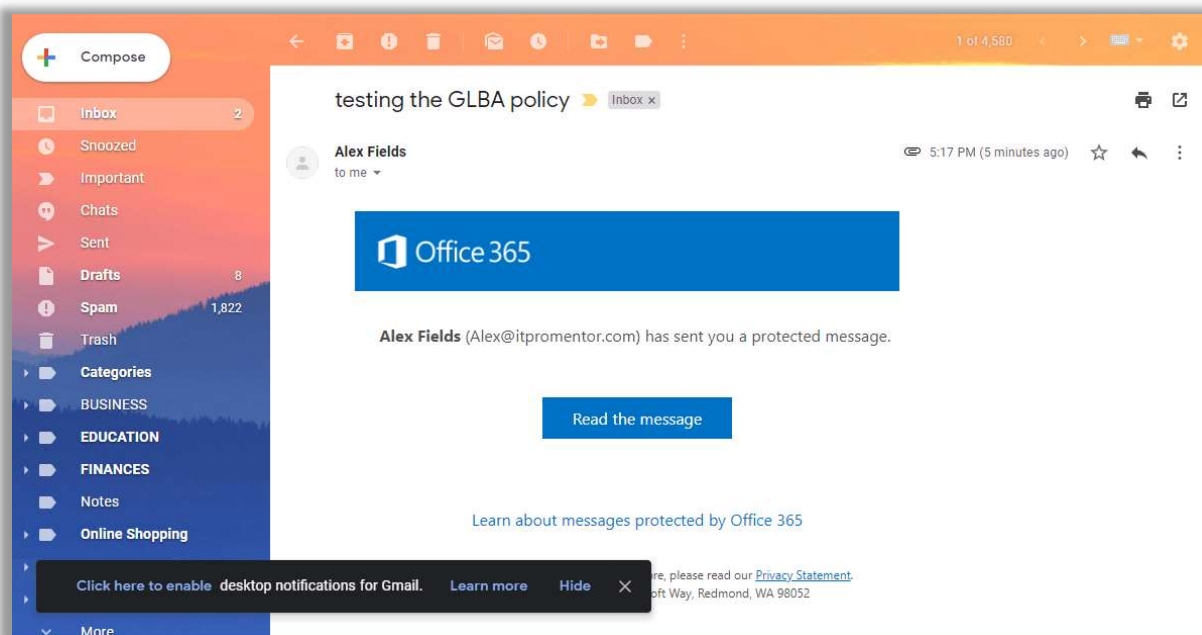
When an end-user drafts an email message or attaches a file containing sensitive content, a Policy Tip will appear in Outlook or Outlook Web Access, telling the recipient that this message will be encrypted:



If you had selected the option to notify the person sharing the content, then they would also receive an email after sending that looks like this:



The recipient experience, in this case, is determined by the fact that we chose to *encrypt* the message. That means they will not receive the actual message contents, but rather a link that will lead them to a Microsoft sign-in page.



This is the same experience described with setting up email encryption using Azure Information Protection—the recipient will be logging into Microsoft’s Outlook on the Web, using either their public email identity (for example, a Gmail account as in the example above), or a Microsoft account. Therefore the message never really leaves the Office 365 environment.

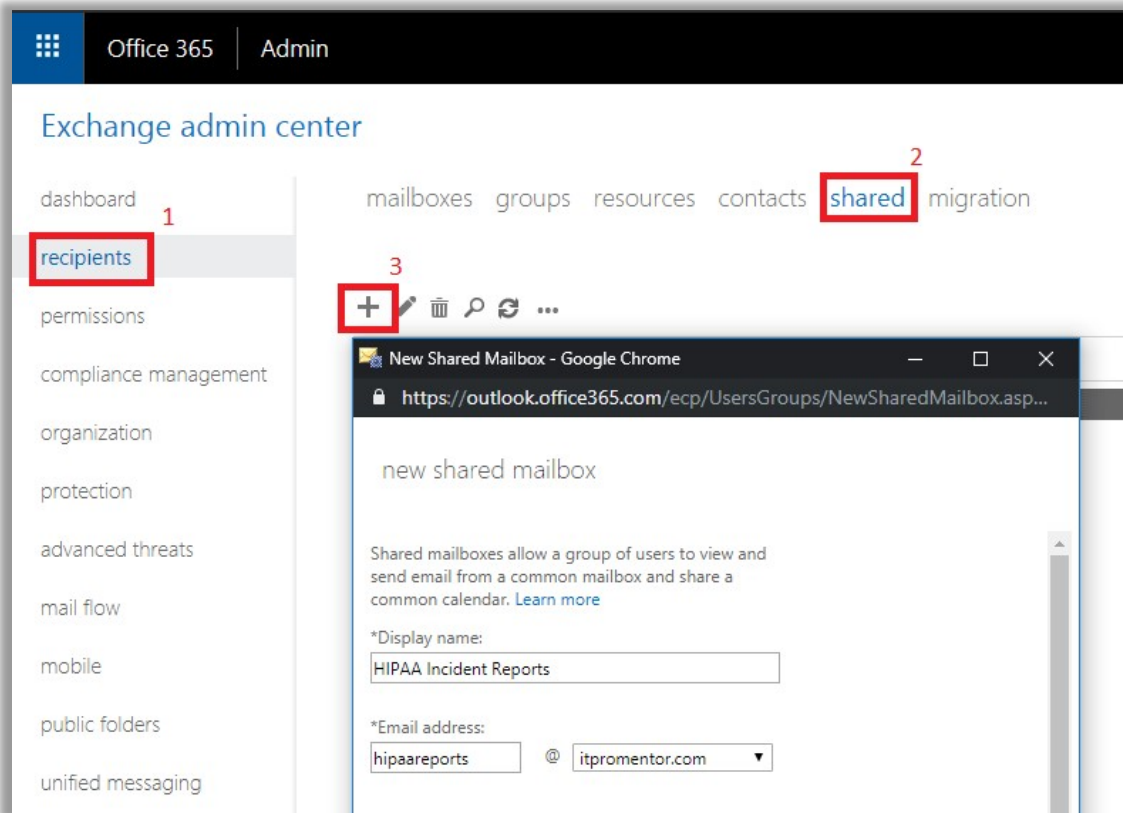
Example 2. HIPAA: File an incident report

Service providers in the U.S. medical industry, and their associates, can be subject to HIPAA laws (Health Insurance Portability and Accountability Act). Usually this means that allowing electronic Protected Health Information (ePHI) outside of the organization (“Covered Entity” in HIPAA language) should be avoided. However, this type of information sharing is sometimes unavoidable and even necessary in the course of normal business—especially with regards to certain vendors and partner organizations with whom the covered entity has a Business Associate Agreement (BAA).

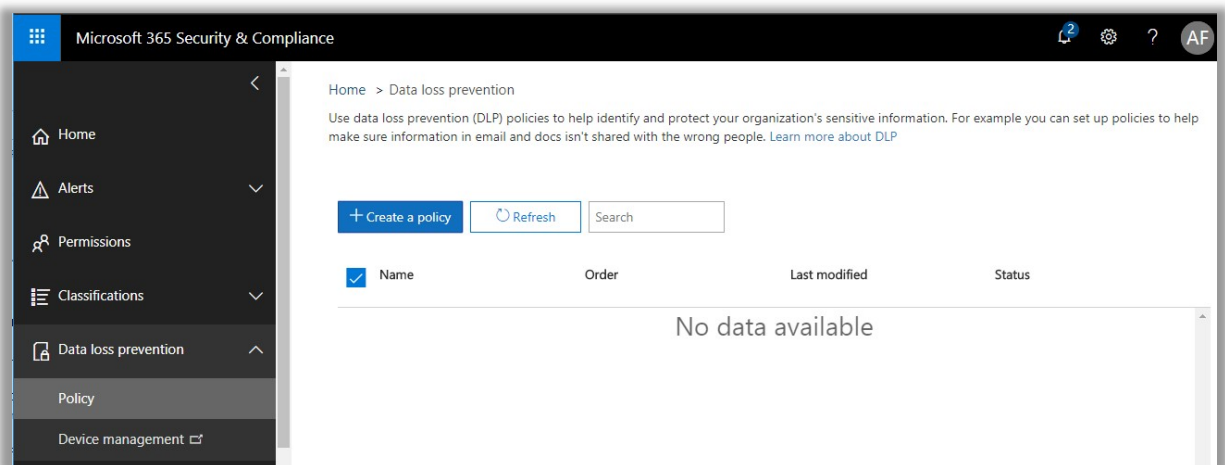
Still, whenever ePHI is shared externally, whether by accident or in the normal course of business, according to HIPAA, there needs to be an incident report kept on file by the Covered Entity. We can automate this filing using a simple shared mailbox and a DLP policy, which will deposit any detected incidents into an email report.

First, create a shared mailbox in Exchange Online, and give it a descriptive name such as “HIPAA Incident Reports.” Go to **recipients > shared > New Shared Mailbox (+)**. From here, fill in the

Display name, email address, and grant access to at least one user (often the designated HIPAA officer). Click **Save** after making your selections.

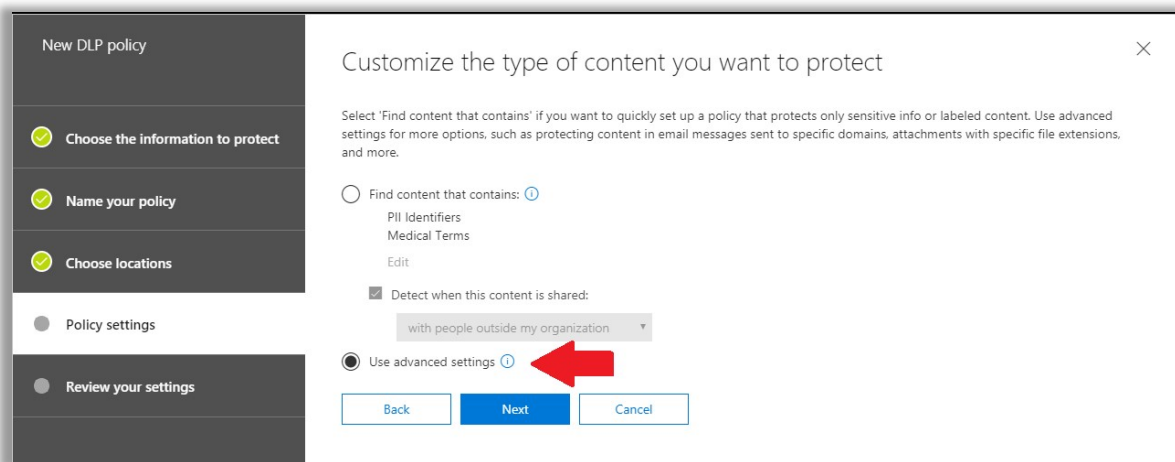


From the **Security & Compliance** center, go to **Data loss prevention > Policy**. Choose **Create a policy**.

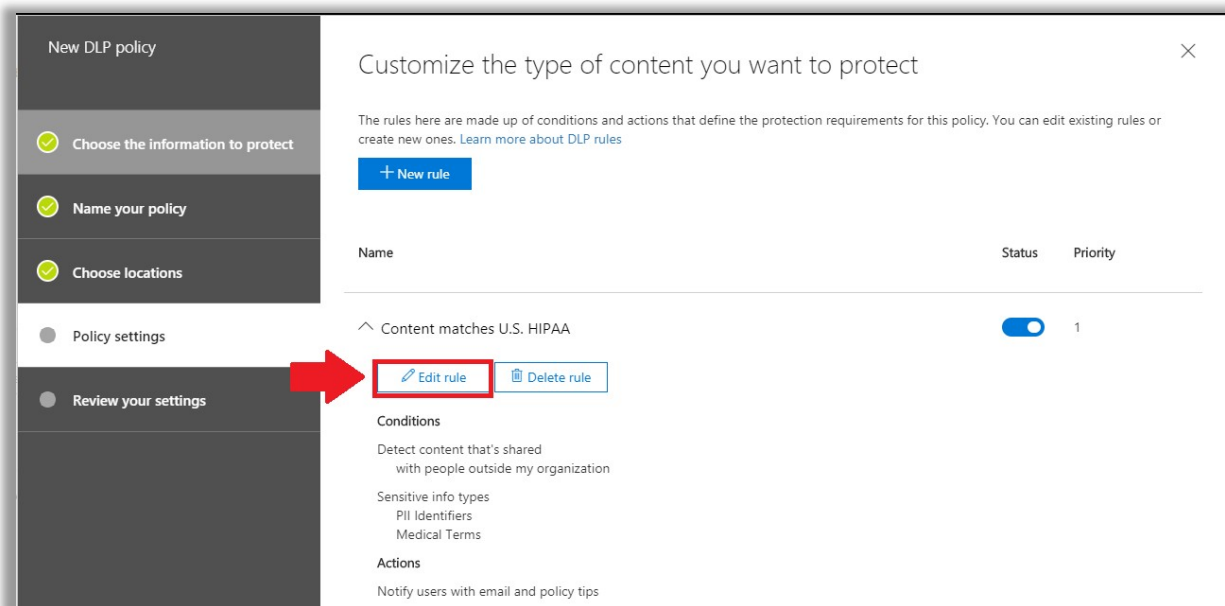


As you step through these screens, give your policy a descriptive name. I will choose to protect **All locations in Office 365** (e.g. SharePoint libraries/Teams sites also) in this example.

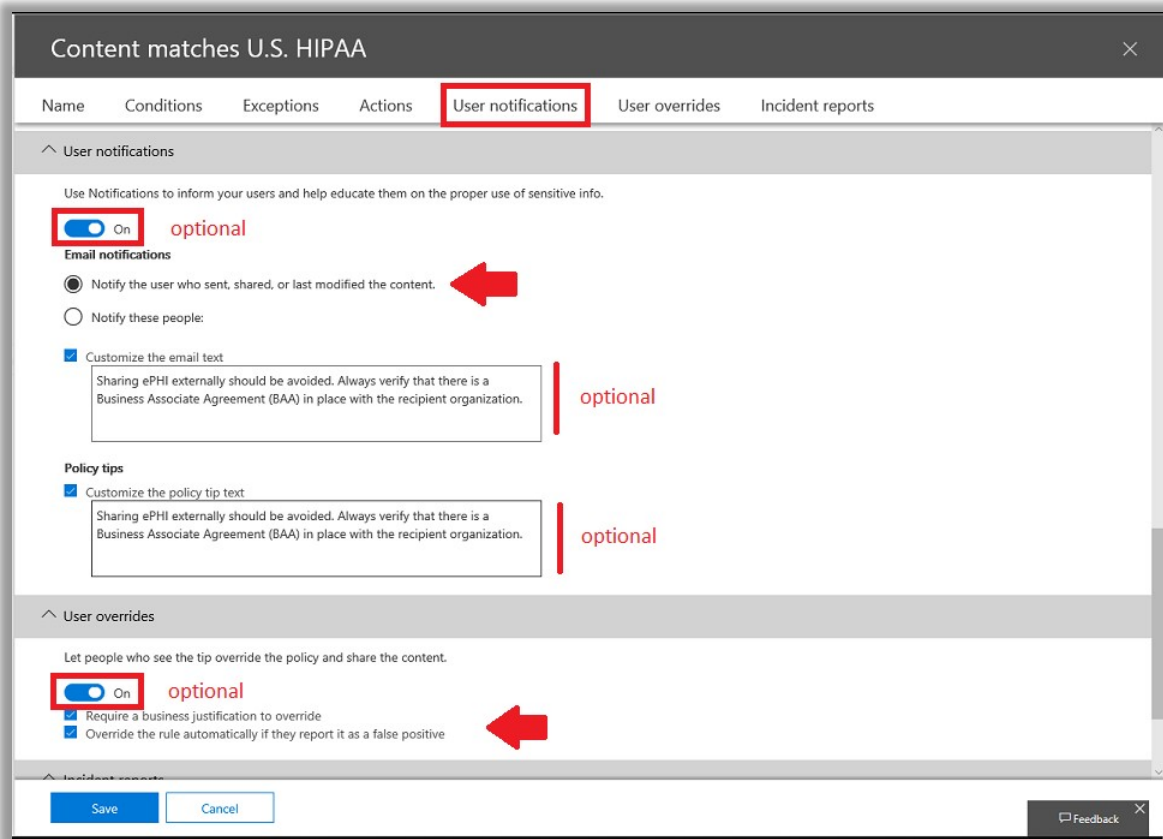
Next you will want to be sure to choose the **Use advanced settings** option, so that we can edit things more to our liking.



Expand **Content that matches U.S. HIPAA**, and choose the option to **Edit rule**.



Optionally: Under **User notifications**, you can notify end-users and give them an opportunity to provide business justification or identify false positives. The “override” piece is useful when policies are designed to *block* sharing—which is configured under **Actions**. But we’re not concerned with that here—we just want incident reports. Don’t worry about the override option in this example, then, because we’ll leave it turned off in this instance. I do want you to be aware, however, that these things are also in your menu of options when deploying DLP. For example, I have also written some custom text for the end-user notifications and policy tips.



Next (and most importantly) configure **Incident reports**. Switch the setting to **On**, and be sure to edit the recipients using **Add or remove people**. Be sure to add your newly configured *HIPAA Reports* shared mailbox.

You will also notice there are options here for whether to include the content that was shared along with the incident report—this may or may not be advisable depending on how you handle incident reports. For instance, you may only need to show *that* an incident was recorded, and not *what* the explicit content actually was. I recommend consulting with an attorney who represents your organization and is versed in HIPAA. **Save** the settings when you are done.

Content matches U.S. HIPAA

Name Conditions Exceptions Actions User notifications User overrides **Incident reports**

^ User overrides

Let people who see the tip override the policy and share the content.

On

Require a business justification to override

Override the rule automatically if they report it as a false positive

^ Incident reports

Use this severity level in admin alerts and reports:

Medium ▾

Use email incident reports to notify you when a policy match occurs.

On

Send notifications to these people

hipaareports@itpromentor.com

[Add or remove people](#) **be sure to edit the recipients using Add or remove people**

All incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered.

You can also include the following information in the report:

- The name of the person who last modified the content
- The types of sensitive content that matched the rule
- The rule's severity level
- The content that matched the rule, including the surrounding text
- The item containing the content that matched the rule

Save Cancel Feedback

Finally, you can say **Yes, turn it on right away**, then **Next** and **Create** on the final screen, to finish the wizard, and after reviewing your choices. This can take some time to take effect. Sometimes it's fast, other times I have waited for more than hour.

New DLP policy

Do you want to turn on the policy or test things out first?

Do you want to turn on the policy right away or test things out first?

Keep in mind that after you turn it on, it'll take up to an hour for the policy to take effect.

Yes, turn it on right away **be sure to edit the recipients using Add or remove people**

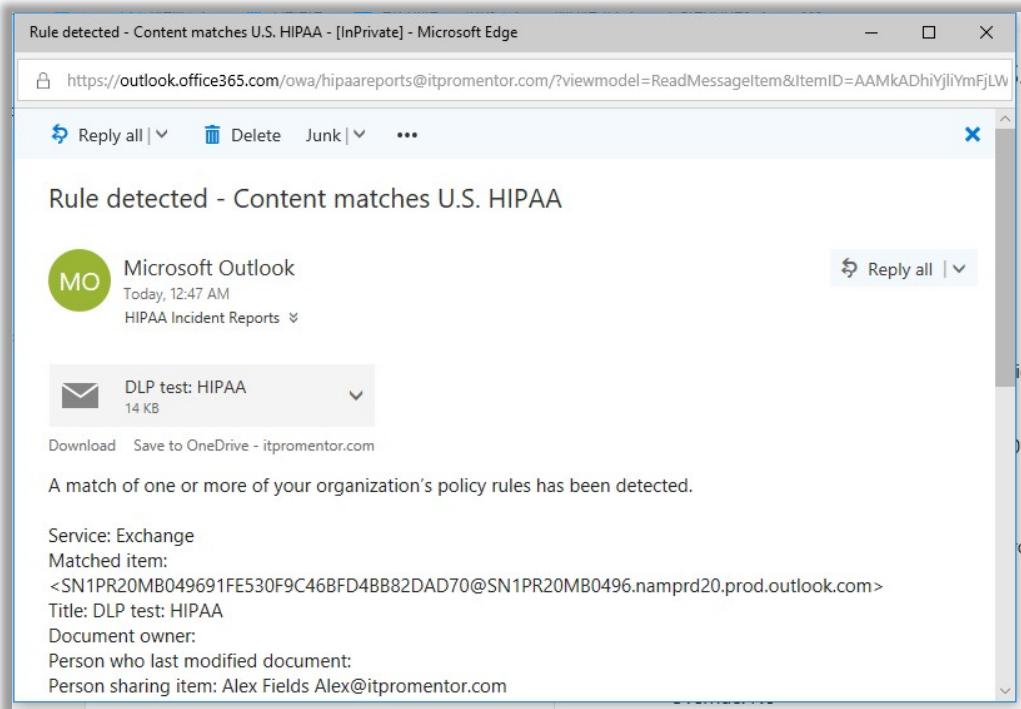
I'd like to test it out first

Show policy tips while in test mode

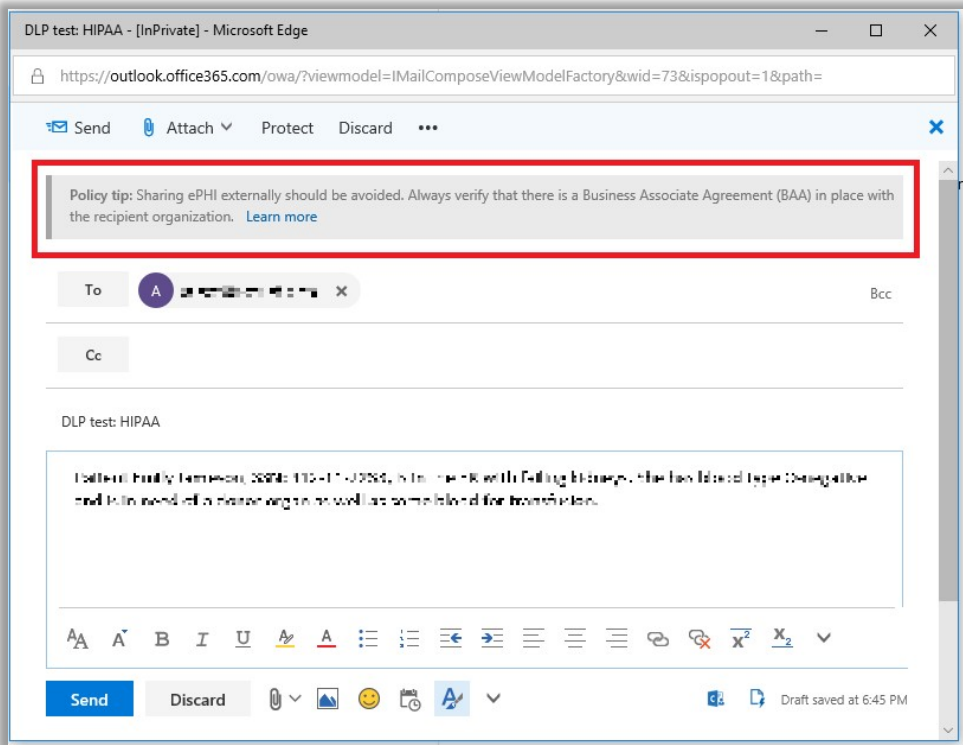
No, keep it off. I'll turn it on later.

Back Next Cancel

The result of this policy is that any detected Personally Identifiable Information (PII) that is used in connection with known Medical Terms will generate an incident report that is filed in our shared mailbox. If ever auditors (or litigators) want to see your incident reports, you can simply do an export of this mailbox to PST. See below an example of one of the messages in the incident reports mailbox.



If you also had the user notifications turned on, then the individual sharing the content will see the custom alert text you entered, known as a *policy tip*. They'll also get an email, after sharing it.



Enable Advanced Threat Protection (ATP) policies

Advanced Threat Protection (ATP) includes the following policies which are configurable from **Threat Management > Policy**:

Safe Links – Hyperlinks which exist in email messages or other content in Office 365 are re-written into a new URL which includes a Microsoft “wrapper.” The Microsoft URL acts like a proxy, launching the links—and the links that are found within those links, and the links within *those* links—before sending your own web browser on to the “real” destination. This allows Microsoft to test out in advance if a website has “gone dark” or contains potentially bad content, before you get there.

WARNING: it is important to realize how this timing works—the scans are taking place literally at the time you click the link, not when the link was created or sent.

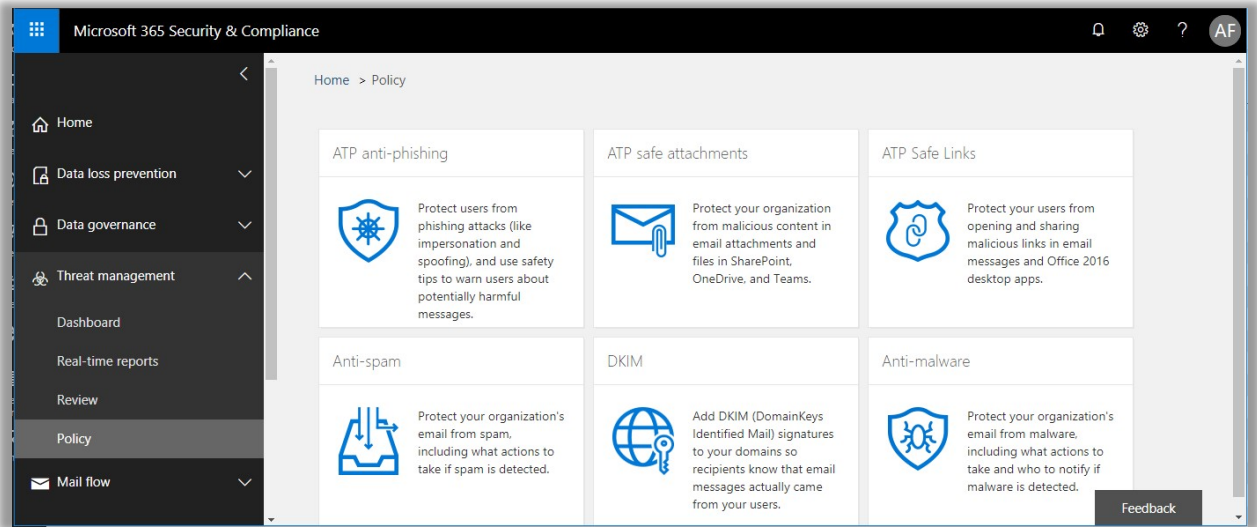
Safe Attachments – Safe attachments will essentially launch any downloadable attachment and execute it in a virtual machine (what they call ‘detonating’), before allowing it to go on to the end-user. This sandbox environment is looking for behaviors that are unusual or abnormal, and which could represent malware. This is beyond virus scanning—it is looking for zero-day threats—stuff without signatures.

WARNING: enabling this feature will cause noticeable delays in delivery of certain content/attachments. In some cases, I have seen some email messages delayed by up to 10 minutes.

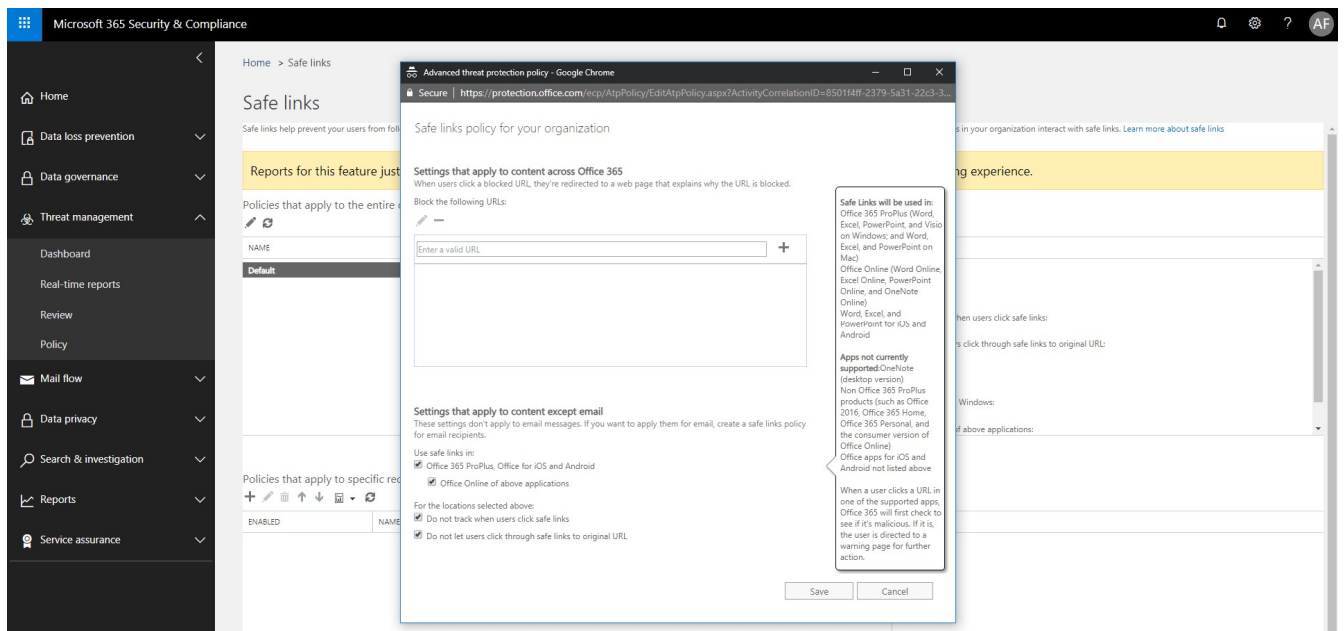
Anti-phishing – ATP anti-phishing policies allow you to put in place some anti-impersonation protections against specific mailboxes and domains. You can enable policy tips that would, for example, raise a user’s attention to the fact that a domain name contains unusual characters (e.g. a zero instead of the letter “O”), which is often exploited in certain attacks/spoof attempts. Furthermore, you can apply “Mailbox intelligence” which applies machine learning to the message exchange patterns between your users and their usual contacts. This helps Microsoft identify when a known contact sends a suspicious message, which may actually be an impersonator standing in the shoes of that contact. I know what you are thinking: SkyNet was just born.

Safe Links

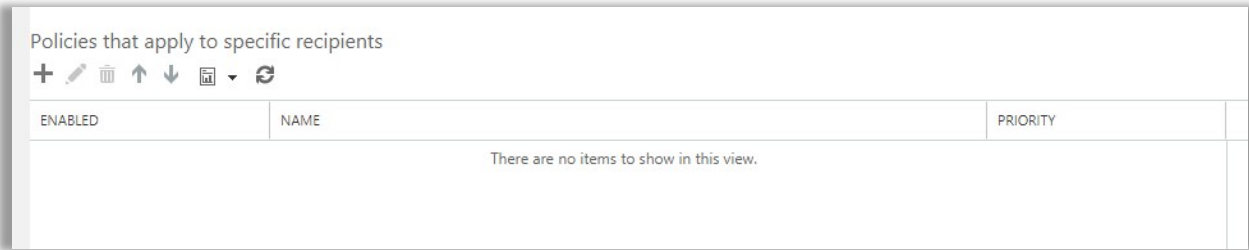
Navigate to the Security & Compliance Center > Threat Management > ATP Safe Links.



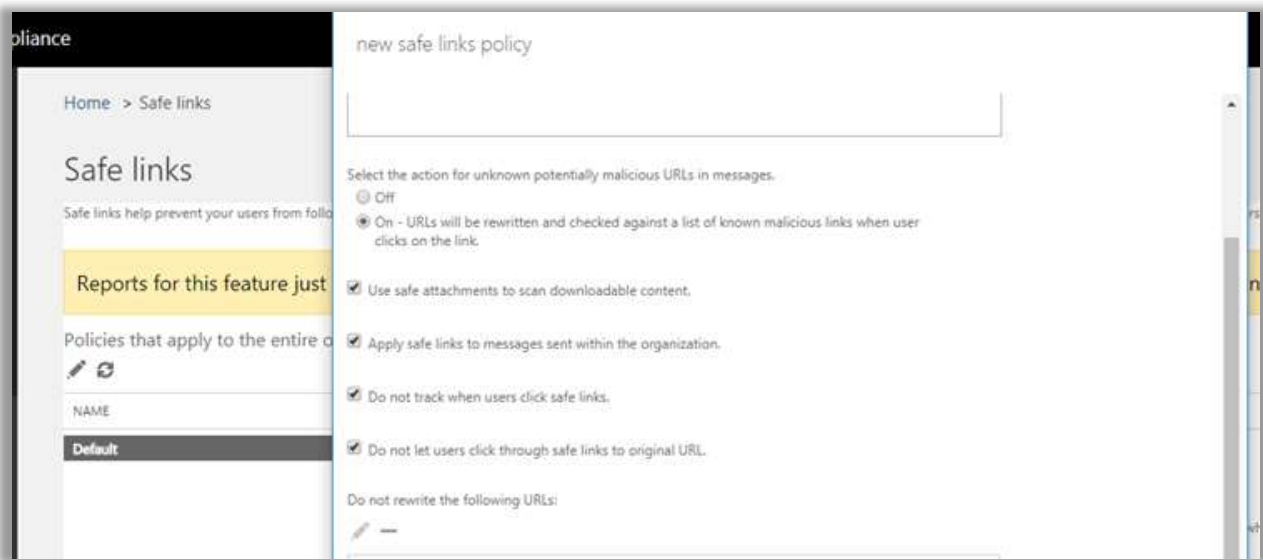
First edit the “organization wide” **Default** policy, from the first box up top. You can choose your own level of involvement here, and outright block specific URLs if you like. Otherwise, you can choose to enable it for Office 365 Pro Plus, Office for iOS and Android, and optionally Office Online apps. Last, you do not have to track the clicks if you don’t want to (I don’t, typically), or to allow users to click through to the destination from a warning page when a problem is detected. **Save** the policy.



Then it is also possible to scroll down and add (+) a new policy that applies to specific recipients/domains.

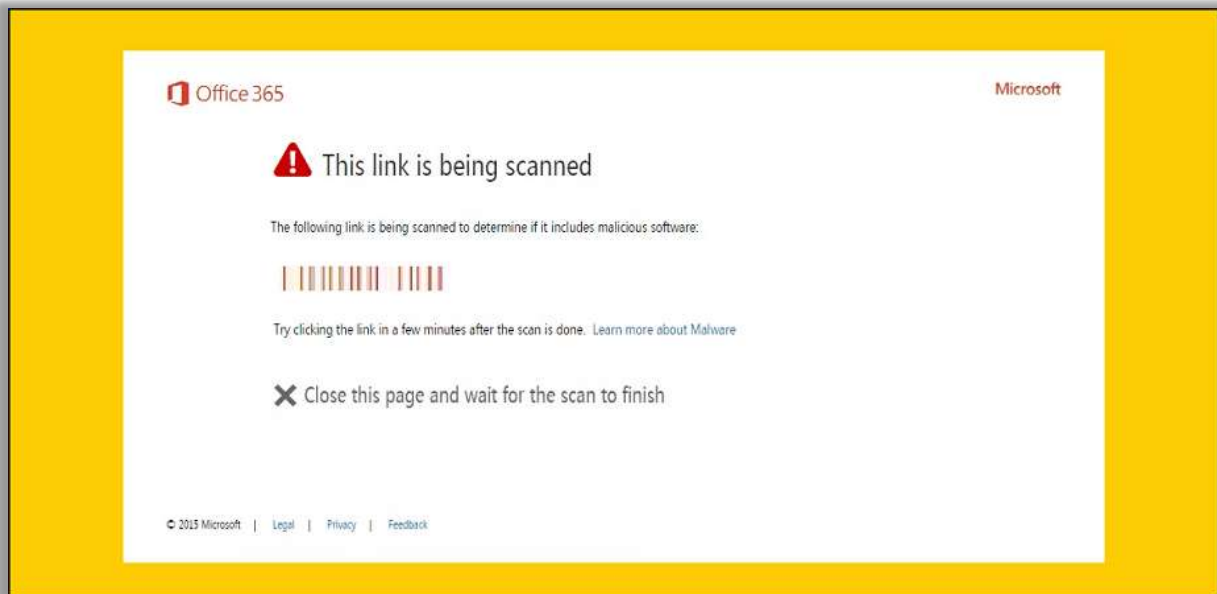


Normally you would select *On* to re-write URLs for incoming messages. I also enable the safe attachment scanning (*Use safe attachments to scan downloadable content*), even though we did set a policy up for attachments on messages, this would apply the safe attachments sandbox detonation to “downloadable content” which are coming from the safe links.

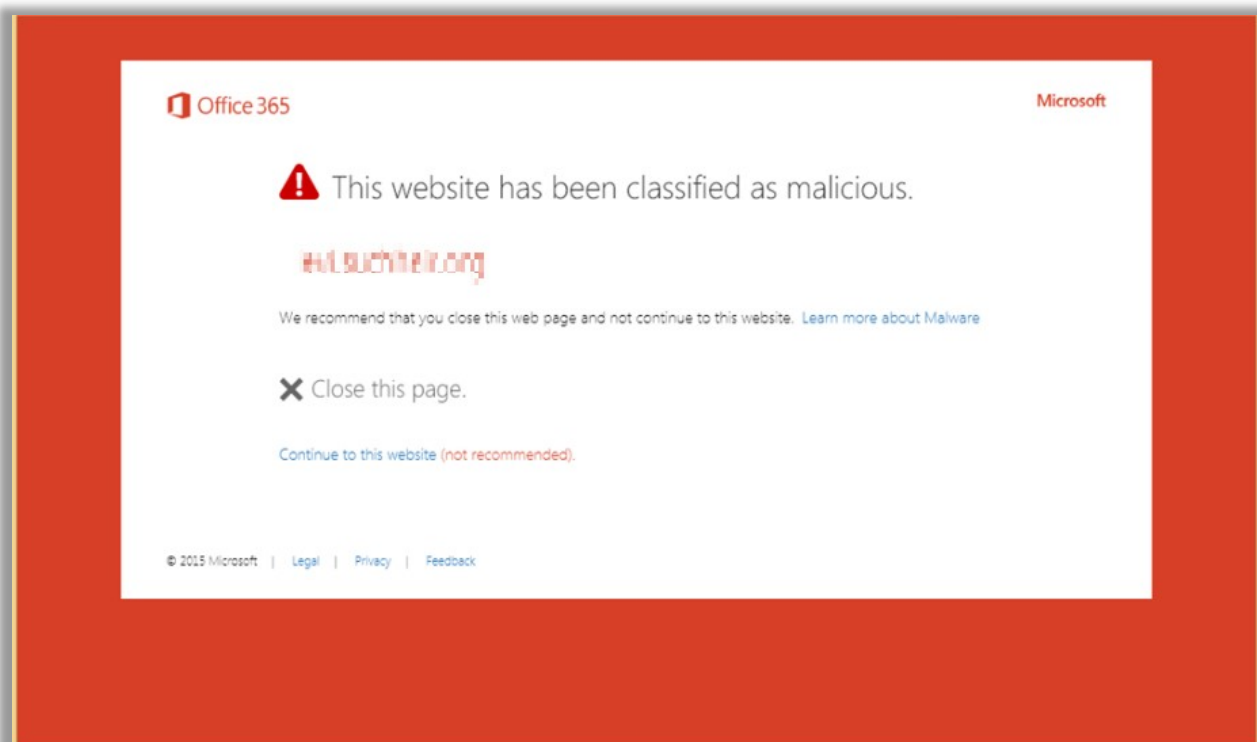


I usually apply this policy to the entire domain, but you can also use group membership, etc. **Save** after making your selections.

In some cases, the scanning may take longer than usual, and the end-user could be presented with this warning page, with an option to click through to the website.

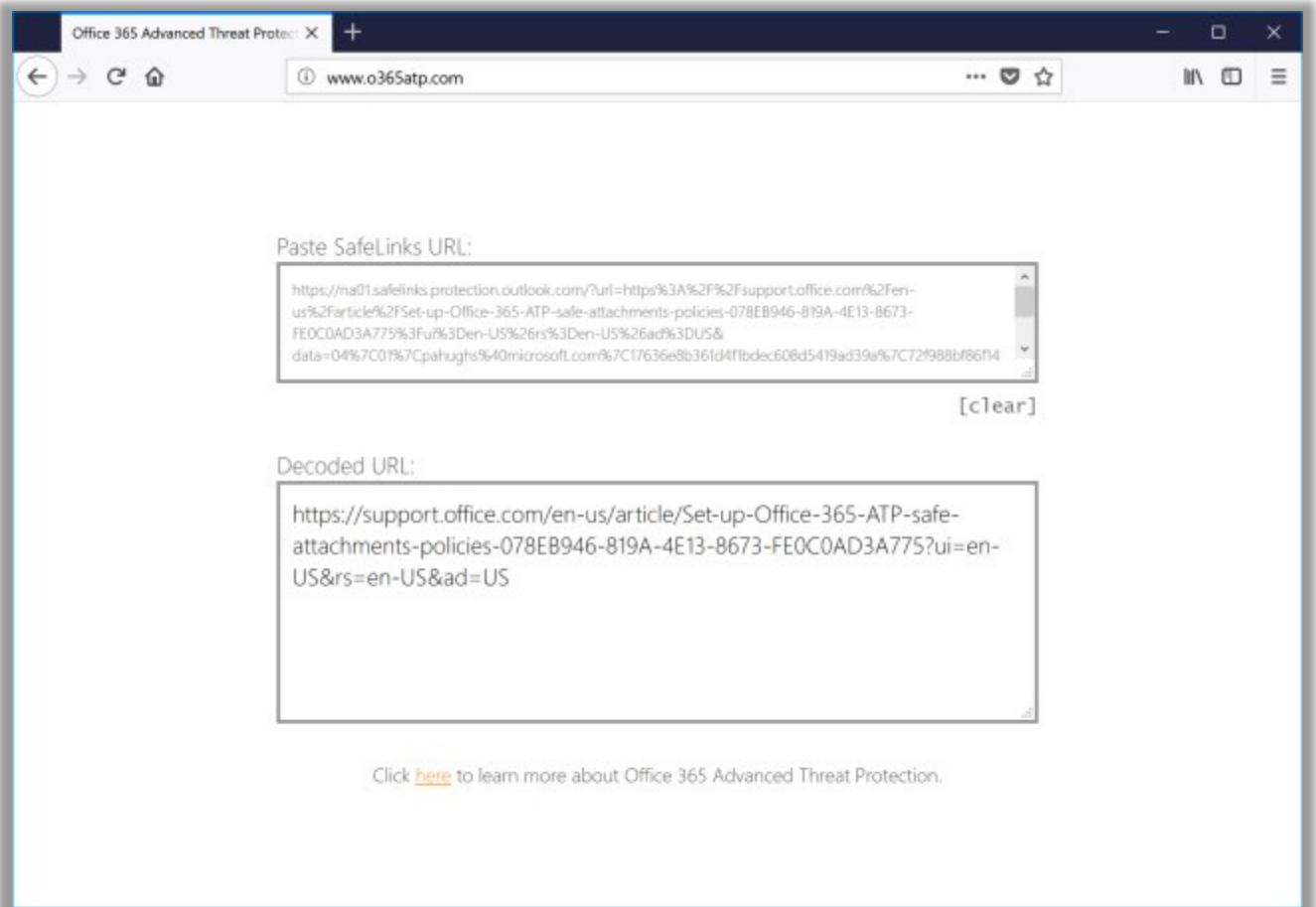


And in other cases, when it finds malicious content, end-users will see this page instead.



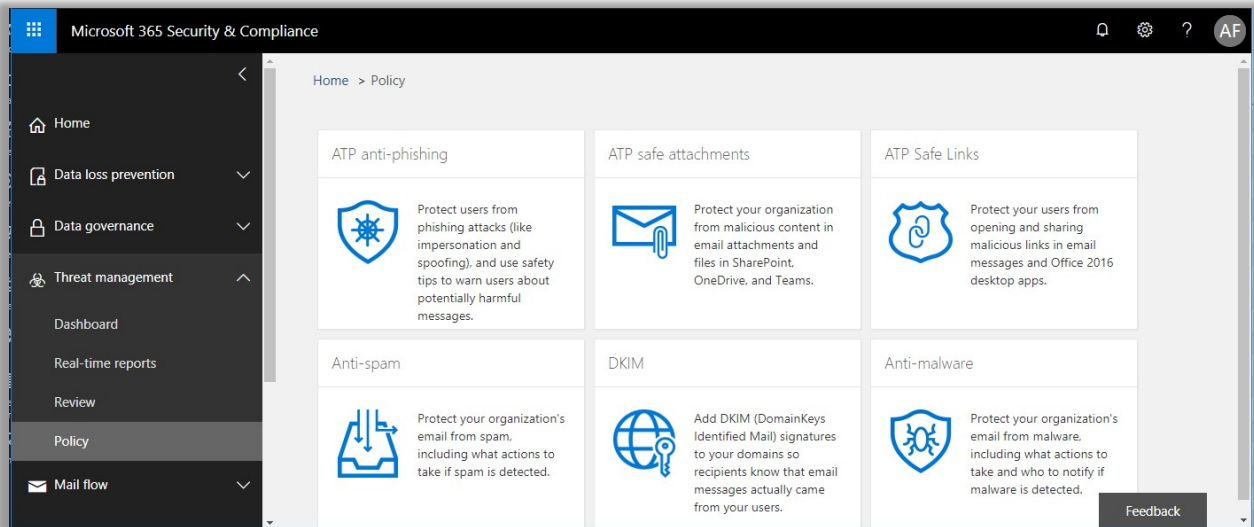
Remember that the option to click through to the site can be presented, or not, as per your policy selections. And while I suppose false positives could be possible, why risk it? I usually prevent them from being able to do this.

Microsoft also has a website for messages that have been processed (and subsequently, rewritten) by Safe Links, you can use this decoder (<https://www.o365atp.com/>) to return the original URL. To use it, simply copy a rewritten URL from a processed message and then paste it in the link window. The decoded link will appear below.

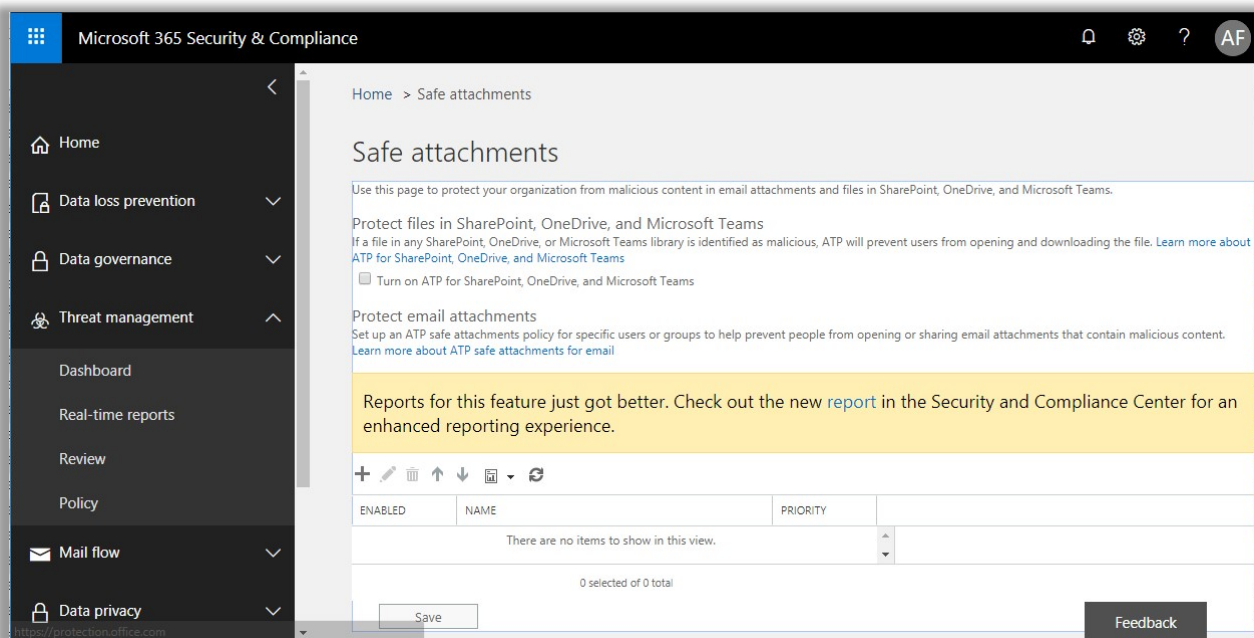


Safe Attachments

Return to the Security & Compliance Center to set it up. From Threat management > Policy choose ATP safe attachments.



Here you can start by checking the box for **Turn on ATP for SharePoint, OneDrive and Microsoft Teams**, but again—be forewarned. This move could impact performance. Now go ahead and click the + plus button to add a new policy.



First choose whether to simply **Monitor** this policy, straight up **Block** detected malware, or **Replace** (remove the attachment but deliver the message body without the attachment). The last option, which is newer, is **Dynamic Delivery**, which is basically picking *Replace* and delivering the message right away, but only reattaching the content if it passes the scan. This can help with those delivery delays I mentioned, but again, attachments can be delayed.

No matter what you pick here, you are also going to want to elect some administrator-monitored address to which content that is flagged or stripped can be redirected. Set your conditions (e.g. domain, group, etc.) and **Save** the policy.

new safe attachments policy

*Name:

Description:

Safe attachments unknown malware response
Select the action for unknown malware in attachments.[Learn more](#)

Warning
Monitor, Replace and Block actions may cause significant delay to email delivery. [Learn more](#)
Dynamic Delivery is only available for recipients with hosted mailboxes. [Learn more](#)
If you choose the Block, Replace or Dynamic Delivery options and malware is detected in attachment, the message containing the attachment will be quarantined and can be released only by an admin.

Off - Attachment will not be scanned for malware.
 Monitor - Continue delivering the message after malware is detected; track scan results.
 Block - Block the current and future emails and attachments with detected malware.
 Replace - Block the attachments with detected malware, continue to deliver the message.
 Dynamic Delivery - Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.

Enable redirect
Send the attachment to the following email address

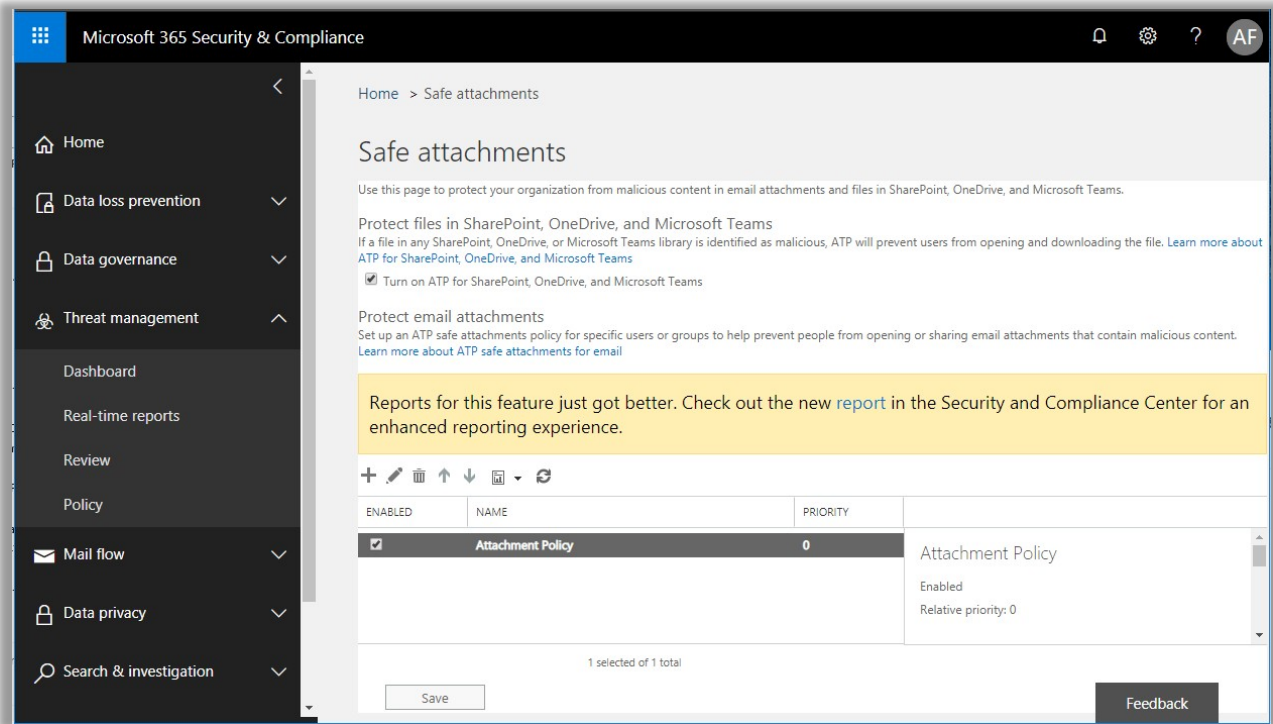
Apply the above selection if malware scanning for attachments times out or error occurs.

Applied To
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

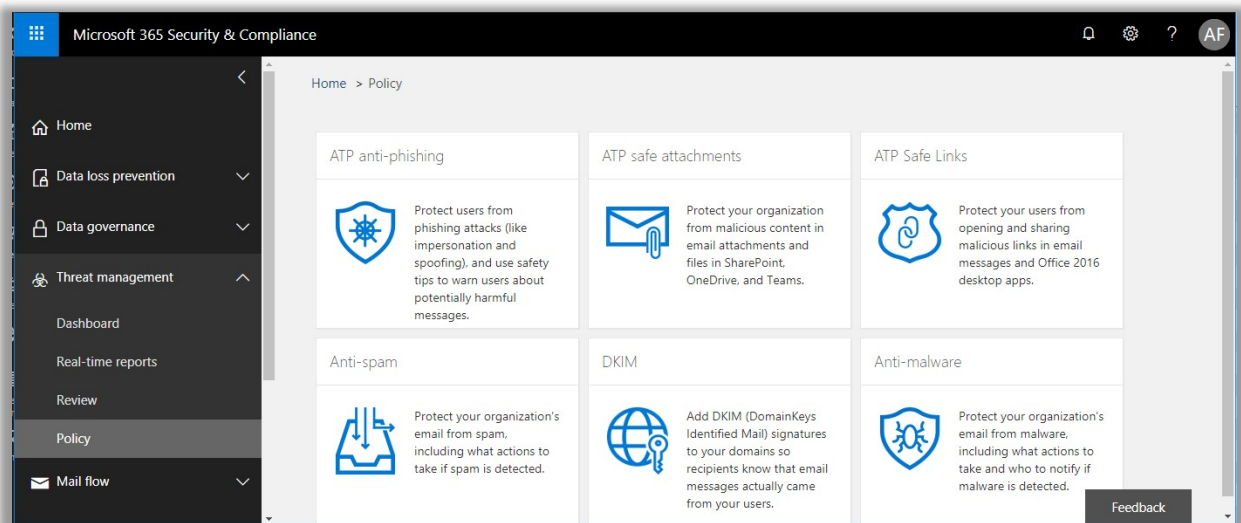
Except if...

If using the **Dynamic Delivery** option, you may receive a warning stating that this option applies to Office 365-hosted mailboxes only (not hybrid on-premises otherwise). After you have reviewed the settings, **Save** again on this page.

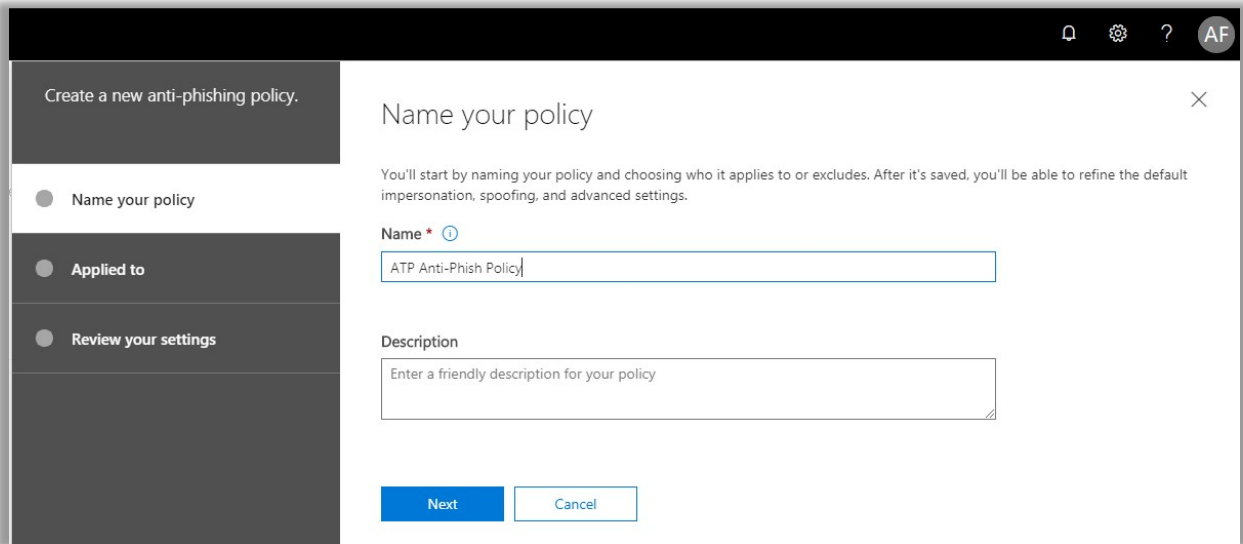


Anti-Phish

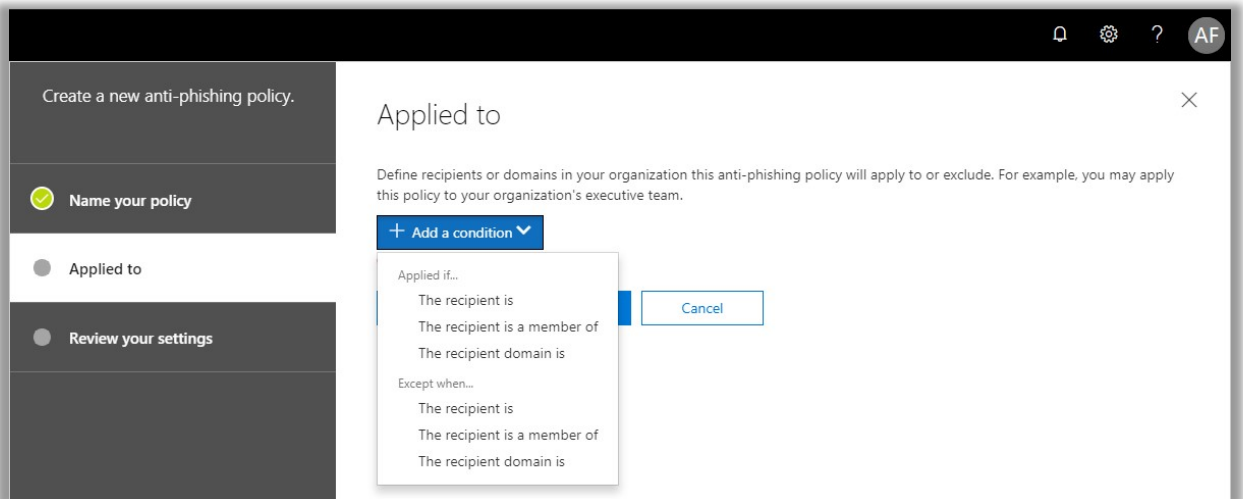
Find **Threat management** > **Policy** from the left menu. Choose **ATP anti-phishing**.



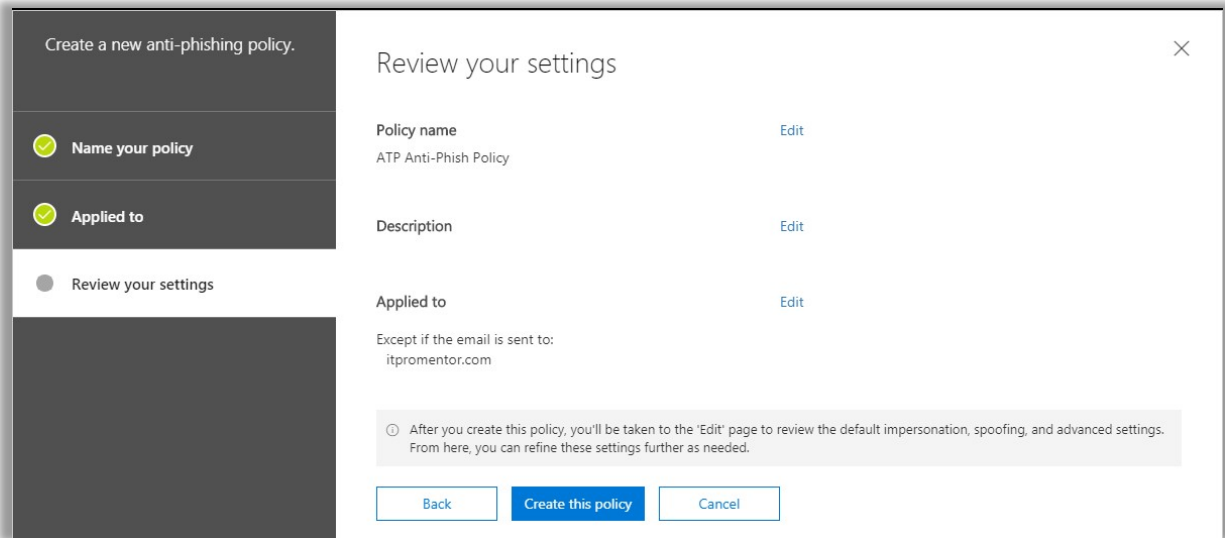
Simply choose to + **Create** a new policy. Give it a name and **Next**.



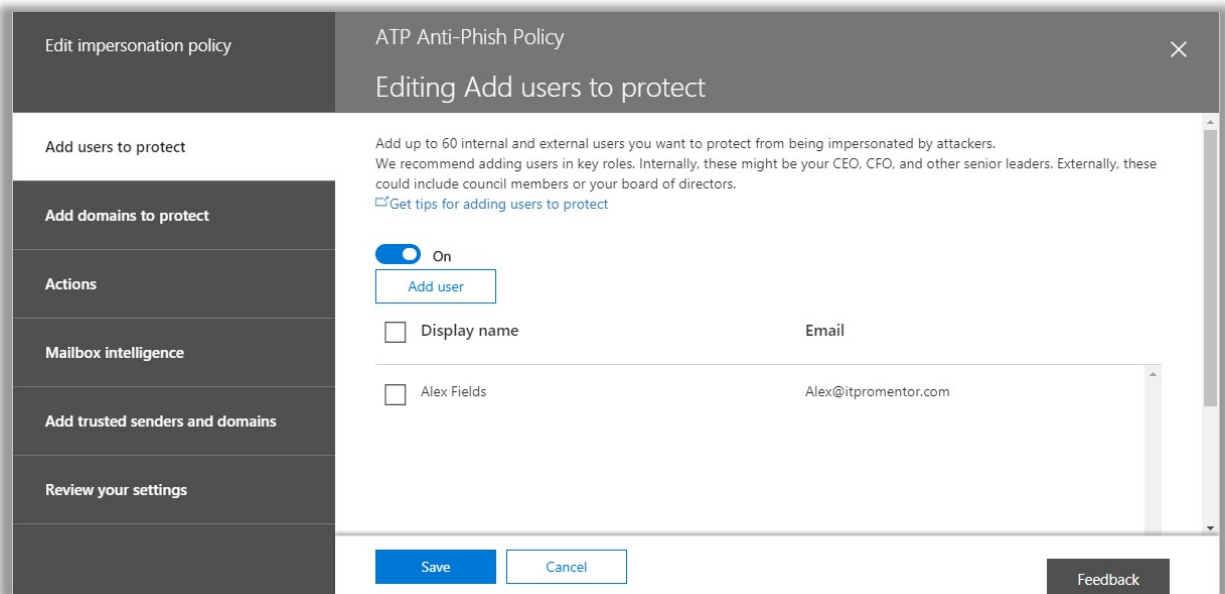
You must add a condition for how this policy is applied. I normally apply this policy to the entire tenant, but you can also use group membership or some combination of a group/domain and exceptions. After completing the conditions, choose **Next**.



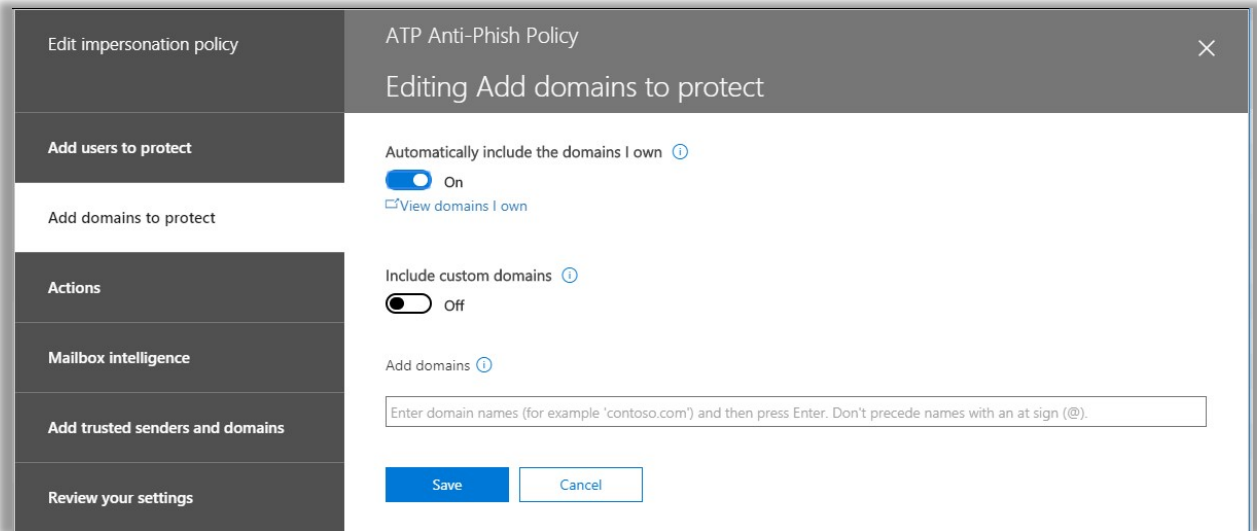
Now you basically **Create this policy**, then go back and edit the individual settings.



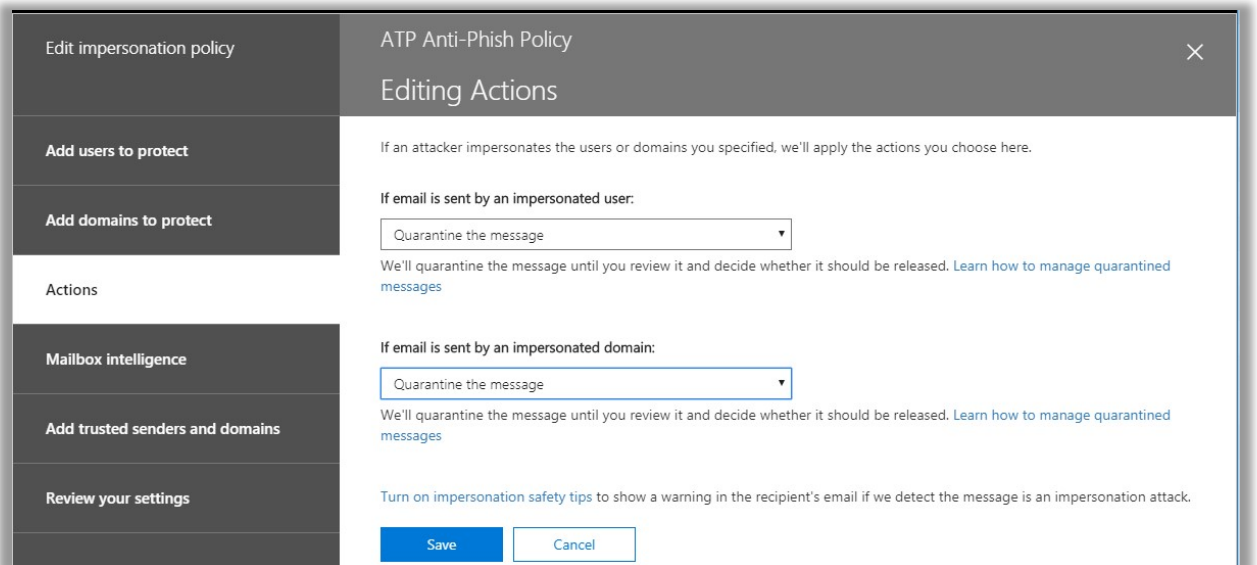
First, **Edit** the **Impersonation** settings. You can only choose up to 60 users for this, so it's recommended to focus on key roles such as CEO, CFO, and the like. Since I'm Chief Awesome Sauce here at ITProMentor.com, I added myself to this list.



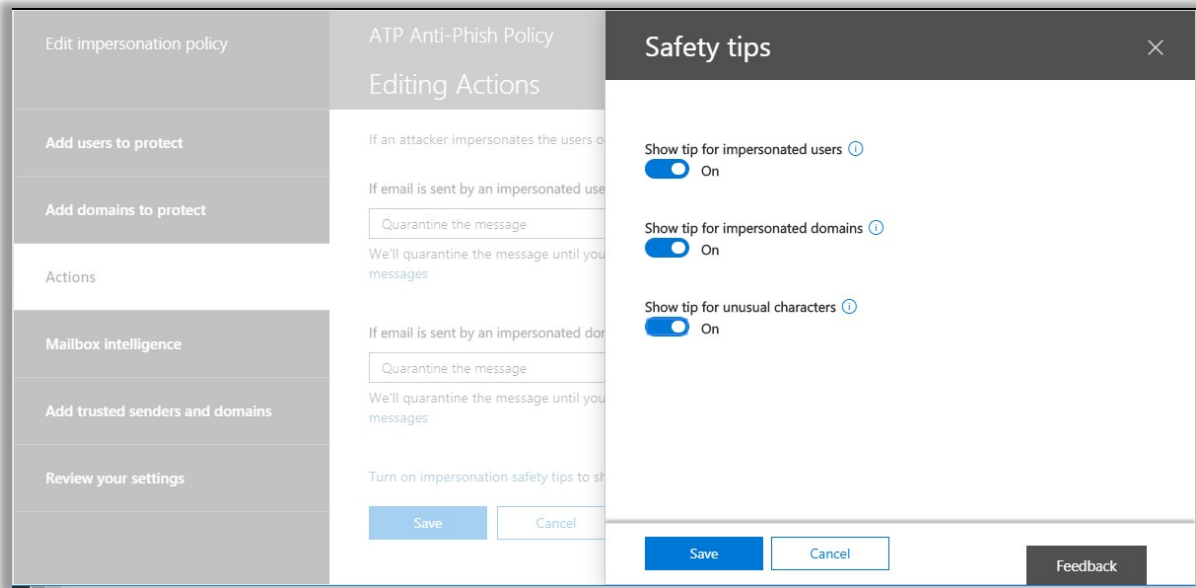
This is self-explanatory, you can choose which domains to include.



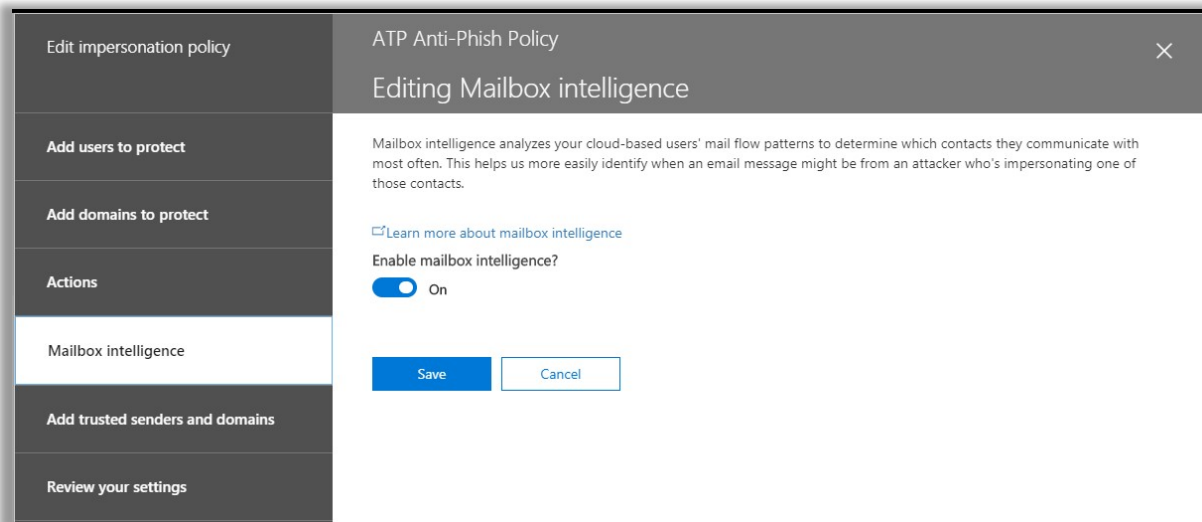
Now you can begin to choose some actions. In this example I am choosing **Quarantine**, but you may prefer to redirect this message to an administrator. Check out the **Turn on impersonation safety tips** link on this page, also.



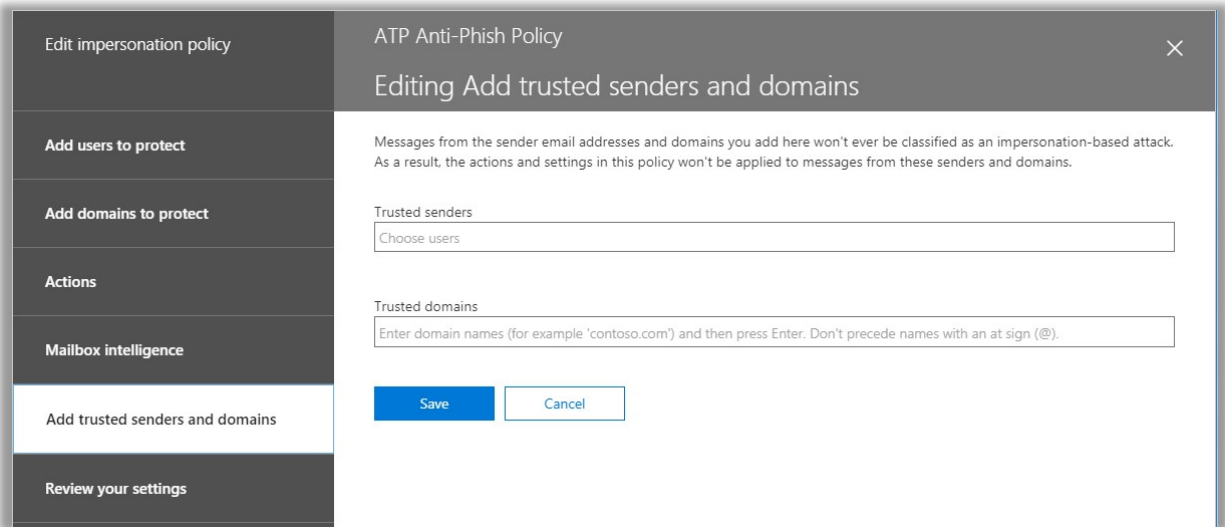
These notifications can help warn users if impersonation is suspected.



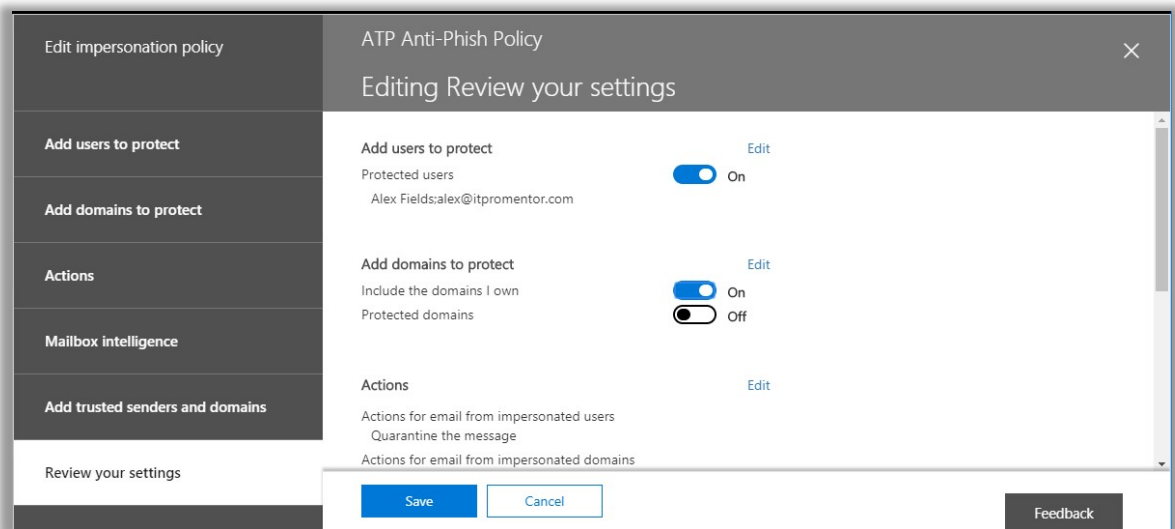
Here is where the machine learning comes in—Mailbox intelligence will figure out what mail-flow patterns are “typical” in the org, and then applies this learning to look for anomalies. If that’s too Big Brother for you, leave it off. I’ll leave it on for a while and report back my findings.



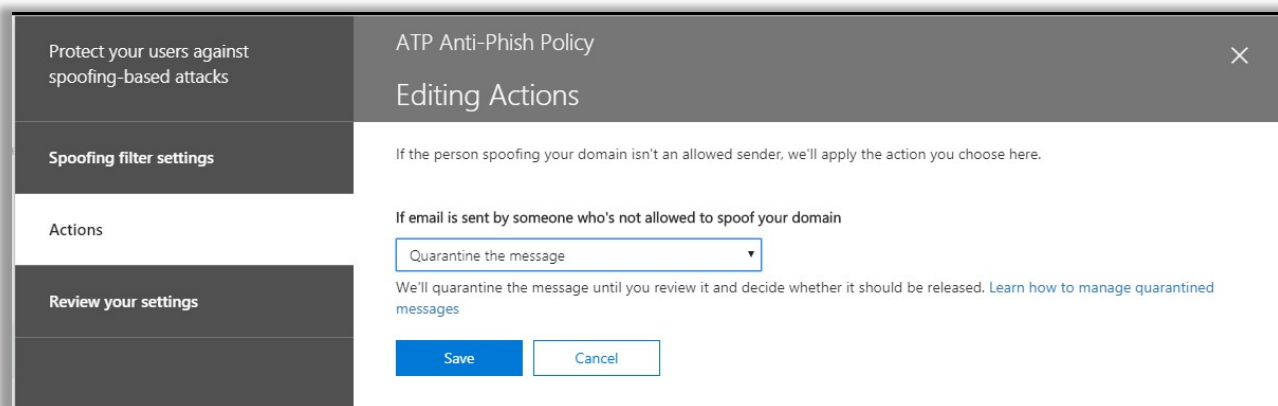
It is also possible to exclude certain senders and domains from this policy, like a whitelist. If you have the same added to your anti-spam policies, it doesn’t matter, you have to add them here also.



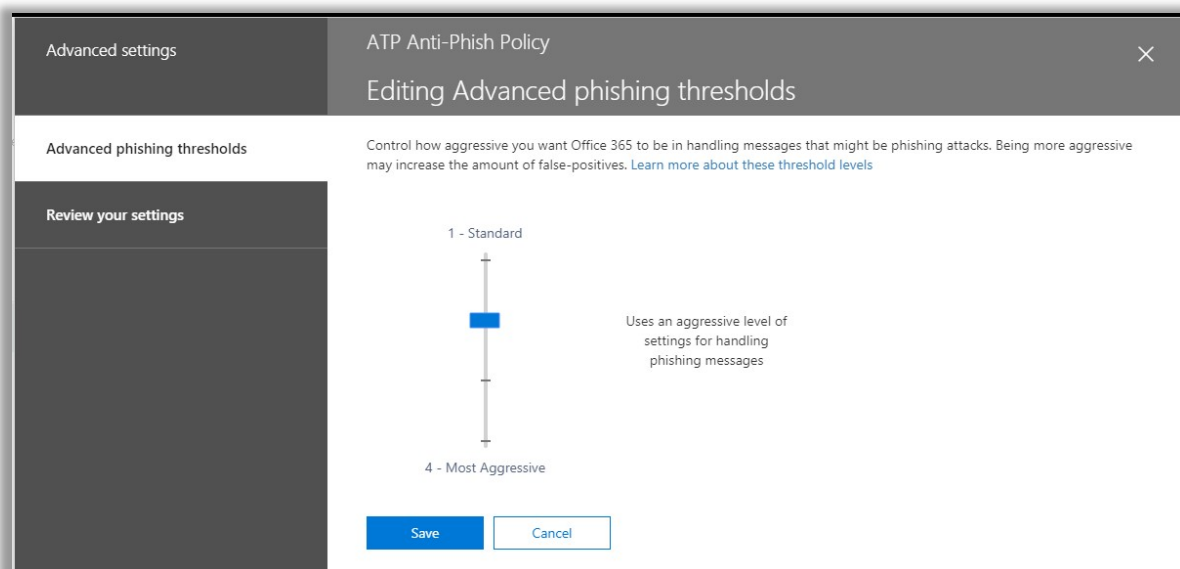
Now you can just review the settings and **Save**.



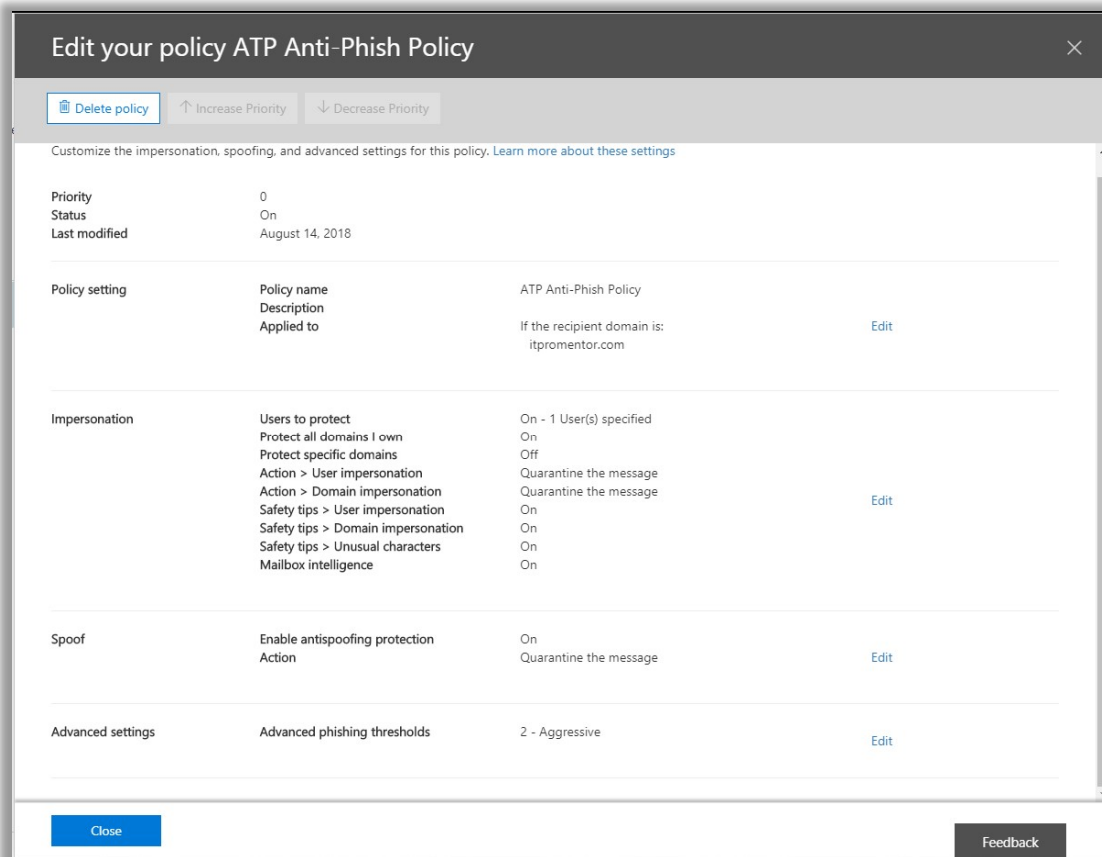
Next edit the **Spoof** settings of the policy. They have this action set to Junk mail folder by default, but I prefer **Quarantine**. Choose **Save**.



Last you can edit the **Advanced** settings. There are four different levels of aggressiveness. It is on 1 (*Standard*) by default, but I recommend at least 2 (*Aggressive*), and you may consider going even higher to 3 or 4 (*Most Aggressive*).



If you like, you can review your settings for the policy again.



Microsoft 365 Business: Continued improvement

The ironic thing about publishing anything in the world of technology is that it is instantly out of date as soon as it goes to print. This is even more true with Microsoft 365 and other cloud products. Things change quickly, and sometimes you can't help but feel like someone moved your cheese on you.

However, the overall structure of the Microsoft 365 bundles should remain basically the same. They will likely always include:

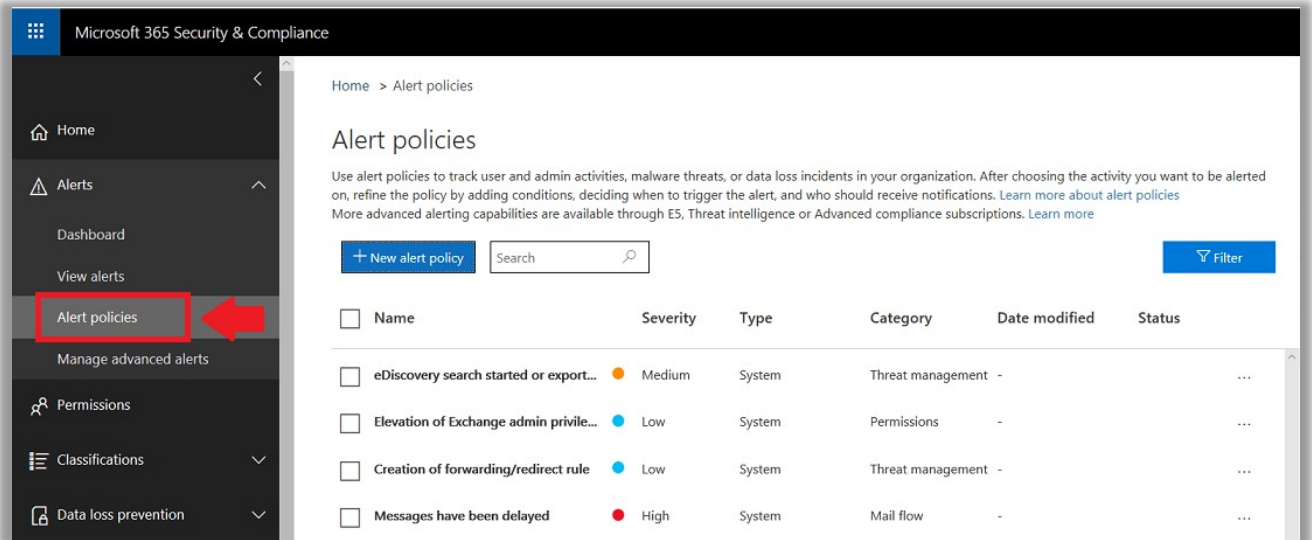
- **Office/Productivity software** such as: email (Exchange Online), chat/communications platform (Teams), and file-sharing and collaboration tools (SharePoint Online). And of course, there are so many more—To-Do, Planner, Bookings, Invoicing, Forms, Flow, PowerApps, StaffHub, Stream, and so on.
- **Identity and Device management** will continue to be supported by Azure Active Directory and Microsoft Intune/Device Management
- **Security & Compliance** tools and add-ons like Azure Information Protection, Archiving and Retention, Data Loss Prevention, Advanced Threat Protection—and maybe others!
- **Windows 10** subscription

There are a few other built-in features I would like bring to your attention before we conclude.

Alert Policies

Alert Policies is something in the Security & Compliance Center (<https://protection.office.com>) that should be on your radar. They allow you to generate email notifications (alerts) when certain events happen in Microsoft 365.

Choose **Alerts > Alert policies**.



Microsoft 365 Security & Compliance

Home > Alert policies

Alert policies

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications. [Learn more about alert policies](#)
More advanced alerting capabilities are available through E5, Threat intelligence or Advanced compliance subscriptions. [Learn more](#)

[+ New alert policy](#) [Filter](#)

| <input type="checkbox"/> | Name | Severity | Type | Category | Date modified | Status |
|--------------------------|----------------------------------------|----------|--------|-------------------|---------------|--------|
| <input type="checkbox"/> | eDiscovery search started or export... | Medium | System | Threat management | - | ... |
| <input type="checkbox"/> | Elevation of Exchange admin privile... | Low | System | Permissions | - | ... |
| <input type="checkbox"/> | Creation of forwarding/redirect rule | Low | System | Threat management | - | ... |
| <input type="checkbox"/> | Messages have been delayed | High | System | Mail flow | - | ... |

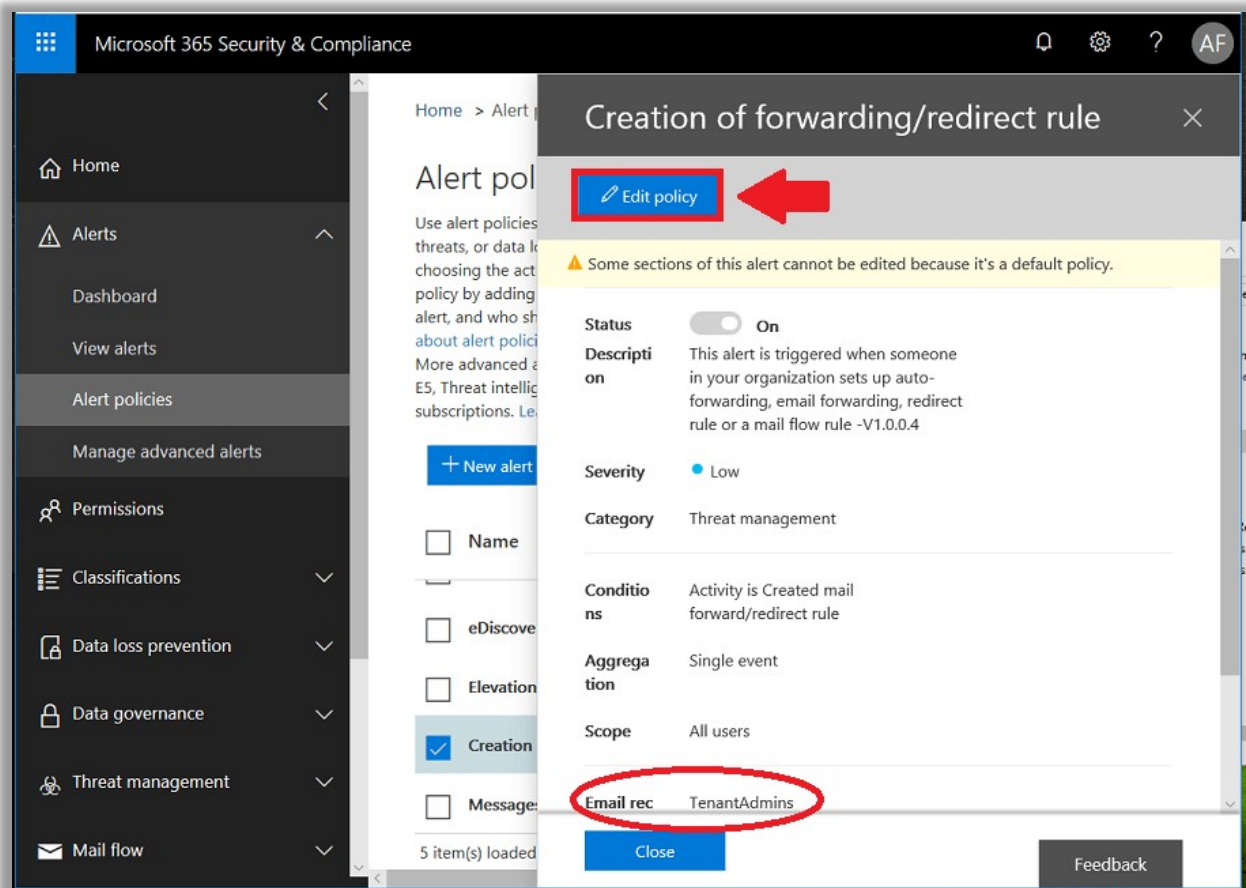
From here, you should see at least a few policies which are created by default, e.g.:

- eDiscovery search started or exported
- Elevation of Exchange admin privilege
- Creation of forwarding/redirect rule
- Messages have been delayed

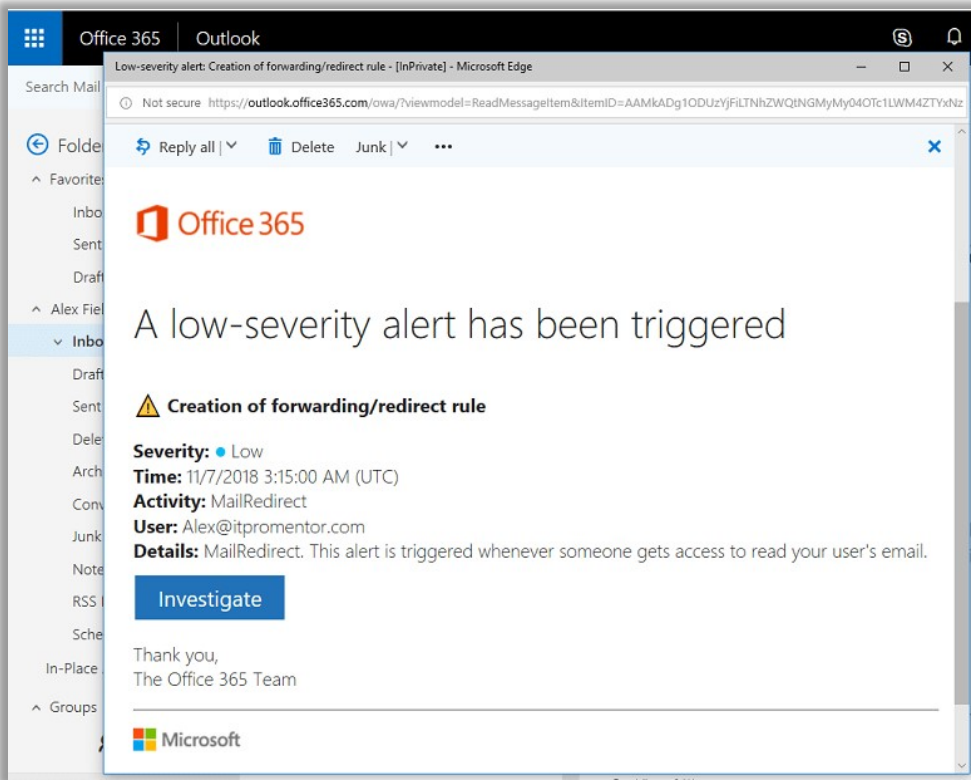
“Bigger” subscription bundles such as E5 include many more alerts. But for the SMB, this is a good list of defaults. I especially like *elevation of privilege* and creation of *forwarding/redirect rules* (this is one of the first things attackers will attempt if they gain control of a mailbox account). See here for more detail on the default policies included with each subscription:

<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

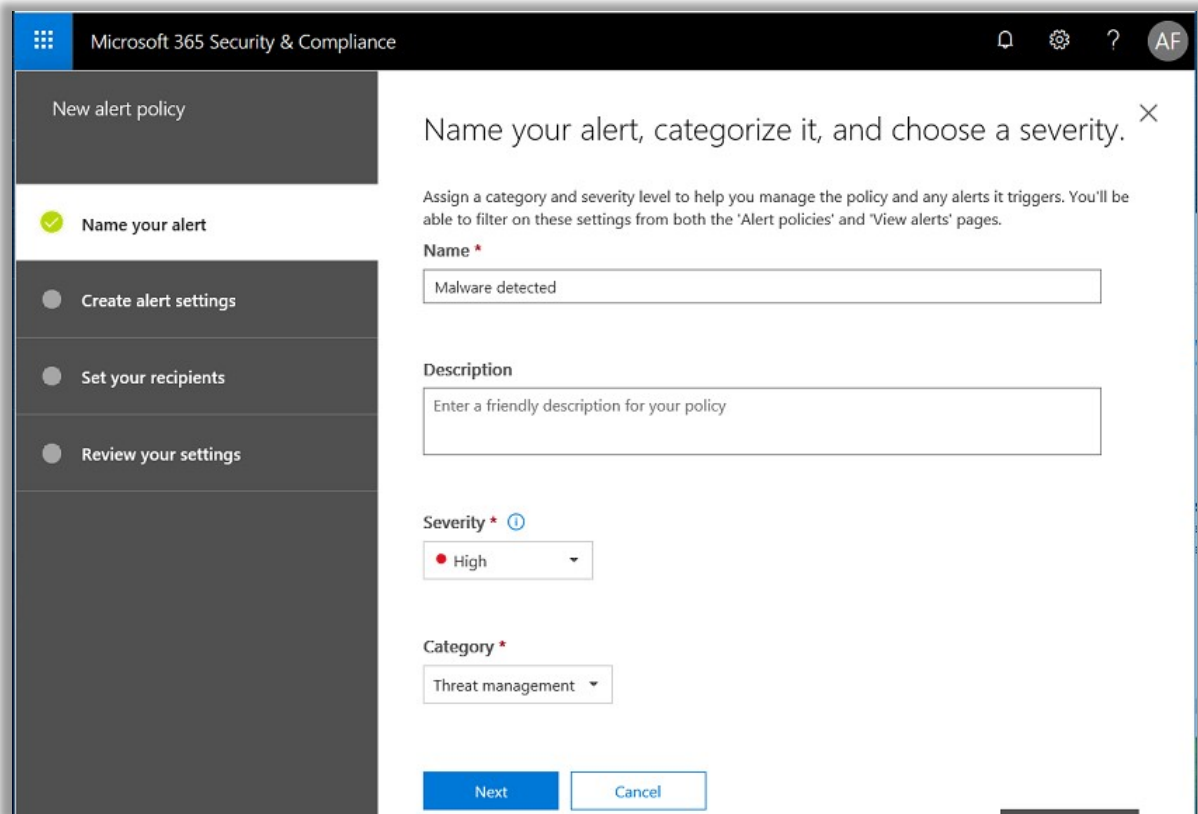
If you don't monitor the inboxes for your tenant admins day to day, then you should probably edit these default policies now, and change the recipients to people who will actually see the alerts and take action.



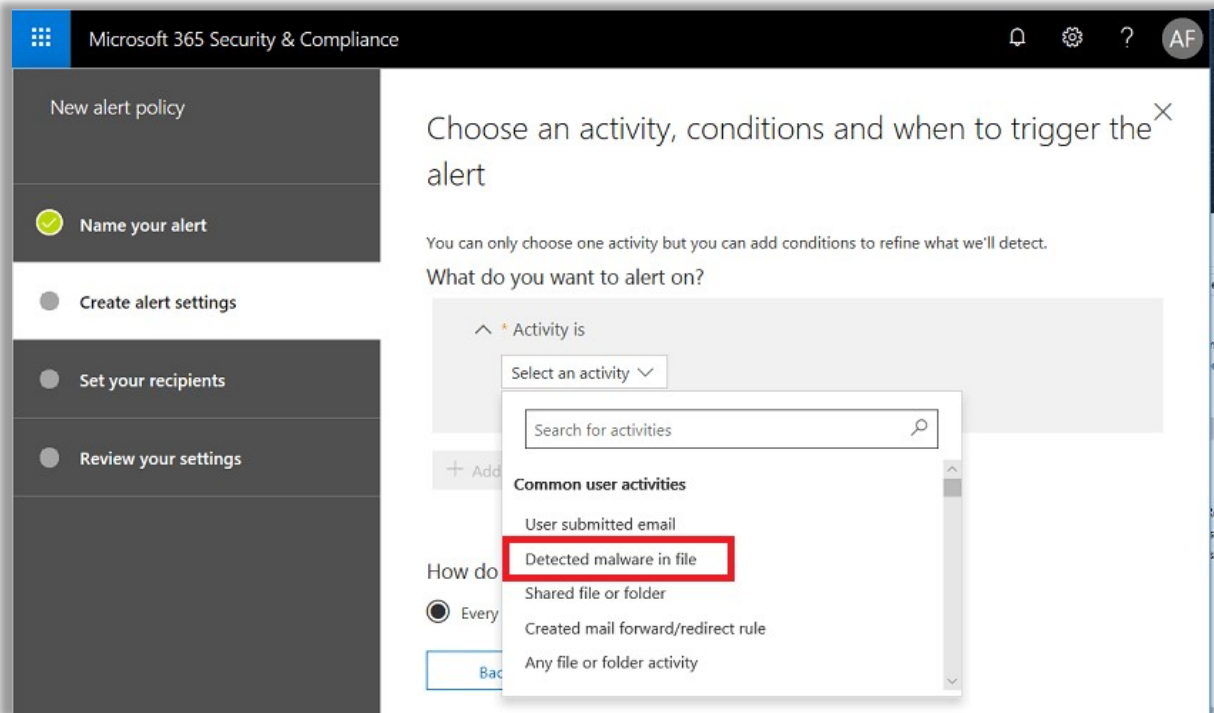
When an event occurs that trips this alert, you can expect an email notification like the one pictured below.



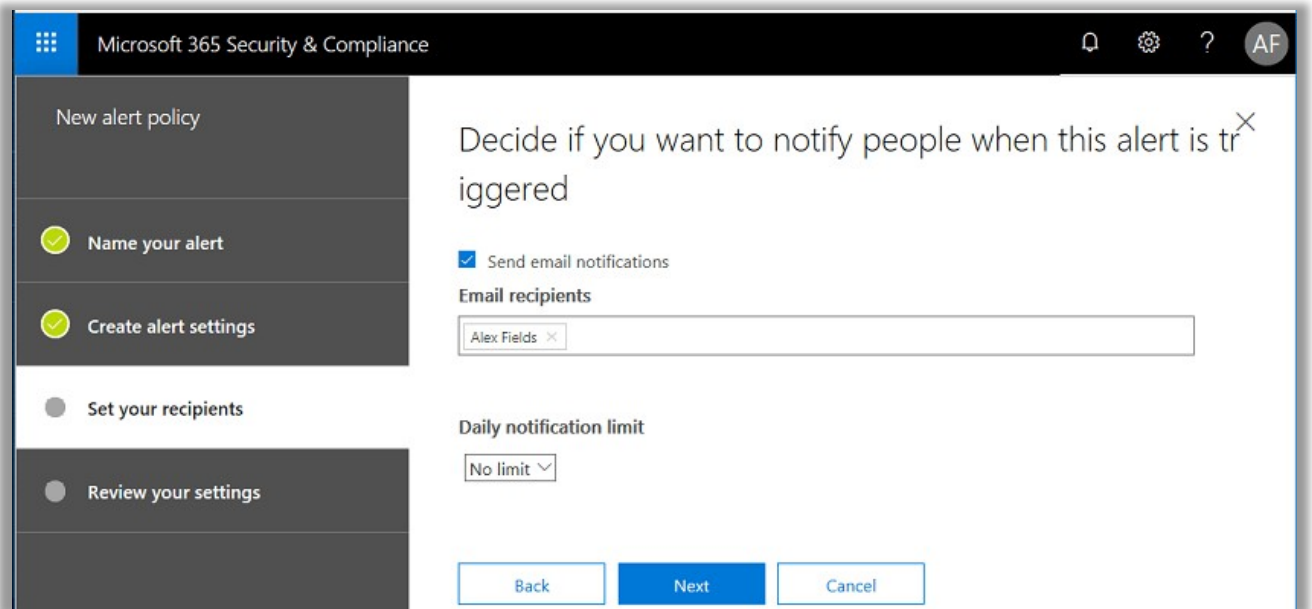
You can also create other alerts to your liking. Every tenant has access to certain alerts, and if you have subscriptions such as E5 or Advanced Threat Protection Plan 2, then you will see even more options available. In this example, I'll create a simple alert for Malware detected in a SharePoint or OneDrive file—this one is available in Microsoft 365 Business.



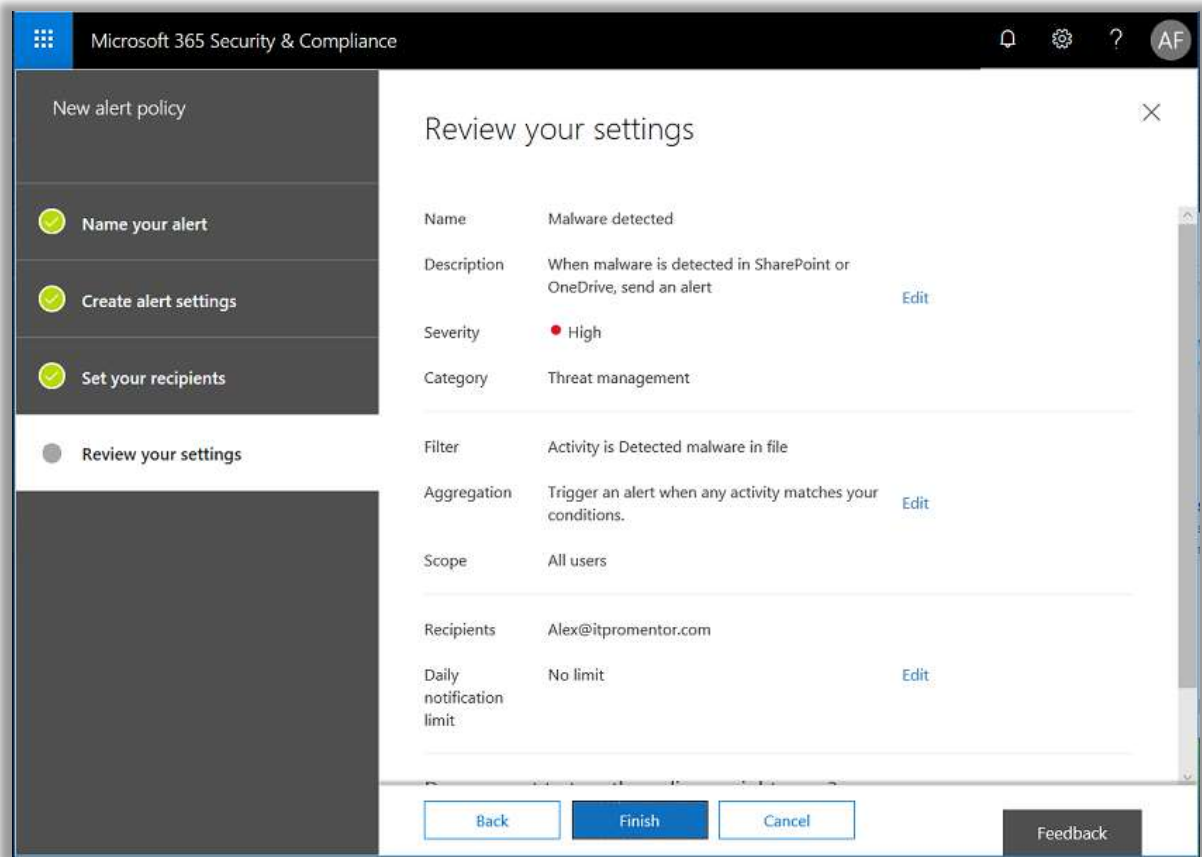
You can search for activities—start typing “malware” to find **Detected malware in file** in this list.



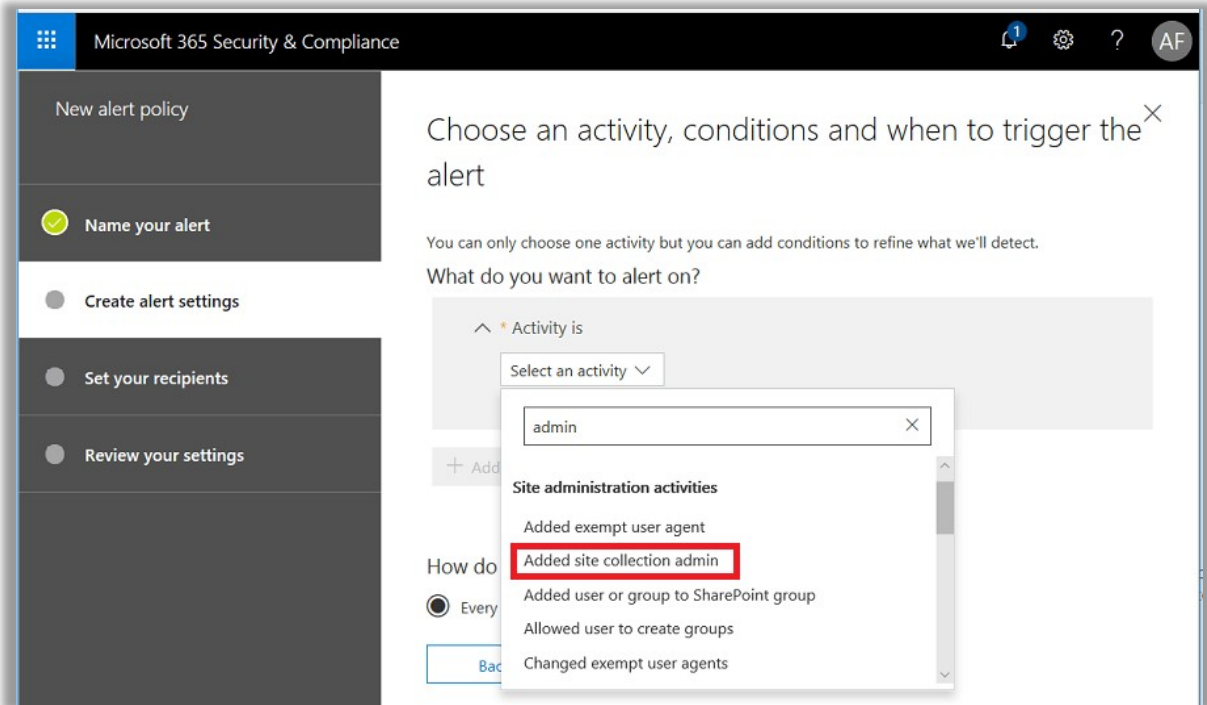
Now choose a recipient (or more than one). If you are a service provider it can be beneficial to add your support contact to the GAL so it's available here.



Review your new alert and click **Finish**.



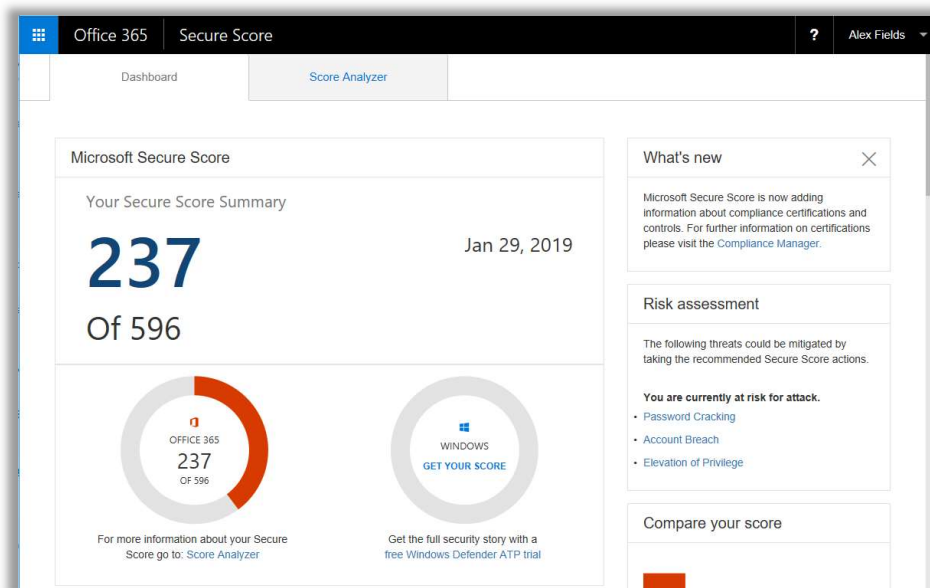
Wasn't that easy? You can create all types of alerts; you can get notified when stuff happens, when groups are changed, deleted, or new admin privilege is given to a site collection (that's a good one, too!).



Think about the things that should or should not happen in your organization. What do you need to know about? See if you can design some alerts based on your own criteria.

Secure Score

Microsoft has a free interactive “security scorecard” available with any subscription. It basically contains a list of actions that you can take to improve your tenant’s overall security posture. Most actions are “scored,” and the more of them you complete, the higher your score.



Beware, though, there is some sales-y stuff going on in here. For example, you can choose to meet security controls in numerous ways, however, they tend to reward you with *more* points for action items taken with products that are more expensive or included only in the E5 bundle. For example: if you use Intune to manage mobile devices it is worth several times more points than if you use the built-in MDM with Office 365.

And if you add Cloud App Security, which is not included with your subscription by default, you could stand to add up to 100 points. Does that purchase really make you “100 points more secure?” And if so, what does that mean, and how do they demonstrate that? Answer: they don’t. The points seem to correspond to price tag more than actual security benefit. So it is designed at least in part to upsell you. Just something to keep in the back of your mind—if you chase the numbers here you may end up spending more money or adding on to what comes bundled in Microsoft 365 Business by default.

But, I like this tool because it does give you some direction and a checklist, if you are lost and don’t know where to start with locking down your tenant.

Compliance Manager

Microsoft also continues to develop the Microsoft 365 platform, adding other new and surprising tools. Take, for instance, the new Compliance Manager—part of the Service Trust Portal found at <https://servicetrust.microsoft.com>.

The screenshot displays the Microsoft Compliance Manager interface. At the top, there are navigation links for 'Service Trust Portal', 'Compliance Manager', 'Trust Documents', and 'Regional Compliance'. The main heading is 'Compliance Manager' with a 'Help' icon. Below this, there are tabs for 'Assessments' and 'Action Items', along with options to 'Show Archived', '+ Add Assessment', and a 'Filter' dropdown.

The interface features several assessment scorecards for different 'Default Group' assessments:

- Office 365 - GDPR:** Compliance Score of 264 / 626. Created and Modified on 1/30/2019. Shows 0 of 65 Customer Managed Actions and 49 of 49 Microsoft Managed Actions.
- Office 365 - NIS:** Compliance Score of 1868. Created and Modified on 1/30/2019. Shows 0 of 60 Customer Managed Actions and 232 of 232 Microsoft Managed Actions.
- Office 365 - ISO:** Compliance Score of 794 / 1078. Created and Modified on 1/30/2019. Shows 0 of 60 Customer Managed Actions and 232 of 232 Microsoft Managed Actions.
- Azure - GDPR:** Assessment Status is 'In Progress'. Created and Modified on 1/30/2019.
- Azure - ISO 27001:** Assessment Status is 'In Progress'. Created and Modified on 1/30/2019.

A modal dialog box titled 'Add a Standard Assessment' is open in the center. It asks 'Which product are you evaluating?' with a dropdown menu set to 'Office 365'. Below this, it asks 'Select a certification' with a dropdown menu listing various standards: CSA CCM301, FFIEC, FedRAMP Moderate, GDPR, HIPAA (highlighted), ISO 27001:2013, ISO 27018:2014, NIST 800-171, NIST 800-53, and NIST CSF.

The basic gist of this tool is that you can select from a number of compliance bodies to generate an assessment scorecard that assists you in identifying how to meet those particular controls within your tenant. You can see "Microsoft Managed Actions" and "Customer Managed Actions." Your job is to focus on the latter with your customers.

| Customer Managed Controls | | | | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------|-----------------------|-------------------------------------------|-------------------------|
| Access authorization (Addressable) | | | | | | 0/1 Assessed ^ |
| Controls / Articles | Compliance Score | Related Controls / Articles | Assigned User | Implementation Status | Implementation Date | Test date / Test result |
| Control ID: 45 C.F.R. § 164.308(a)(4)(ii)(B) Control Title: Access authorization (Addressable) Description: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | 8 | ISO 27001:2013: A.13.2.4 FedRAMP Moderate: PS-6(a) NIST 800-53: PS-6(a) | Assign Manage Documents | Select | <input type="text"/> <input type="text"/> | Select |
| More ∨ | | | | | | |
| Access establishment and modification (Addressable) | | | | | | 0/1 Assessed ∨ |
| Accountability (Addressable) | | | | | | 0/1 Assessed ∨ |

Drilling into an individual assessment, you can then assign individuals within the organization to certain tasks, and they can upload any associated documents such as policies and procedures that support the control. From this interface, you can track progress on individual tasks and improve your overall posture, and any supporting documentation or screenshots will be included and stored here for reference, giving you ease of access for future auditor review.

Pretty cool, right?

Conclusion

I encourage you to continue exploring your subscription, given the ever-expanding nature of the Microsoft Universe. In this guide, I have attempted to cover all of the major products/components that make up the “management backbone” of Microsoft 365 Business.

In my opinion, this is a compelling end-to-end solution:

- Manage cloud and hybrid **user identities** alike with **Azure Active Directory** and tie your identities to other third-party SaaS applications, too!
- Manage **device platforms** of all types with **Microsoft Intune/Device Management** including Windows, macOS, iOS and Android
- Secure your corporate resources with additional **data and application-level protections** including **Azure Information Protection, Archiving, Data Loss Prevention** and **Advanced Threat Protection**, to name a few

On top of that, new tools like Compliance Manager are being added to the subscription all the time. All of these things are available at an affordable price-point for small and mid-sized businesses. Adoption for this SKU is growing, and it is already becoming clear that these tools will be the future of modern management after the “four walls” paradigm has crumbled under the tides of change, which was first introduced with the advent of mobile devices and cloud-based applications.