Guide to the Azure Active Directory Best Practices Checklist

Alex Fields, ITProMentor.com

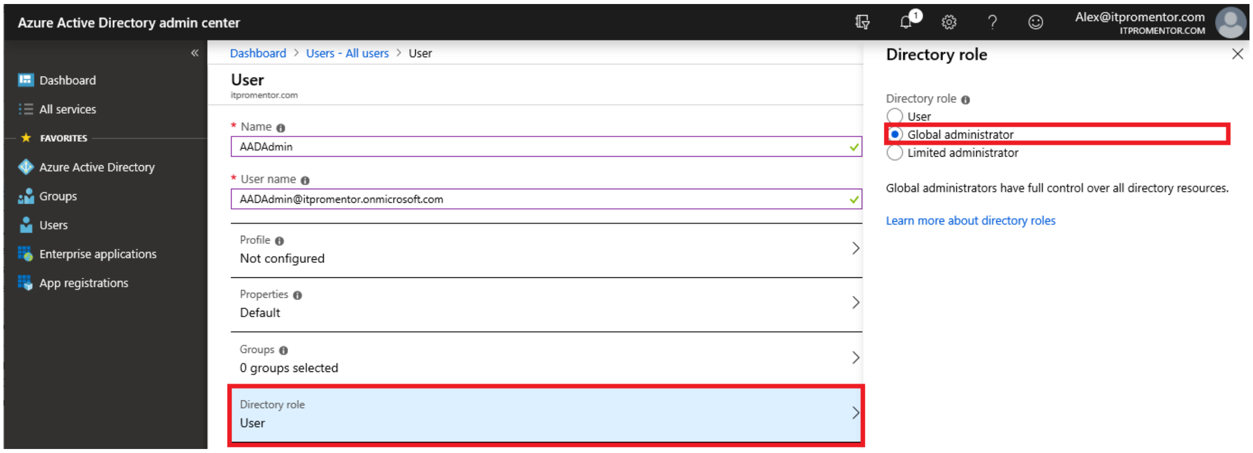
Updated: 07/15/2019

This resource corresponds to The Microsoft 365 Azure AD Best Practices Checklist, and is intended to be used as a baseline for provisioning new Microsoft 365 tenants according to best practices. With the SMB in mind, Azure AD Premium P2 / E5 features are excluded on purpose.

Table of Contents

☐ Create an emergency access global admin account

Microsoft recommends leaving one emergency access or “break glass” admin account excluded from each multi-factor authentication and Conditional access policies. Go to **Users > New user**.



User
itpromentor.com

* Name
AADAdmin

* User name
AADAdmin@itpromentor.onmicrosoft.com

Profile
Not configured

Properties
Default

Groups
0 groups selected

Directory role
User

Directory role

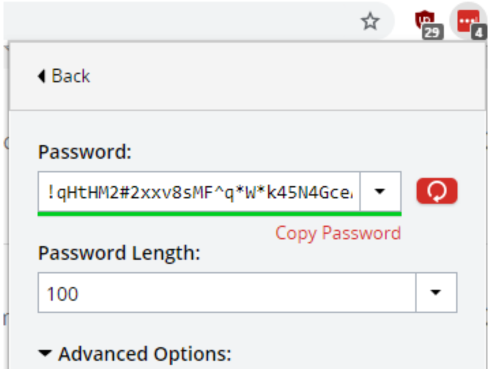
Directory role
○ User
● Global administrator
○ Limited administrator

Global administrators have full control over all directory resources.

Learn more about directory roles

Assign name & username (use the “onmicrosoft.com” domain). Pick **Directory role > Global administrator**. **Create** the account, noting the temporary password.

Login using the temporary password. Make sure to reset the password using a very long character string, such as 100 characters (e.g. randomly generated with a tool such as LastPass).



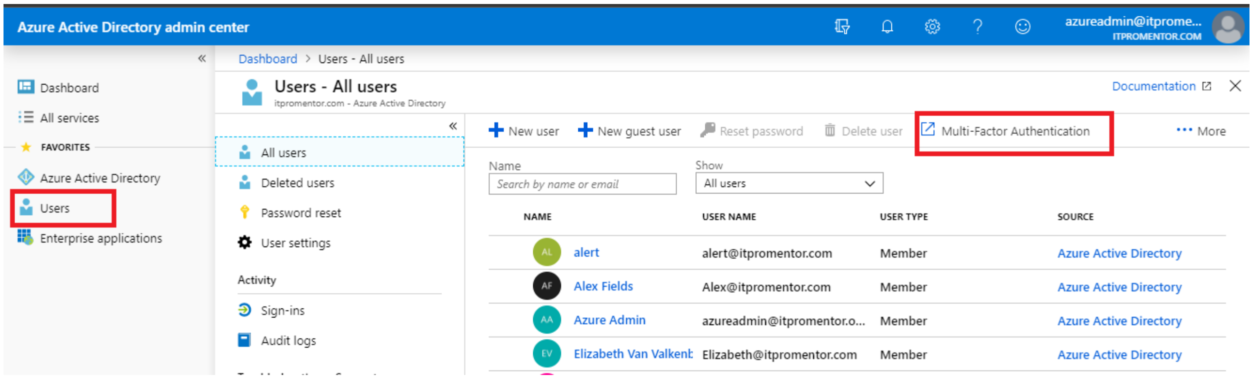
Password:
!qHtHM2#2xxv8sMF^q*W*k45N4Gce

Password Length:
100

I also recommend creating a security group called “Excluded from CA” and adding one account to that group, then assigning that group to the “Exclude” tab of every Conditional access policy. Anyone else who needs to be excluded from CA can be added or removed from the group easily, a needed. Be sure to review other guidance about these accounts on Microsoft’s own article.

☐ Configure multi-factor authentication settings

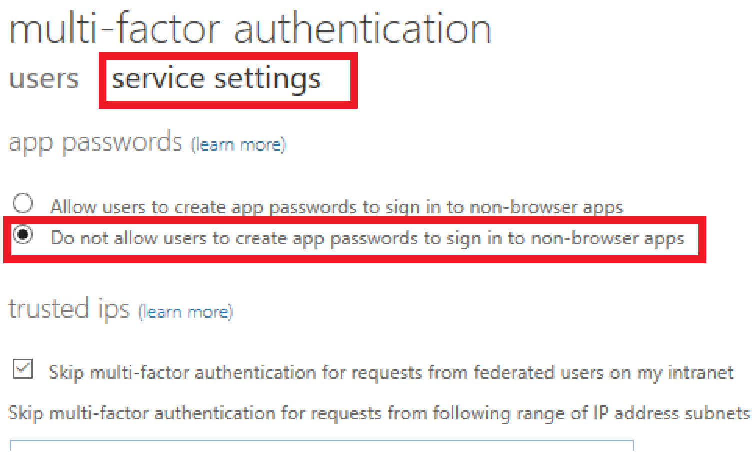
Before enabling multi-factor authentication for individual accounts, make some adjustments to the default service settings. Go to **Users** and click **Multi-Factor authentication**.



NAME	USER NAME	USER TYPE	SOURCE
alert	alert@itpromentor.com	Member	Azure Active Directory
Alex Fields	Alex@itpromentor.com	Member	Azure Active Directory
Azure Admin	azureadmin@itpromentor.o...	Member	Azure Active Directory
Elizabeth Van Valkent	Elizabeth@itpromentor.com	Member	Azure Active Directory

Click on **service settings** at the top of the screen, and make these adjustments:

- **Do not allow users to create app passwords to sign in to non-browser apps:** App passwords are only needed when apps do not support modern authentication and MFA. It is recommended to use apps that support modern auth, and to avoid using app passwords (a.k.a. MFA bypass).
- **Trusted IP addresses** (e.g. corporate offices) will bypass MFA. This feature requires Azure AD Premium. Note: you must use external (not internal) IP addresses—they must be internet routable.



○ Allow users to create app passwords to sign in to non-browser apps

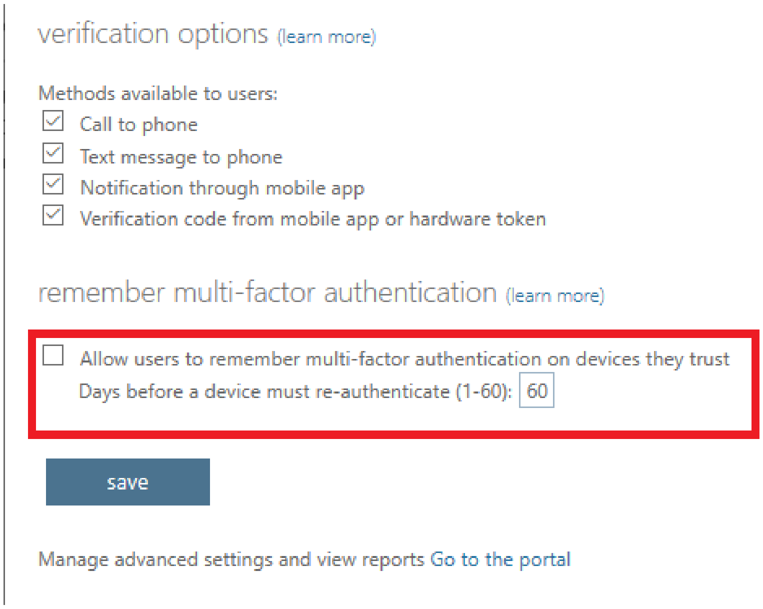
● Do not allow users to create app passwords to sign in to non-browser apps

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

Scroll down further. Note that mobile apps and hardware tokens are considered more secure than SMS text messages or phone calls. Consider excluding those options. Also, it is recommended that you do not allow users to remember devices. If an unmanaged device is lost or stolen but it has been marked to "remember" for MFA, this could introduce an unnecessary risk.

Instead, it is better to leverage Conditional access to 1) Require device compliance (which gives you more leverage over the device), and 2) *Always* require MFA on unmanaged devices. More on Conditional access soon.



verification options (learn more)

Methods available to users:

☑ Call to phone

☑ Text message to phone

☑ Notification through mobile app

☑ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

☐ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 60

Manage advanced settings and view reports Go to the portal

Save your selections.

You *could* enable accounts for MFA individually even now, however we can also improve the end-user experience by using Conditional access to require MFA under specific conditions, and also by setting up combined registration for self-service password reset (SSPR) at the same time—more on that later. Nevertheless, it is always recommended to enable MFA for all user accounts (excluding emergency access and service accounts as needed).

When you do turn it on for users, it is recommended to provide them with some instructional links in advance of this change, so they know what to expect. For example:

Setup 2-step verification for Office 365 (describes the MFA registration experience)

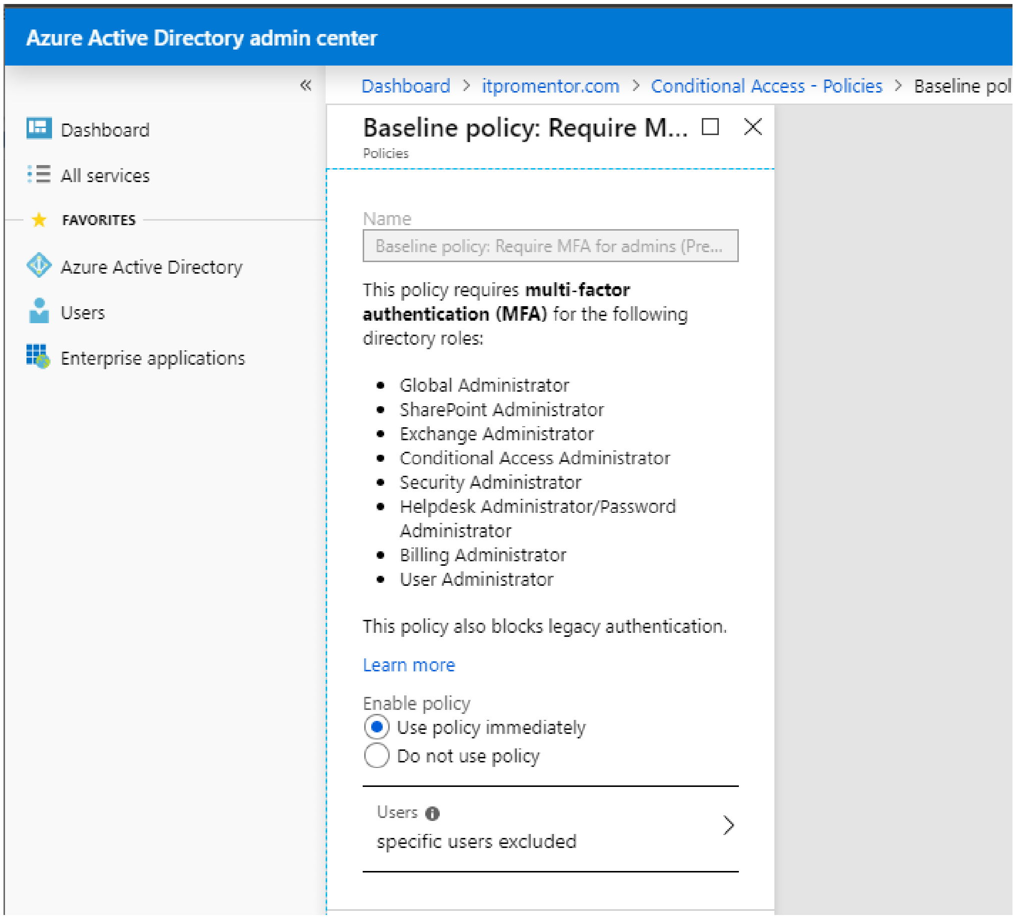
https://aka.ms/authappstart (configure the Microsoft Authenticator app)

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 MFA registration link)

☐ Setup Conditional access

Baseline policies are included with every tenant, and you should strongly consider enabling them, especially Require MFA for admins (excluding your break glass account of course).



Azure Active Directory admin center
«
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > itpromentor.com > Conditional Access - Policies > Baseline pol

Baseline policy: Require M...

Policies

Name

Baseline policy: Require MFA for admins (Pre...

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password Administrator
- Billing Administrator
- User Administrator

This policy also blocks legacy authentication.

Learn more

Enable policy

● Use policy immediately

○ Do not use policy

Users

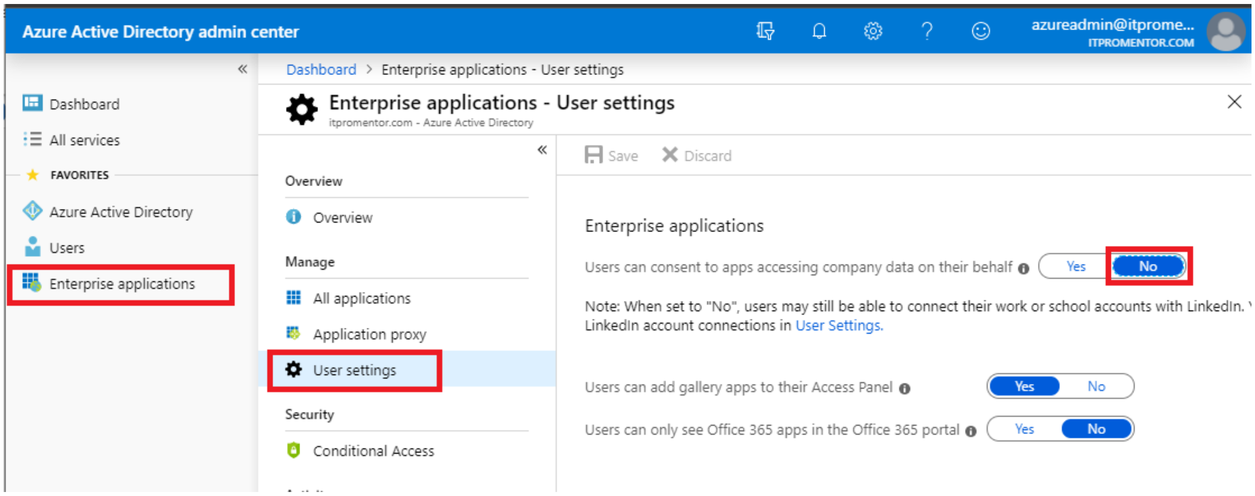
specific users excluded

Users will be prompted to register their security information for Multi-Factor Authentication once they are compelled to perform MFA via a Conditional Access policy. This applies to the baseline policies entitled “Require MFA for admins” and “End user protection,” as well as any custom policies that require multi-factor authentication as an access control.

For additional guidance on Conditional access policies, refer to this resource.

☐ Block users from consenting to apps requesting permissions

Find this in the Azure AD admin portal by navigating to **Enterprise applications > User settings**. Set the option **Users can consent to apps accessing company data on their behalf** to **No**.



Enterprise applications - User settings

Enterprise applications

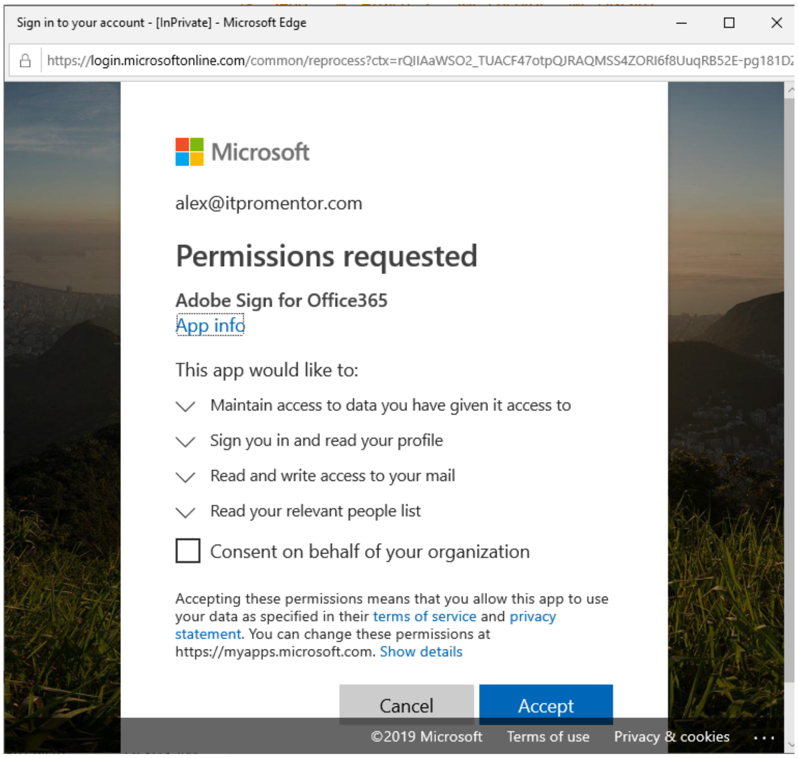
Users can consent to apps accessing company data on their behalf: Yes [✓ No]

Note: When set to "No", users may still be able to connect their work or school accounts with LinkedIn.
LinkedIn account connections in User Settings.

Users can add gallery apps to their Access Panel: [✓ Yes] No

Users can only see Office 365 apps in the Office 365 portal: Yes [✓ No]

This setting should be enabled by default for new tenants moving forward, but on existing tenants you may still need to change it. What does it do? Here's the deal: users may try to connect other apps to their Office 365 services. When they do, they may be asked to grant that outside application permissions to interact with the data behind the Office 365 service.


Sign in to your account - [InPrivate] - Microsoft Edge
https://login.microsoftonline.com/common/reprocess?ctx=rQIIAaWSO2_TUACF47otpQJRAQMSS4ZORI6f8UuqRB52E-pg181D
Microsoft

alex@itpromentor.com

Permissions requested

Adobe Sign for Office365
App info

This app would like to:

- Maintain access to data you have given it access to
- Sign you in and read your profile
- Read and write access to your mail
- Read your relevant people list

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

For legitimate apps this may be perfectly fine. But there are also known ransomware campaigns now which target Office 365 users specifically, and trick them into granting permissions to resources in 365.

By disabling this capability, only administrators will have the keys to consent to trusted applications on behalf of the organization. So if someone ran up against the restriction, and subsequently requested that the app be approved (by emailing the helpdesk or whatever), then an administrator could review the request and approve that app (one time for all users).

This same setting is available in PowerShell. To connect to Azure AD, run Connect-MsolService. Then:

```
Set-MsolCompanySettings -UsersPermissionToUserConsentToAppEnabled $false
```

Also check out this article for enabling exceptions in conjunction with this setting.

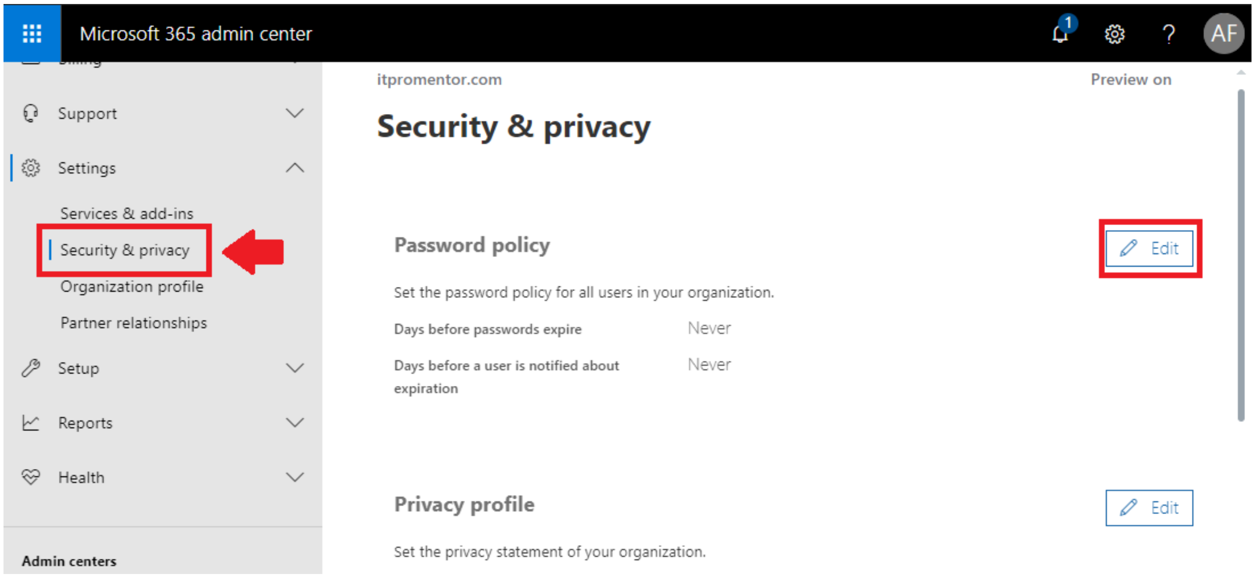
☐ Configure the password policy in the Microsoft 365 admin center

Navigate to **Settings > Security & Privacy** from the left menu of the Microsoft 365 admin center. Microsoft's new password guidance suggests that you can set the passwords to **Never** expire. I have spent a lot of time thinking and debating with others in the industry about this. And I have come to the conclusion that this is not great advice for most organizations in the real world, for a few reasons.

1. Credential leaks are still happening every day
2. MFA is usually not adopted org-wide, and even then, attacks that bypass MFA are on the rise
3. Most organizations are not doing a great job of watching their security logs for indicators of compromise, which would tell them when they need to change passwords

Therefore, unless you already have all of the above in place, you will probably want to rotate the password at least annually. Or, once passwordless (which is currently in preview) goes to general availability, and we have the option to literally remove the password attribute from Azure AD (this option is not there yet). I am not even going to cover passwordless in this guide because it's not time. Yet.

If you are successfully leveraging all of the other critical identity protections such as MFA, password protection, Conditional access and so forth, across the *entire* organization AND you feel confident that you would be able to detect and respond to an identity breach, only at that point should you move to non-expiring passwords. Otherwise, stick to expiry.



itpromentor.com

Security & privacy

Password policy

Set the password policy for all users in your organization.

Days before passwords expire: Never

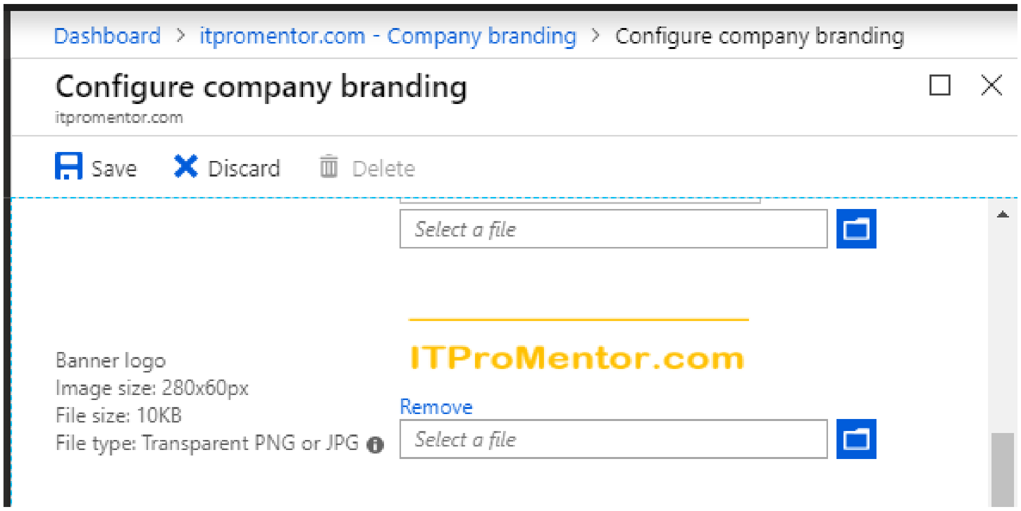
Days before a user is notified about expiration: Never

Privacy profile

Set the privacy statement of your organization.

☐ Configure Company branding

Company branding is usually viewed as something highly optional and purely aesthetic, but actually I believe it is fairly important for security, too. The reason being: many phishing campaigns will send users to fake login pages that mimic the popular cloud services like Office 365. Therefore, if you customize the login experience with your brand, it is less likely that users will fall for the generic “look-alikes.”

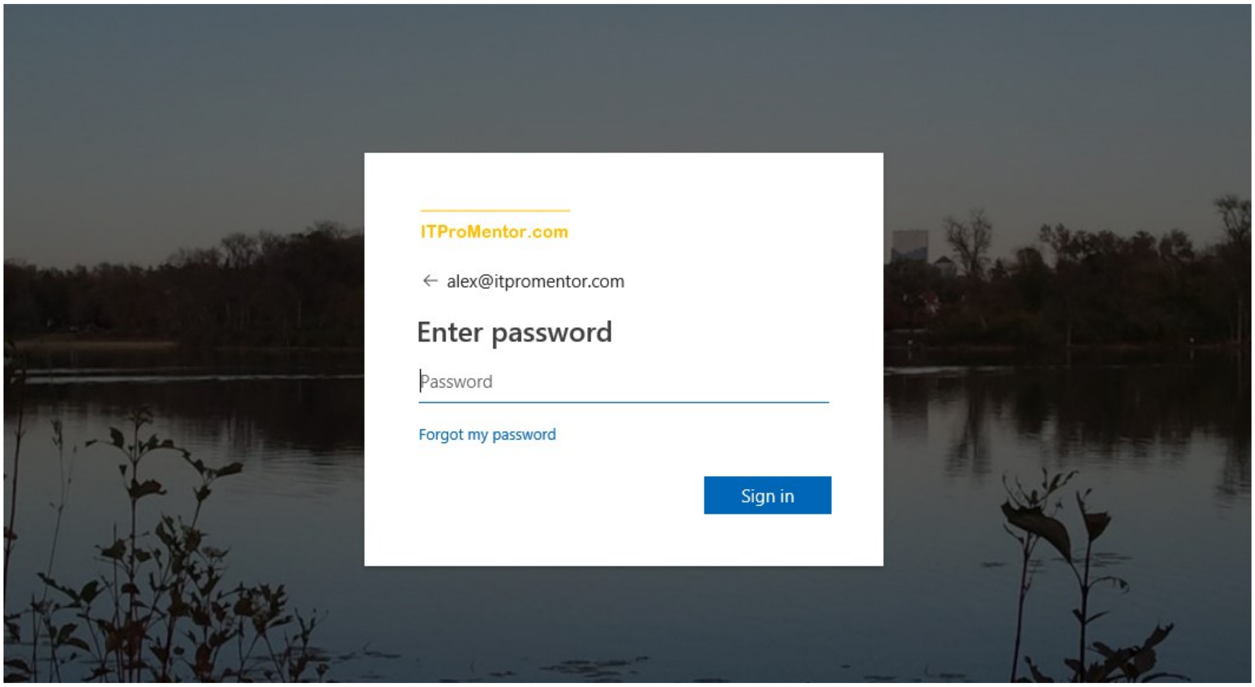

Dashboard > itpromentor.com - Company branding > Configure company branding
Save
Discard
Delete
Select a file
ITProMentor.com
Remove
Select a file

Configure company branding

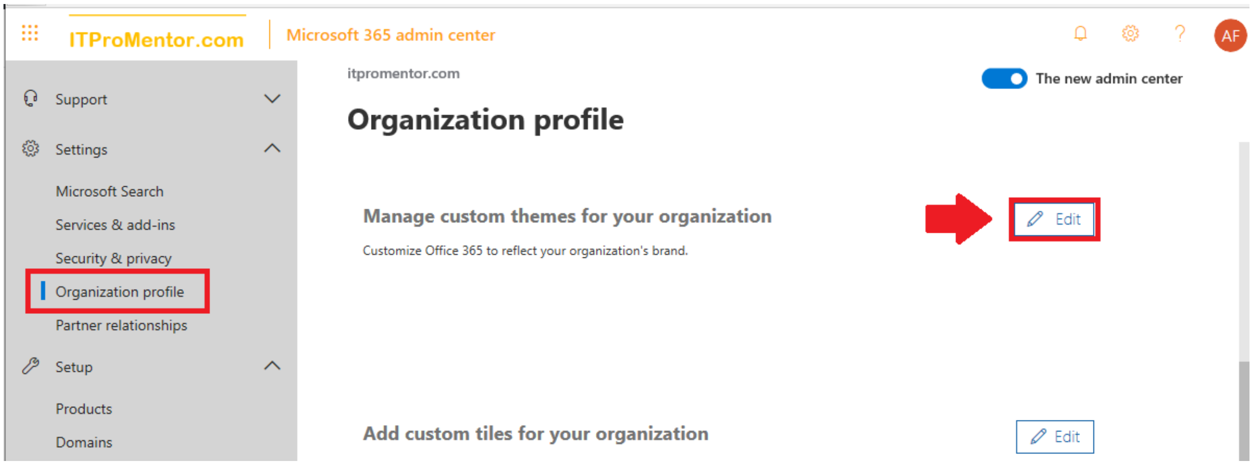
itpromentor.com

Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG or JPG

From Azure Active Directory admin center, click 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.



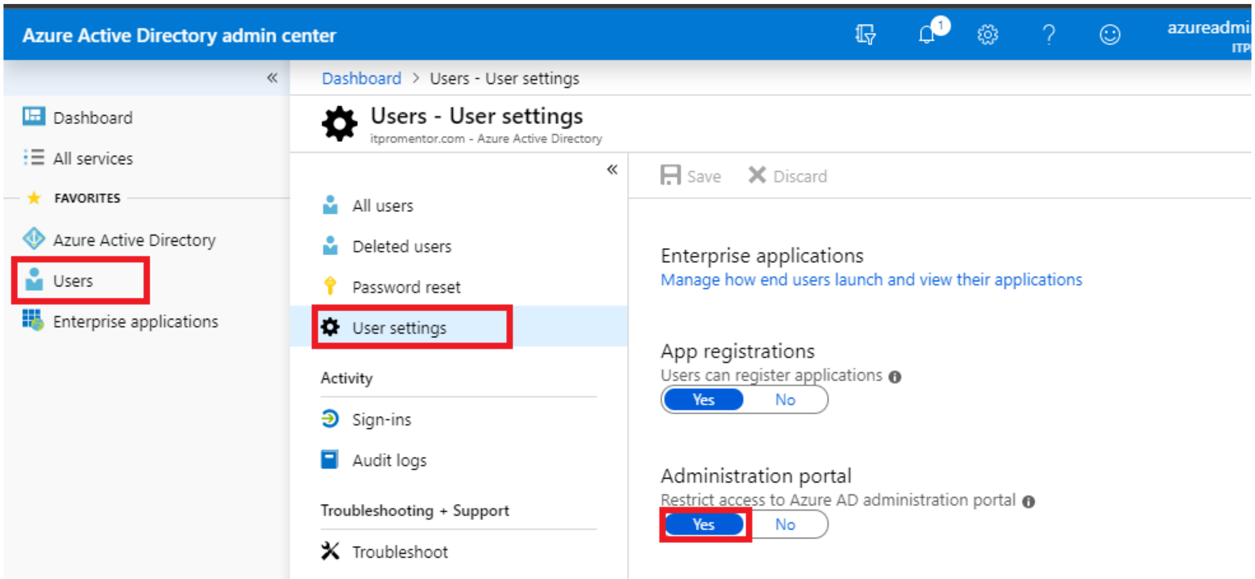
The logo you upload here will flow through into some other areas (e.g. the application access panel at myapps.microsoft.com), but there are other branding options in the 365 admin center, which are used as part of your "theme" in Office 365. **Settings > Organization profile**.



And neither of these customizations will flow through to the branding for encrypted emails, either—that is yet another *separate* configuration. I hope that Microsoft collapses these disparate areas into one single place someday.

☐ Restrict user access to the Azure AD admin portal

By default, any user can login to the Azure AD admin portal, and gain access to certain directory information that you may not want them to see. While they cannot change information, you may still want to limit this visibility, especially if an account becomes compromised.



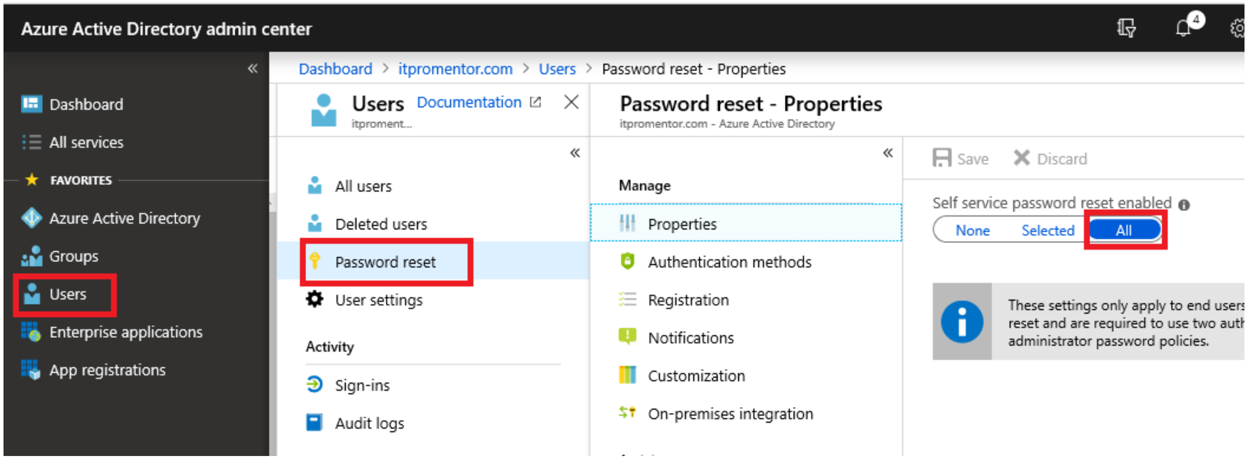
Enterprise applications
Manage how end users launch and view their applications

App registrations
Users can register applications: [✓ Yes] No

Administration portal
Restrict access to Azure AD administration portal: [✓ Yes] No

☐ Enable Self-service password reset (SSPR) for cloud accounts

Navigate to **Users > Password reset**. Pick **All** to enable SSPR for all users.



Self service password reset enabled: None Selected [✓ All]

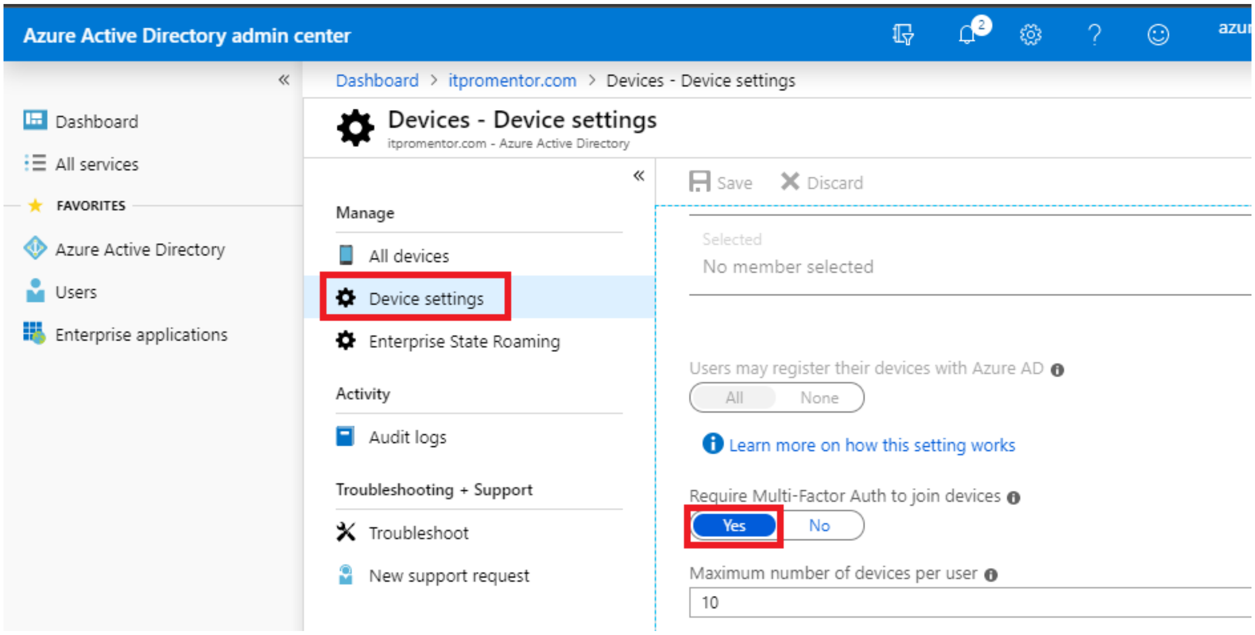
These settings only apply to end users
reset and are required to use two auth
administrator password policies.

You can also accomplish this in PowerShell. To connect to Azure AD, run [Connect-MsolService](). Then:

```
Set-MsolCompanySettings -SelfServePasswordResetEnabled $true
```

☐ Configure device settings for Azure AD joined devices

Go to Azure AD and navigate to **Devices**. Find **Device settings**. Scroll down to find **Require Multi-Factor Auth to join devices**. This setting applies to Windows 10 devices which are joining Azure AD.



Devices - Device settings
itpromentor.com - Azure Active Directory

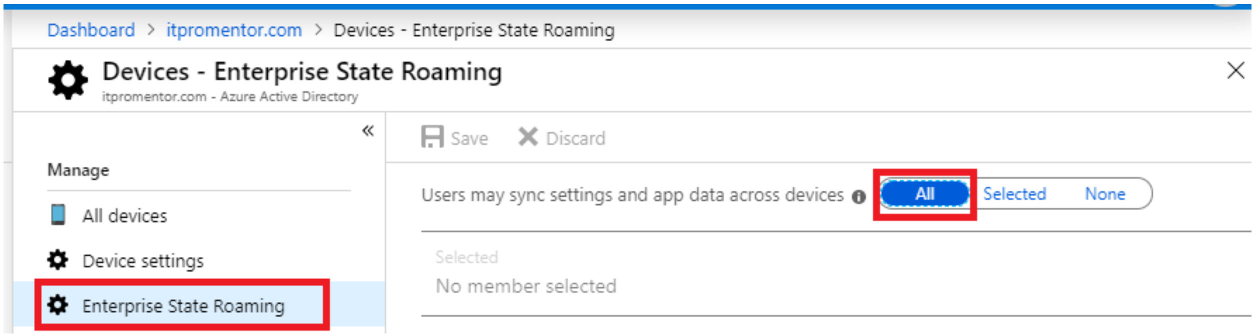
Selected
No member selected

Users may register their devices with Azure AD: All None

Require Multi-Factor Auth to join devices: [✓ Yes] No

Maximum number of devices per user: 10

While you're in here click on **Enterprise State Roaming**. Enable this setting for **All** users. Being able to sync settings across devices makes for a better end user experience and easier deployments.



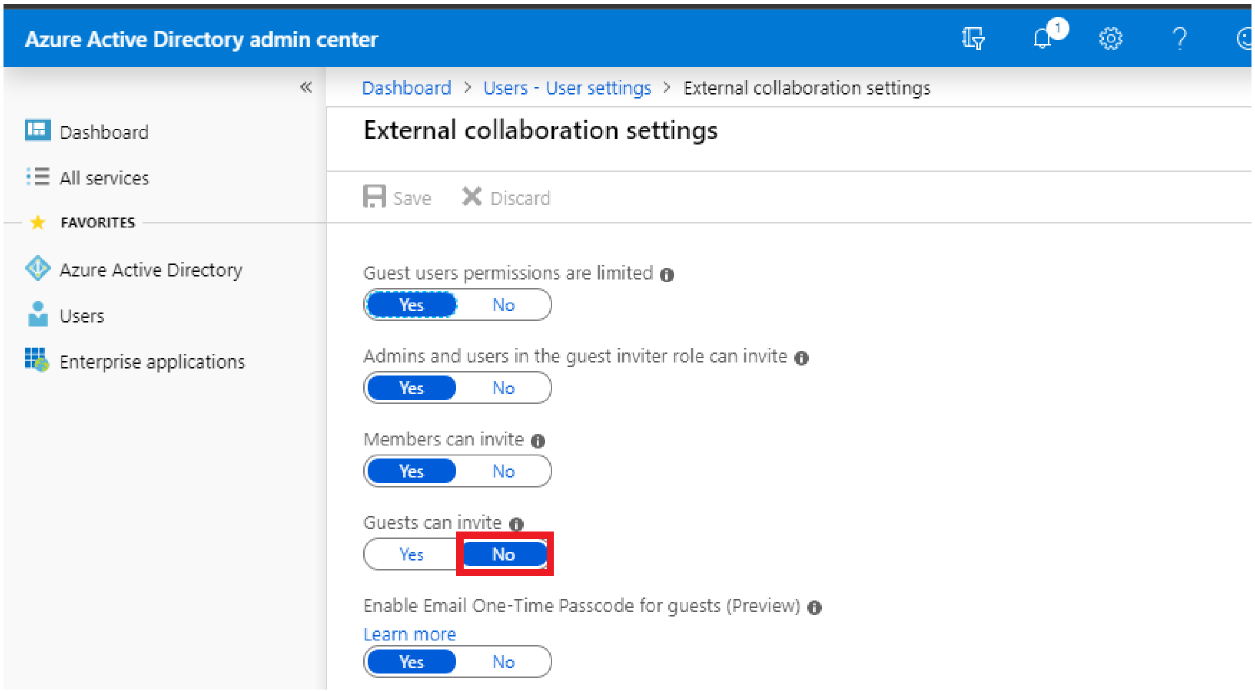
Devices - Enterprise State Roaming
itpromentor.com - Azure Active Directory

Users may sync settings and app data across devices: [✓ All] Selected None

Selected
No member selected

☐ Configure external collaboration settings

You can get more granular with your external collaboration settings at the service level (e.g. SharePoint admin center), but there is one setting I want to draw your attention to, and this would impact all services globally: **Users > User settings > External collaboration settings**.


Azure Active Directory admin center
Dashboard > Users - User settings > External collaboration settings
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Save
Discard
Learn more

External collaboration settings

Guest users permissions are limited: [✓ Yes] No

Admins and users in the guest inviter role can invite: [✓ Yes] No

Members can invite: [✓ Yes] No

Guests can invite: Yes [✓ No]

Enable Email One-Time Passcode for guests (Preview): [✓ Yes] No

Guests are users outside of the organization who have been invited to collaborate on resources. Most people are happy to share certain content with partners and customers outside of their own organization, but very rarely do they want those people turning around and sharing out or inviting *other guests* to that same content.

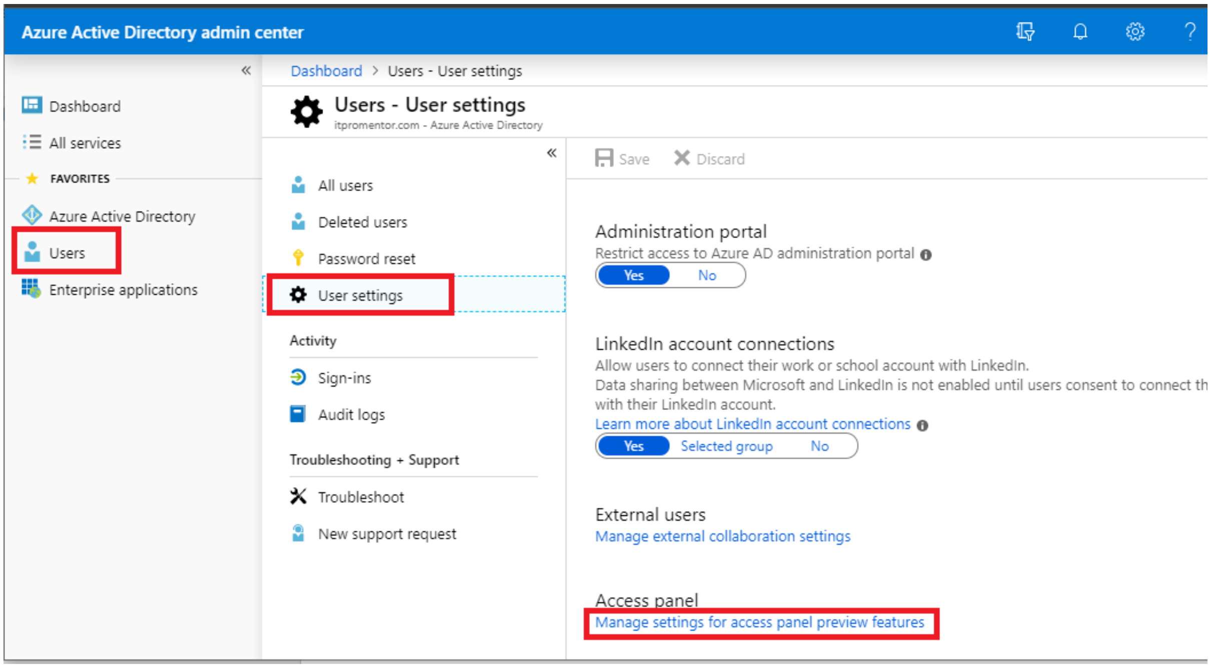
This may not always be true for every business, but it very often is the preferred configuration. In fact, most people assume the default behavior would be similar to this experience, and don't realize the opposite is on by default.

Note: On this page, also take note of Enable Email One-Time Passcode for guests (Preview). When this goes to General Availability, it will make life easier for guests who do not have a Microsoft account.

□ Enable combined registration of MFA and SSPR

To craft a better end-user experience, it is possible to combine the registration of Multi-Factor authentication with Self-service password reset (so that users only have to provide this information once for both services on their first login). This feature is in preview at the time of this writing.*

From **Users > User settings**, choose **Manage settings for access panel preview features**.



Users - User settings
itpromentor.com - Azure Active Directory

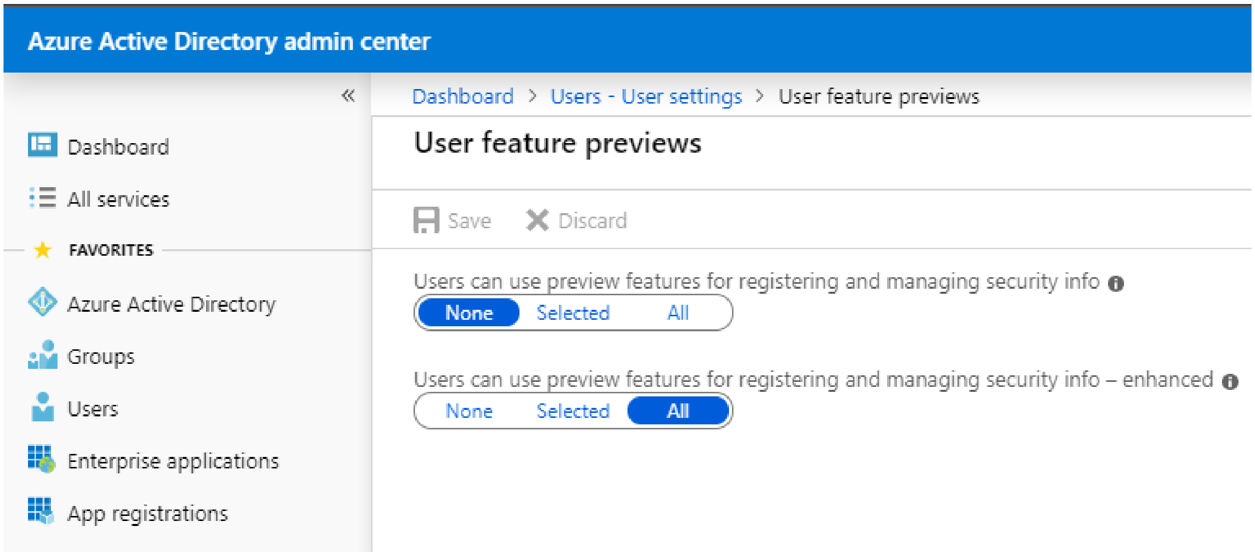
Administration portal
Restrict access to Azure AD administration portal
[✓ Yes] No

LinkedIn account connections
Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect th
with their LinkedIn account.
Learn more about LinkedIn account connections
[✓ Yes] Selected group No

External users
Manage external collaboration settings

Access panel
Manage settings for access panel preview features

Then, simply select **All** under **Users can use preview features…** Finally, **Save.** If you have two versions of this option present in your tenant, choose the one that says “enhanced” at the end.



User feature previews

Users can use preview features for registering and managing security info
[✓ None] Selected All

Users can use preview features for registering and managing security info – enhanced
None Selected [✓ All]

The next login via the web portal should prompt users if they haven’t yet setup MFA/SSPR. Otherwise, you can send users to this page to setup their security info: https://aka.ms/setupsecurityinfo

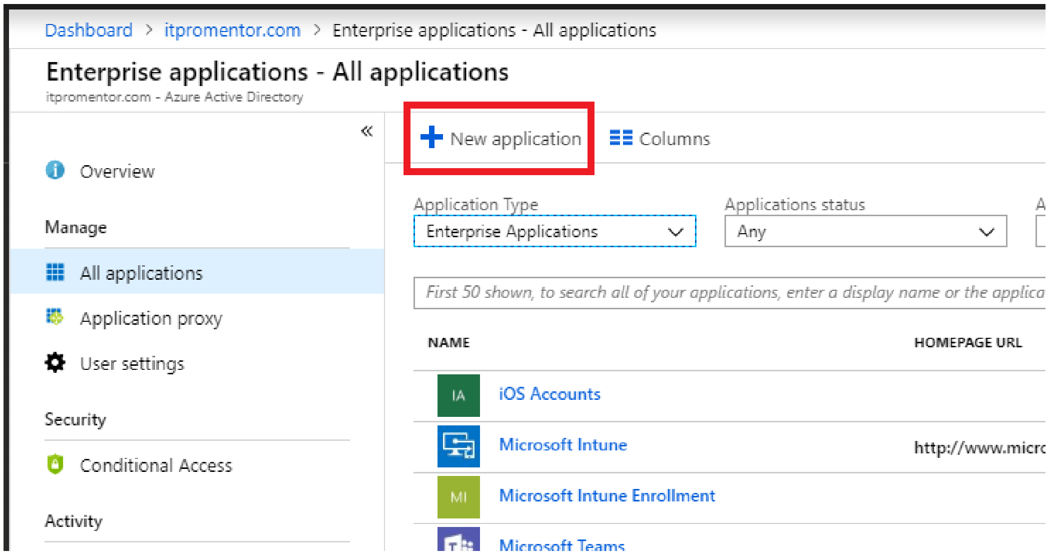
**Note*: At the time of this writing, I still find that enabling this setting will cause the registration experience to “loop” a couple of times when users go to set it up. Sort of annoying, but still better than two disparate registration experiences that look like websites from 10 years ago.*

☐ Configure Enterprise applications

There is a lot of power in this feature and I often advocate for people to start using it more. I should probably even consider upgrading this item from “Optional” to “Recommended.” Even if you do not go as far as configuring Single Sign-On, just the exercise of assigning apps to users and groups is valuable in itself, since you will have a better overall picture and inventory of the apps in your organization.

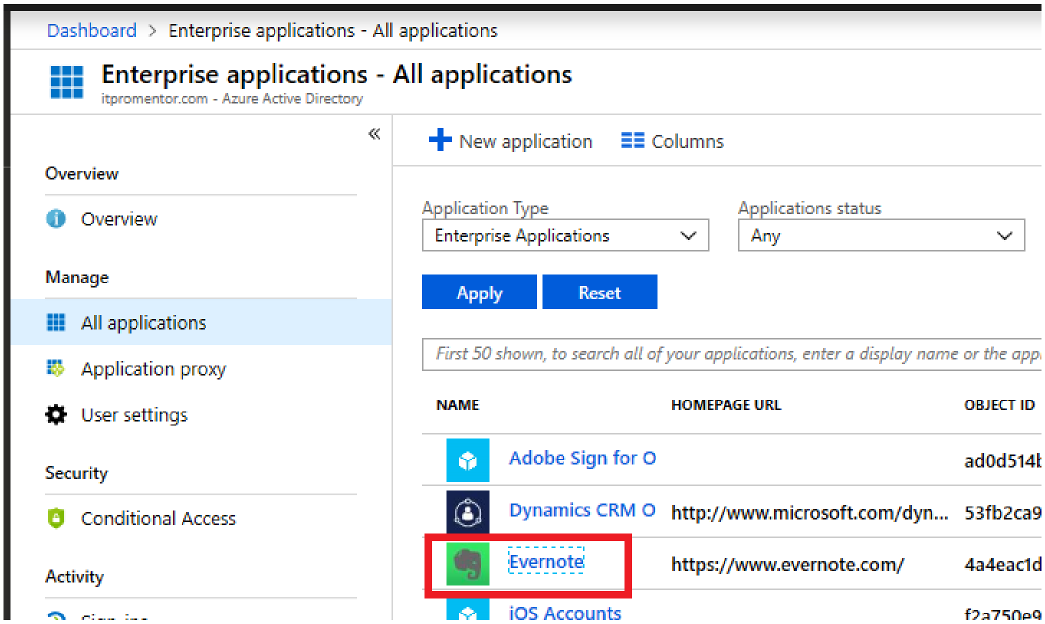
Once you actually *know* what you have, then it is much easier to take steps to *protect* the associated assets. If you need help identifying apps to begin with, look to your RMM, or use a tool such as Cloud app discovery (I will have an upcoming publication covering this in more detail).

To get started go to Azure Active Directory, find **Enterprise Applications > All applications**. Click **New application**. There a few thousand applications now available in the app gallery.


Dashboard > itpromentor.com > Enterprise applications - All applications
Enterprise applications - All applications
itpromentor.com - Azure Active Directory
«
Overview
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Activity
+ New application
Columns
Application Type
Enterprise Applications
Applications status
Any
A
First 50 shown, to search all of your applications, enter a display name or the applica

NAME	HOMEPAGE URL
IA iOS Accounts	
Microsoft Intune	http://www.micr
MI Microsoft Intune Enrollment	
Microsoft Teams	

By way of example only, I will search for and add an application from the gallery—in this case *Evernote*.



Enterprise applications - All applications

itpromentor.com - Azure Active Directory

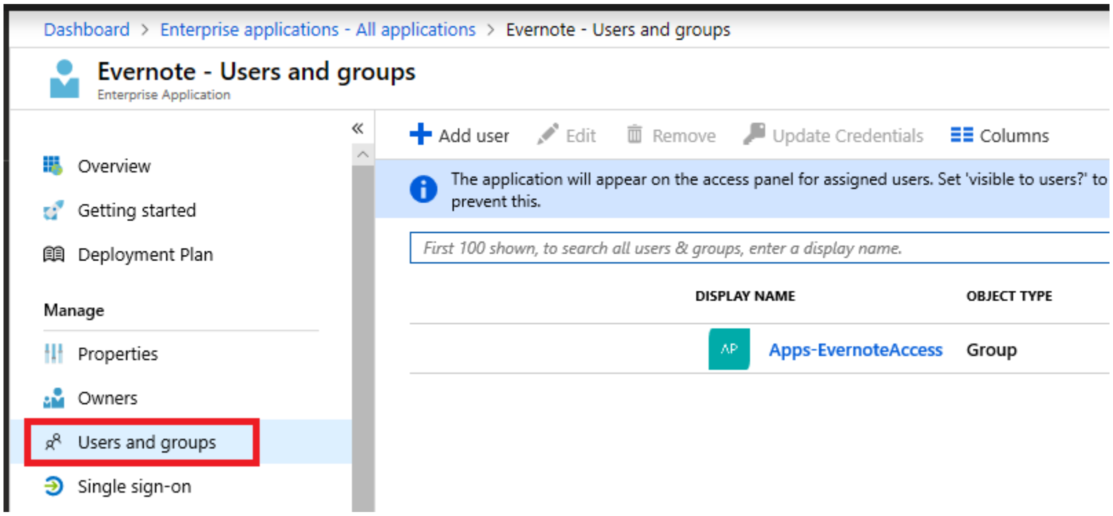
Application Type: Enterprise Applications

Applications status: Any

First 50 shown, to search all of your applications, enter a display name or the app

NAME	HOMEPAGE URL	OBJECT ID
Adobe Sign for O		ad0d514k
Dynamics CRM O	http://www.microsoft.com/dyn...	53fb2ca9
Evernote	https://www.evernote.com/	4a4eac1d
iOS Accounts		f2a750e9

Next, I can assign the application to individual users, or to a security group which I have created for this purpose. Click the application and find **Users and groups** to make your assignments.



Evernote - Users and groups

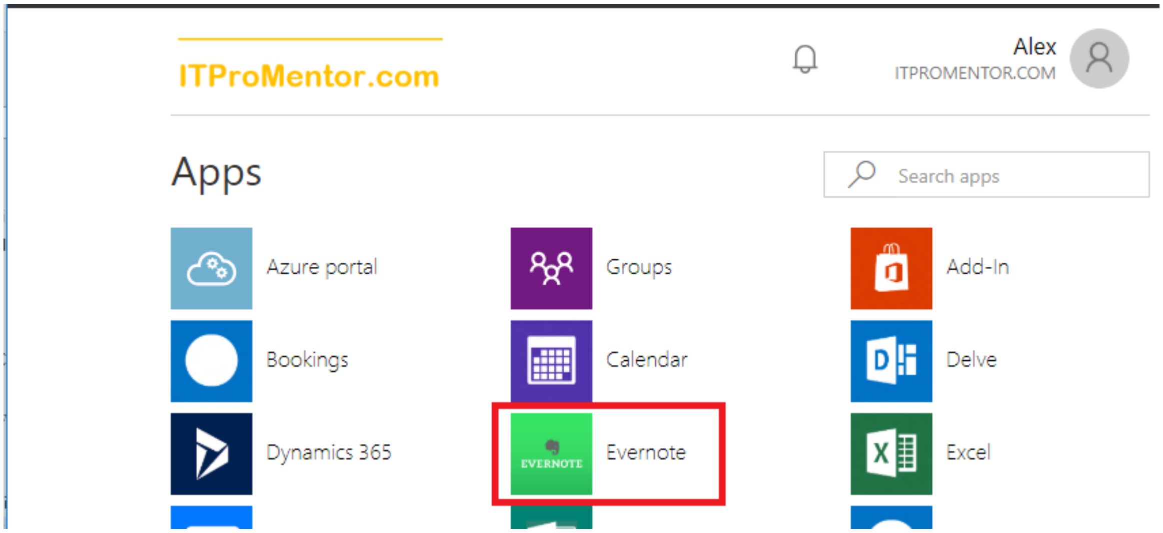
Enterprise Application

The application will appear on the access panel for assigned users. Set 'visible to users?' to prevent this.

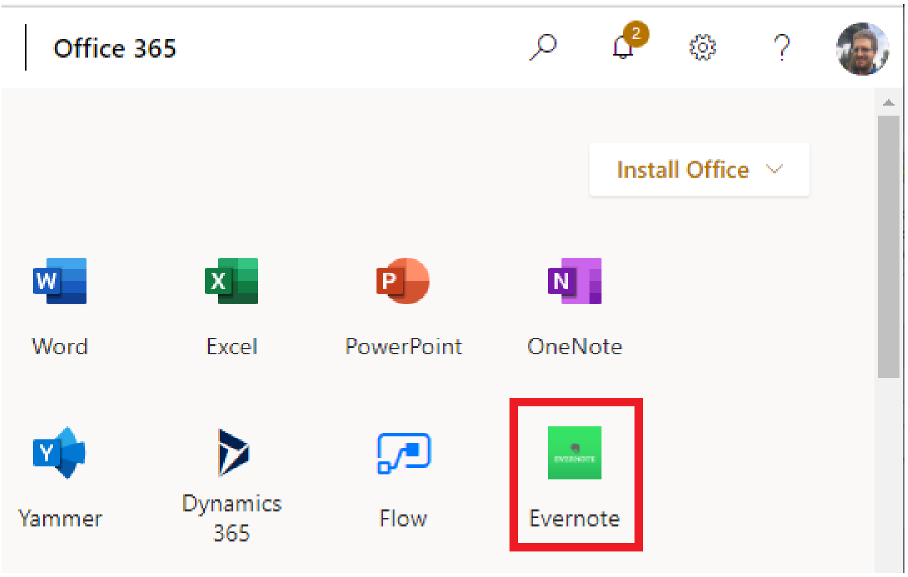
First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE
AP Apps-EvernoteAccess	Group

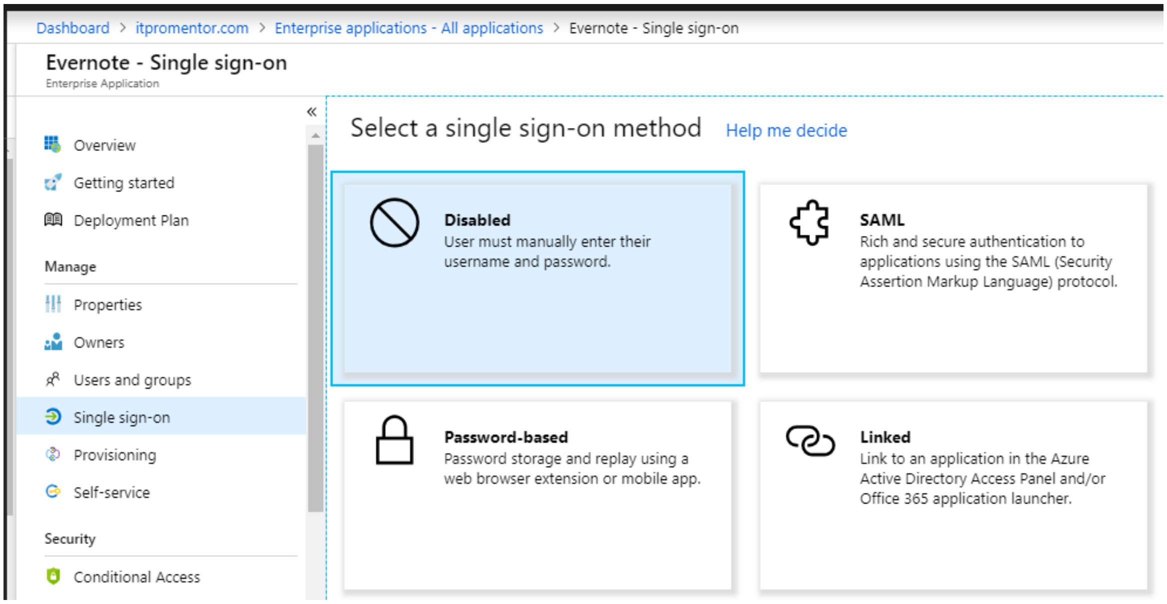
After you have configured your apps and assigned them to groups, your users will be able to access the applications via the Azure AD access panel located at https://myapps.microsoft.com



Enterprise apps can also be displayed in the app launcher for Office 365.



Now 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, and explained below.



Evernote - Single sign-on
Enterprise Application

Select a single sign-on method

Disabled
User must manually enter their username and password.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

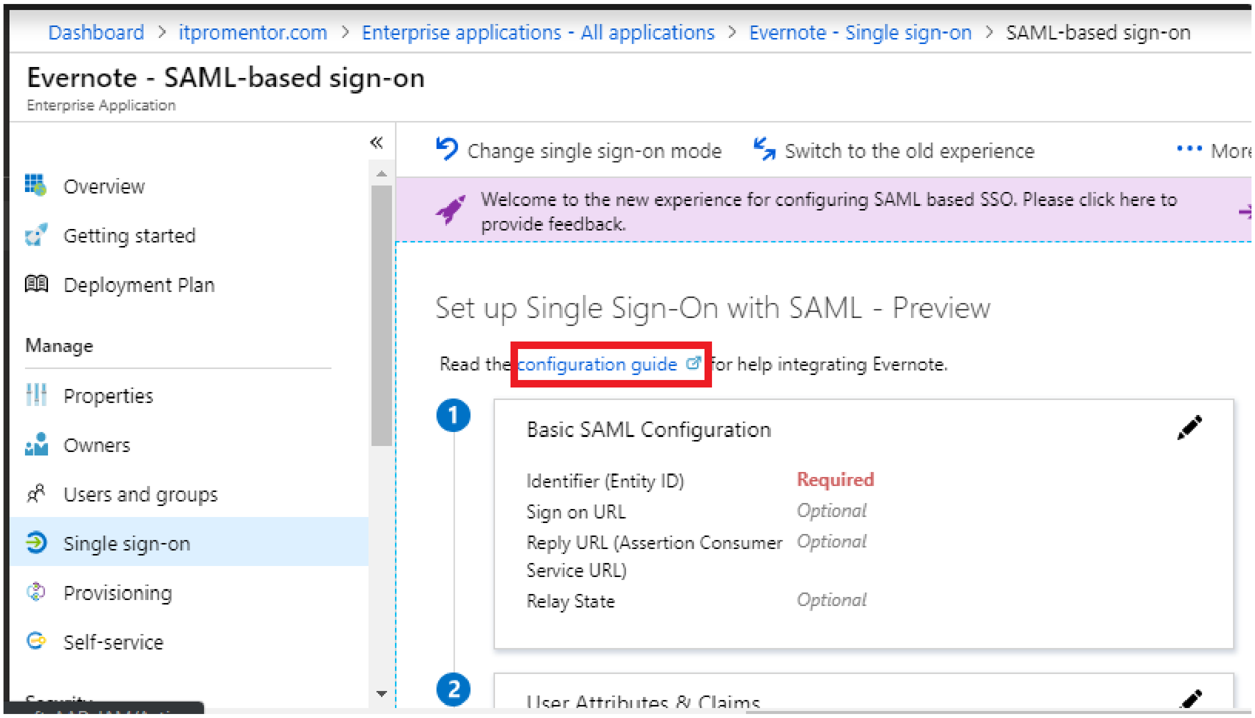
Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

SAML is the option you want. If the app supports SAML (Security Assertion Markup Language), that means it will be capable of “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.

The security benefits of SSO are just too great to ignore, since you can reduce the number of identities you manage and centralize the security logs in Azure AD. Plus, you can apply things like Conditional Access and MFA to the logon requests as well, just as you do with the Microsoft apps. 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.


Dashboard > itpromentor.com > Enterprise applications - All applications > Evernote - Single sign-on > SAML-based sign-on
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Self-service
Change single sign-on mode
Switch to the old experience
More

Evernote - SAML-based sign-on

Enterprise Application

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback.

Set up Single Sign-On with SAML - Preview

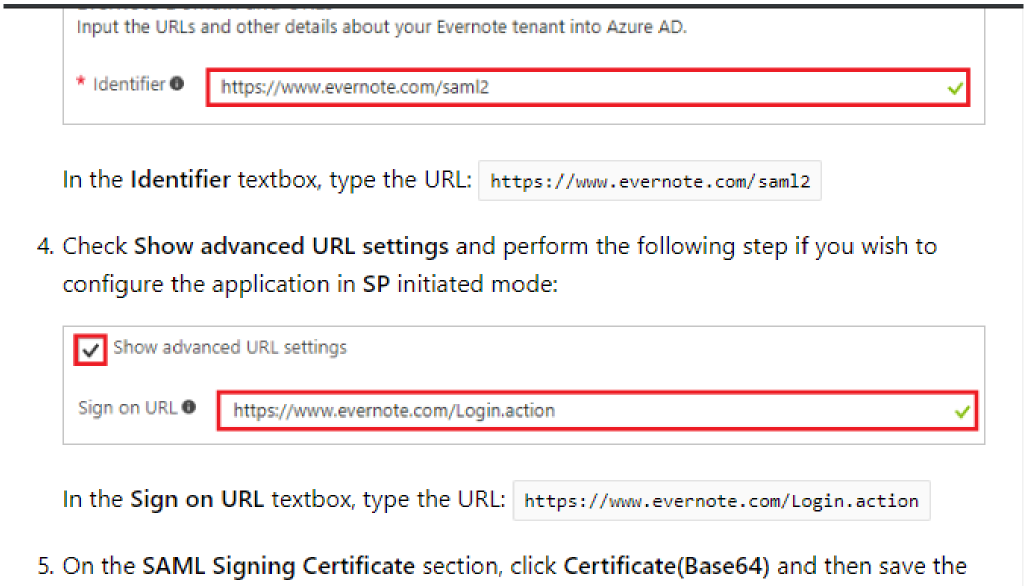
Read the configuration guide for help integrating Evernote.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Sign on URL	Optional
Reply URL (Assertion Consumer Service URL)	Optional
Relay State	Optional

2 User Attributes & Claims

In almost all cases where SAML is available, you will need to provide Azure AD and the third-party application 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: https://www.evernote.com/saml2

In the **Identifier** textbox, type the URL: `https://www.evernote.com/saml2`

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: https://www.evernote.com/Login.action

In the **Sign on URL** textbox, type the URL: `https://www.evernote.com/Login.action`

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

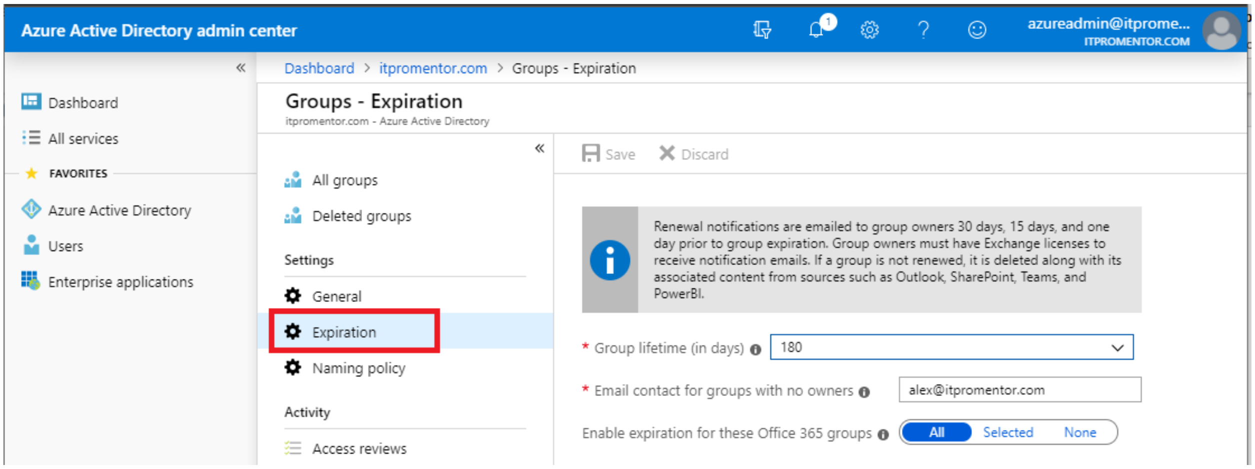
It is difficult to express just how important this Enterprise Application feature could be for your organization or practice. Even if you cannot configure true SSO with SAML to every one of your applications, just the fact that you can *track* application assignments to users alone is huge.

☐ Configure optional settings for Office 365 Groups

Most of the settings related to *Groups* are completely up to the preference of each organization. Browse them on your own to see what I mean. I will only call attention to two items related to groups, which impact many services in Office 365 such as Outlook, Teams, SharePoint and Planner.

The first is **Expiration**. Many groups that are created, for example via the Microsoft Teams application, are temporary in nature: they are stood up for an express purpose or project. When the project is wrapped, or if it never took off and instead fizzled, the group object and all of the associated resources still exist. Therefore, it is a good practice to enable an expiration policy, which notifies the group owner(s) regularly about the upcoming expiration of their groups, and gives them the chance to extend the life of the group, or let it fade into dust via expiration (read: deletion).

Go to **Azure Active Directory > Groups > Expiration**. You can define a Group lifetime (in days), as well as an email contact for groups without owners (e.g. Owners who have since departed the organization).



Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

* Group lifetime (in days): 180

* Email contact for groups with no owners: alex@itpromentor.com

Enable expiration for these Office 365 groups: [✓ All] Selected None

The second consideration is: does the organization care to **restrict *who* can create Office 365 Groups**? If so, then follow the instructions in this article. Just know that this action has impacts on end-user experience. Standard users will not be able to create Teams, Planner groups and so forth. Generally, I recommend leaving this wide open rather than closed or restricted. Instead, I suggest that you lean on the expiration policy described above, as well as the **Naming policy** (and don't forget retention policies), to manage concerns related to "Group clutter."

Again most of this stuff is totally optional and like many settings, has no real bearing on this "baseline" conversation. Which brings me around to the last point…

☐ Other Azure AD settings (that we didn't cover)

To address the elephant left standing in the room, at the end of this guide: hybrid configurations…. I did not include hybrid configurations on purpose. The major consideration for hybrid would be to enable directory synchronization and decide on SSO options.

In general, I believe that small businesses should be taking steps toward a "cloud-only" configuration (trust me), and not relying on hybrid moving into the future, as this actually presents more risks and complications than benefits in my opinion. However, if you are stuck on hybrid, I recommend the following (bullet point advice only):

- **Password Hash Sync:** is the only right choice, and don't try do something fancier than that. Oh, and get rid of ADFS is that is still around. Yuck.
- **Password policy on-prem:** Make sure you actually have a good password policy in place here, or you just end up bringing your crappy practices into the cloud (no bueno). You can improve password security and the end-user experience using password-write back for self-service password reset, and via enabling password protection for on-premises servers.
- **Limit the scope of your sync**: Whether you filter via OU, account attributes or both, just do not let the clutter from your on-premises environment come along for the ride. The fewer accounts you have to manage, the better.
- **Disable any shared accounts**: You should not be signing into shared accounts interactively. Generally speaking, you delegate access to resources (e.g. shared mailbox) to other user accounts, which have "real" people behind them.
- **Consider ditching distribution lists**: When you move to Office 365, you may want to get rid of traditional DL's in favor of Office 365 Groups, which come with a lot more benefits. You need to remove the lists from on-premises AD and re-create them in the cloud as Groups instead.
- **Get to know what changes where and when**: Some changes have to be made on-prem (new accounts, name change, new alias, hide from address list, enable archive, etc.) while others, like delegations, forwarding, etc., are still managed in the cloud. It's dumb. One more reason to get off the legacy hybrid stuff.
- **You still need global admin account in the cloud**: We covered this.
- **There are probably others**: Like I said, hybrid is not known for simplicity. I think it's a great tool for onboarding, but then it's better to get rid of it and go cloud-only.

I also mentioned that I'd be leaving out Azure AD Premium P2 features. Basically the only thing to consider there, and it would be recommended for those with the SKU, is Identity Protection. But my focus is the SMB/SME, the majority of whom will stick to the Microsoft 365 Business plan (which does not include Azure AD Premium P2).

There exist many other Azure AD settings and options which we did not cover. For example, some people get bent out of shape over user account enumeration. But don't turn that off, as it breaks stuff and it won't protect you that much anyway. And I could go on commenting on others, and why I didn't address them here. But at 20 pages, I've said enough already.

Again, this is meant as a baseline for best practices, and it is not intended to be a comprehensive overview of every setting. So many options are completely up to the preference of an organization; it would be volumes to write into that much detail (and a lot of it won't make a difference when it comes to security anyway).