Microsoft 365: Azure Active Directory Setup Checklist

Alex Fields, ITProMentor.com

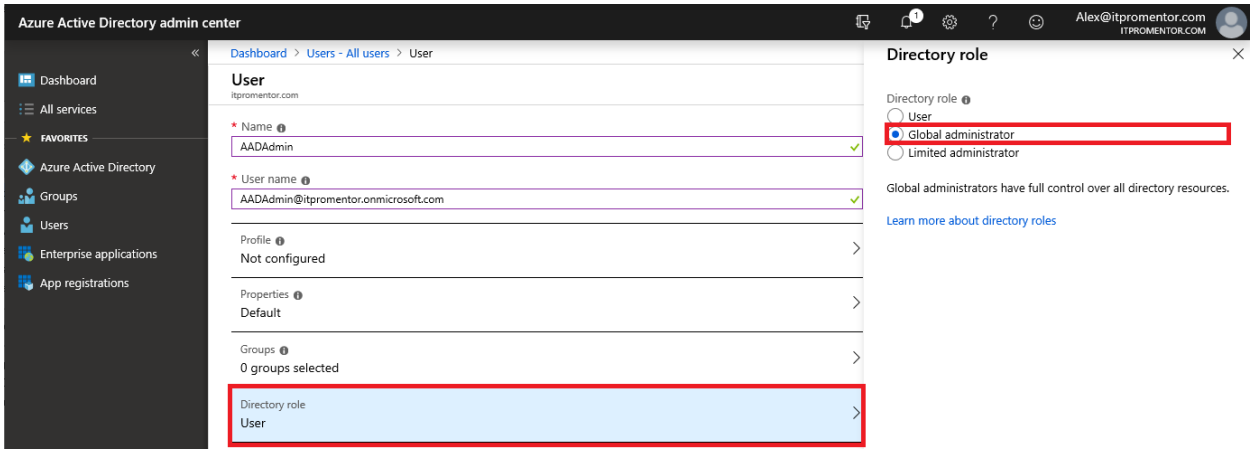
This resource is intended to be used as a guideline for provisioning new Microsoft 365 tenants according to best practices. After the checklist, screenshots and explanation of each item will be provided. Recommended implementation order:

Checklist item	Notes	Importance
Create an emergency access global admin account	Cloud-only account in the "onmicrosoft.com" domain; long (e.g. 100 character) password. Excluded from all CA policies.	**Critical**
Enable Conditional access baseline policies*	Azure AD > Conditional access • Especially: *Require MFA for admins* • Also refer to this guide for further Conditional access recommendations.	**Critical**
Disable users consent to apps requesting permissions	Enterprise Applications > User settings • Users can consent to apps… (**No**)	**Critical**
Adjust MFA Service Settings	Multi-Factor Authentication > service settings • Do not allow users to create app passwords • Add Trusted IP's (if applicable)	**Highly Recommended**
Restrict user access to the Azure AD admin portal	Users > User settings • Restrict access to Azure AD… (**Yes**)	**Highly Recommended**
Enable Self-service password reset (SSPR) for cloud accounts	Users > Password reset • Self-service password reset enabled (**All**)	**Highly Recommended**
Configure device settings for Azure AD joined devices	Devices > Device settings • Require Multi-Factor Auth to join devices	**Highly Recommended**
	Devices > Enterprise State Roaming • Users may sync settings and app data across devices (**All**)	**Optional**
Configure optional external collaboration settings	Users > User settings • Manage external collaboration settings > Guests can invite (**No**)	**Optional**
Enable combined registration of MFA and SSPR*	Users > User settings > Access panel • Manage settings for access panel preview features > Users can use preview… (**All**)	**Optional**
Configure optional settings for Office 365 Groups	• Groups > Settings > Expiration • Restrict who can create Office 365 Groups	**Optional**

*Still in preview at the time of this writing. Use preview features at your own risk.

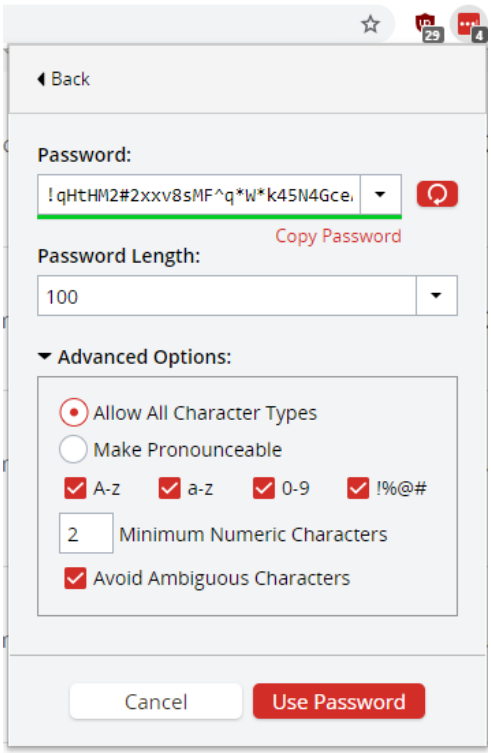
Create an emergency access global admin account

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



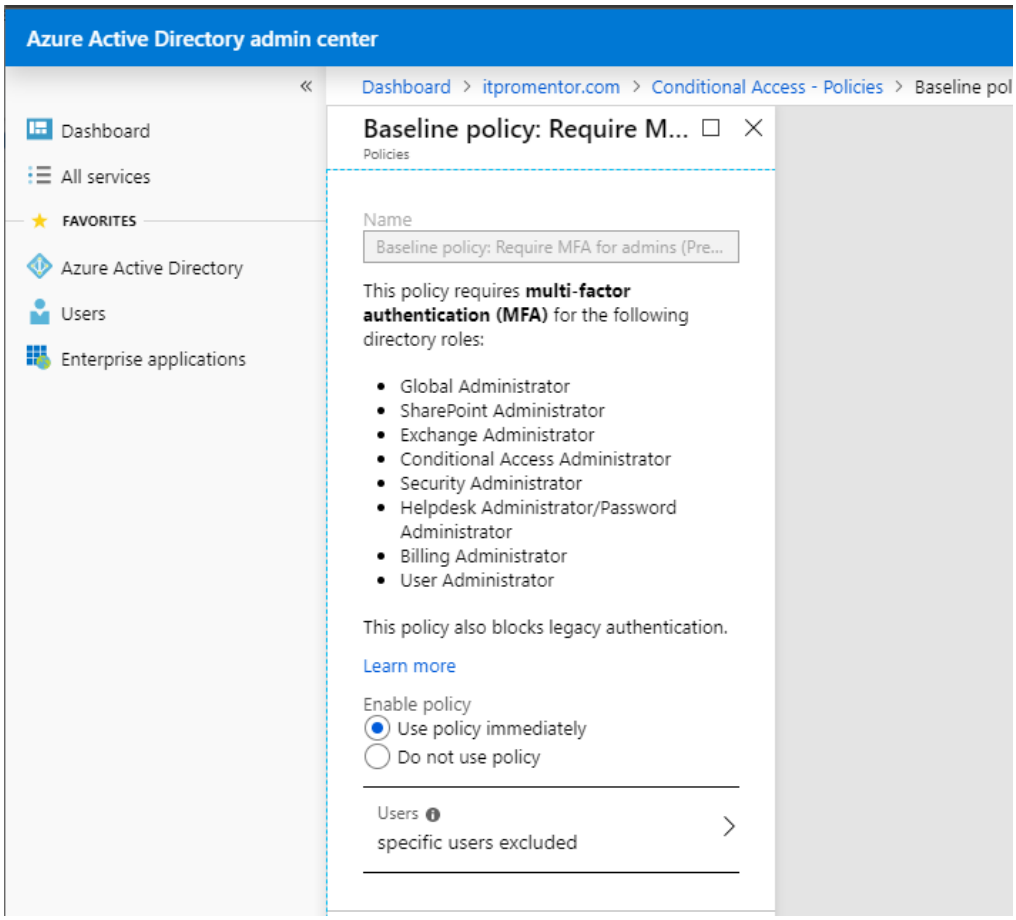
Assign name & username (use the "onmicrosoft.com" domain). Pick **Directory role > Global administrator**. **Create** the account, noting the temporary password.

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).



Enable Conditional access baseline policies

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).

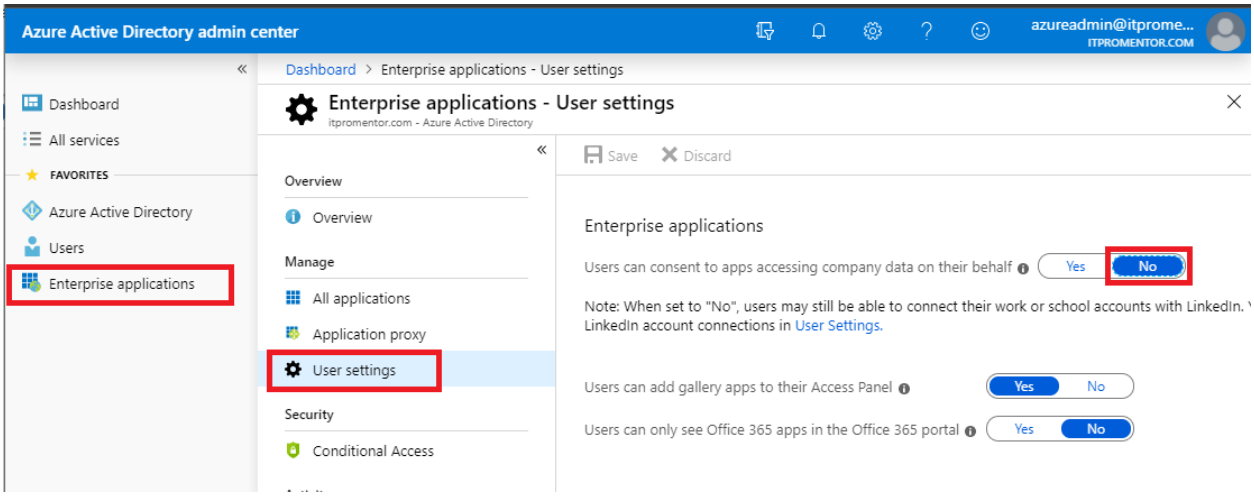


Users will be prompted to register their security information for Multi-Factor Authentication once they are compelled to perform MFA via a Conditional Access policy. This applies to the baseline policies entitled “Require MFA for admins” and “End user protection,” as well as any custom policies that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

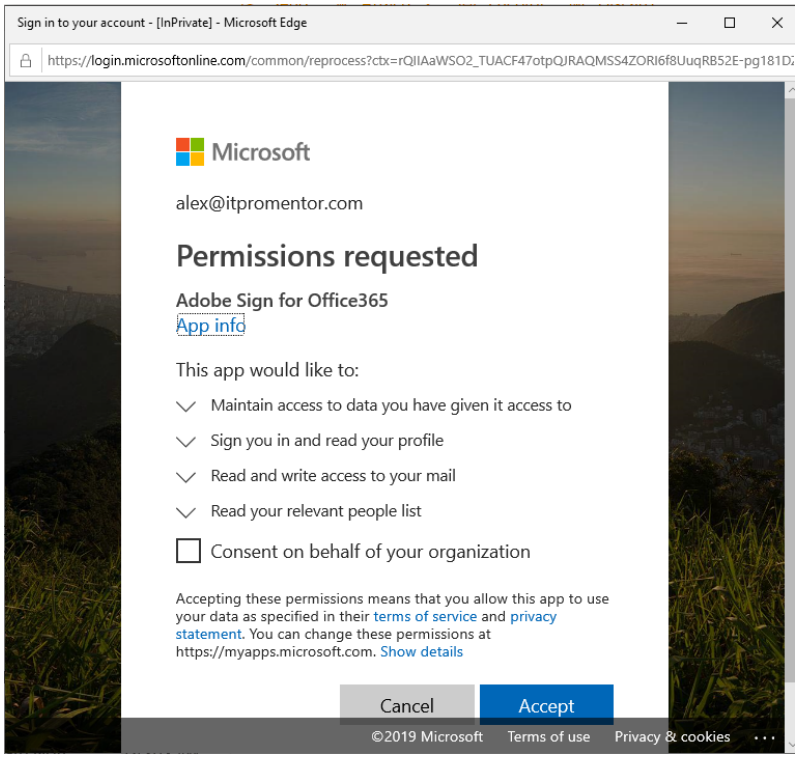
For additional guidance on Conditional access policies, refer to this resource.

Disable users' ability to consent 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**.



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.



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).

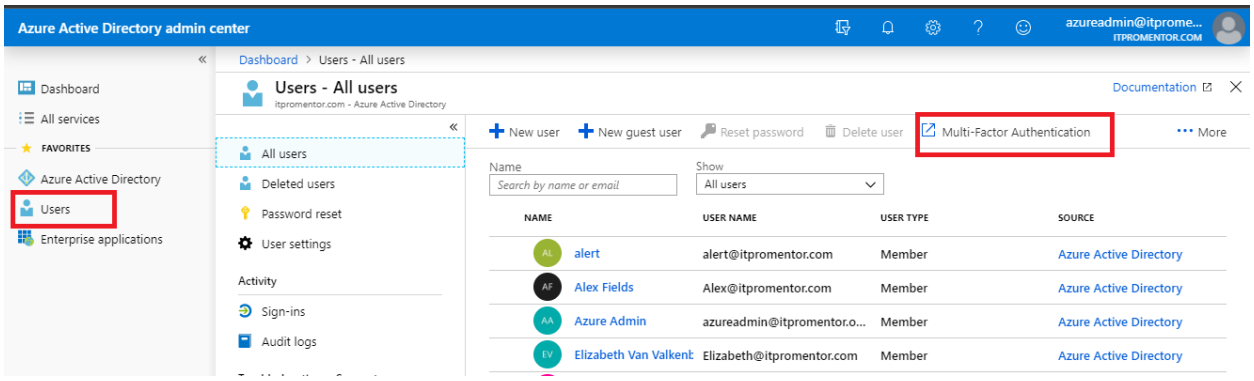
This same setting is available in PowerShell. To connect to Azure AD, run Connect-MsolService. Then:

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

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

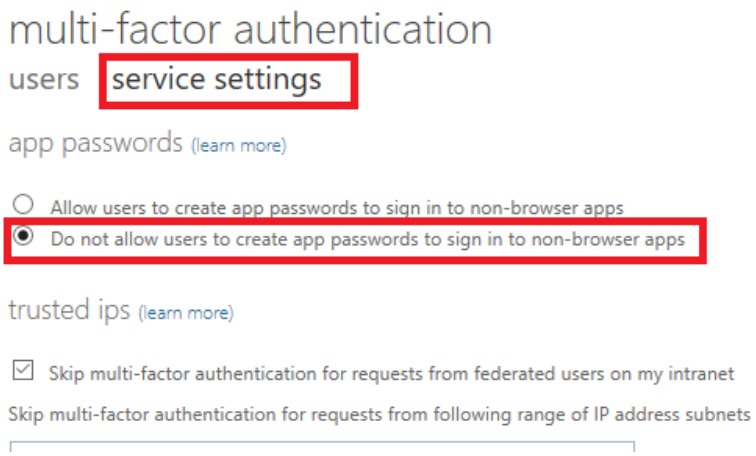
Adjust MFA Service Settings

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



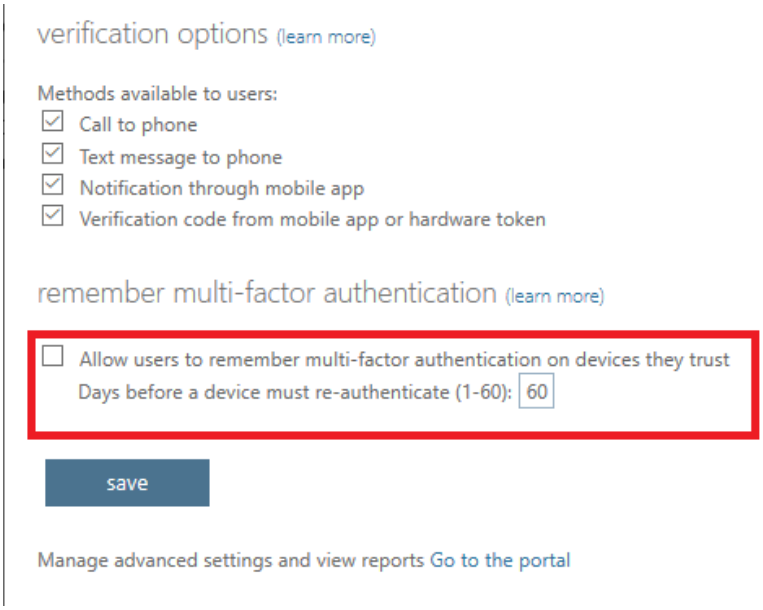
Click on **service settings** at the top of the screen, and make these adjustments:

- **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.



Scroll down further. Note that mobile apps and hardware tokens are considered more secure than SMS text messages or phone calls. 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.

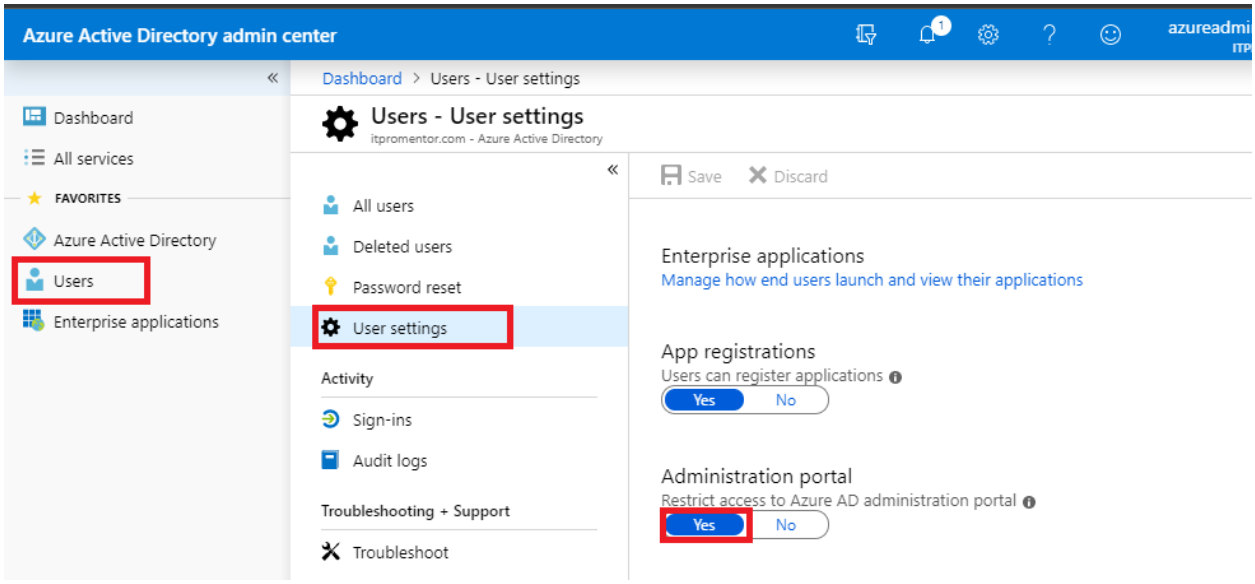
Instead, it is better to leverage Conditional access to 1) Require device compliance, and 2) *Always* require MFA on unmanaged devices. More on Conditional access soon.



Save your selections. You *could* enable accounts for MFA individually even now, however we can also improve the end-user registration experience by setting up self-service password reset at the same time.

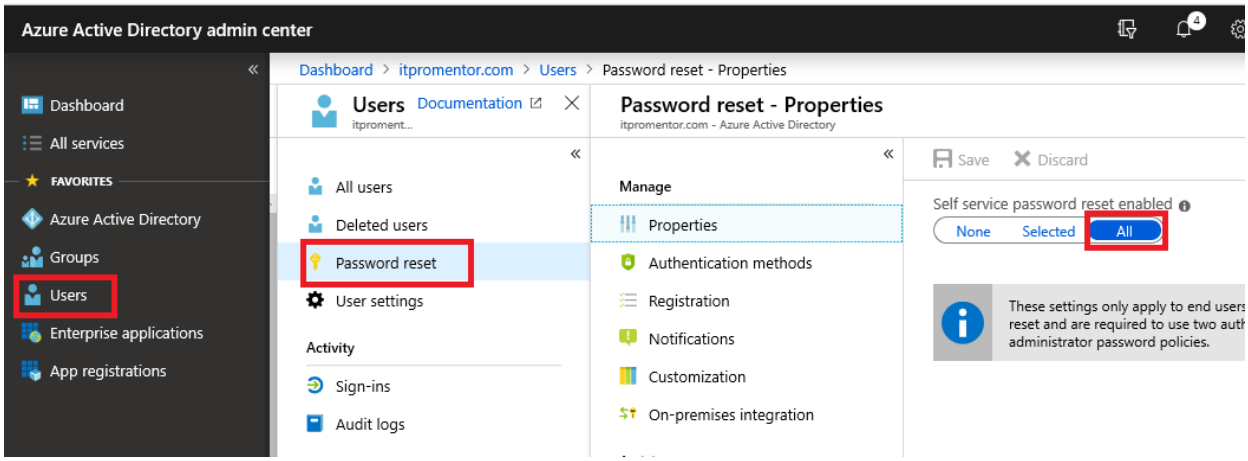
Restrict user access to the Azure AD admin portal

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.



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

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

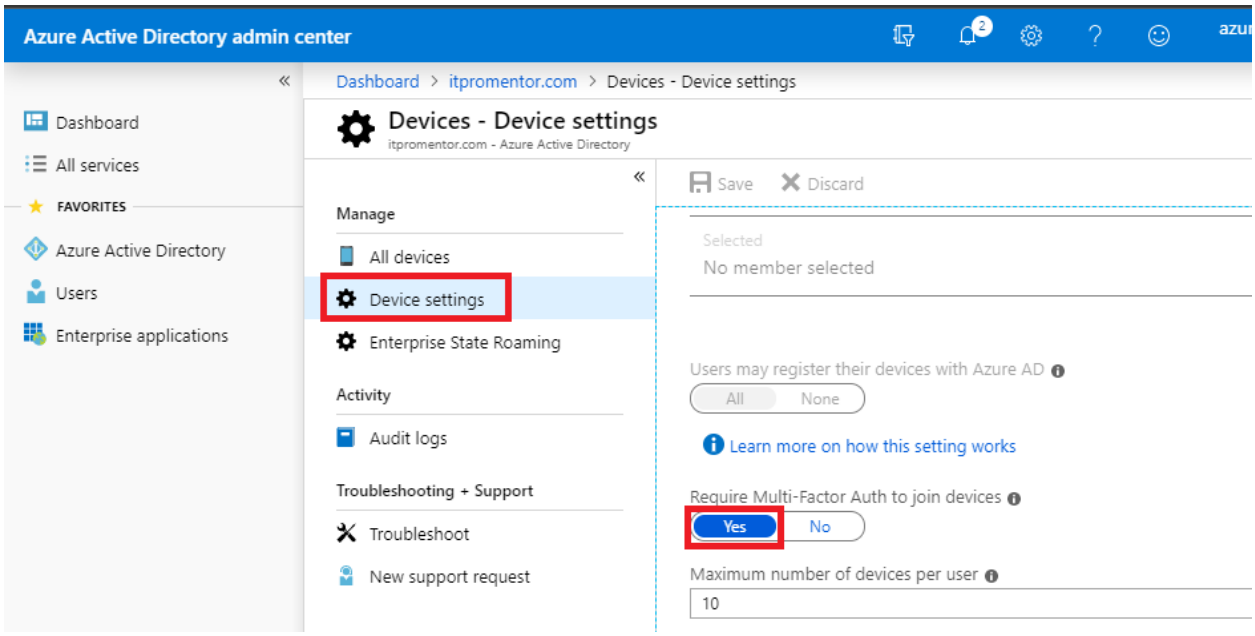


You can also accomplish this in PowerShell. To connect to Azure AD, run Connect-MsolService. Then:

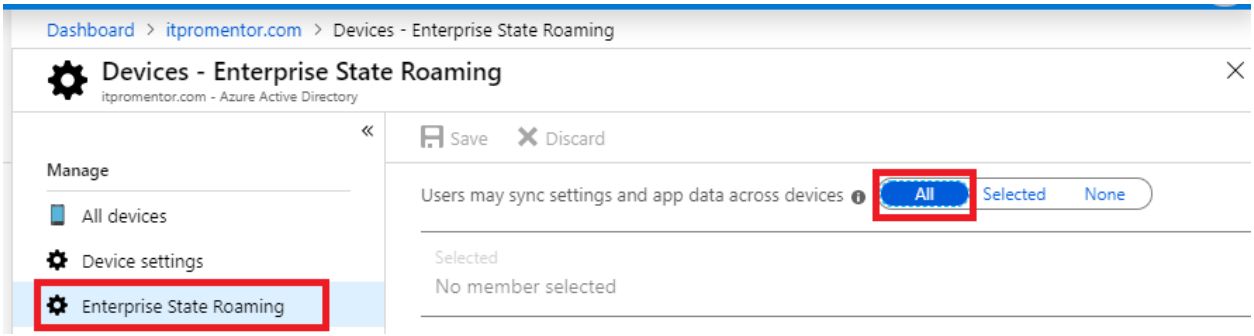
```
Set-MsolCompanySettings -SelfServePasswordResetEnabled $true
```

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.

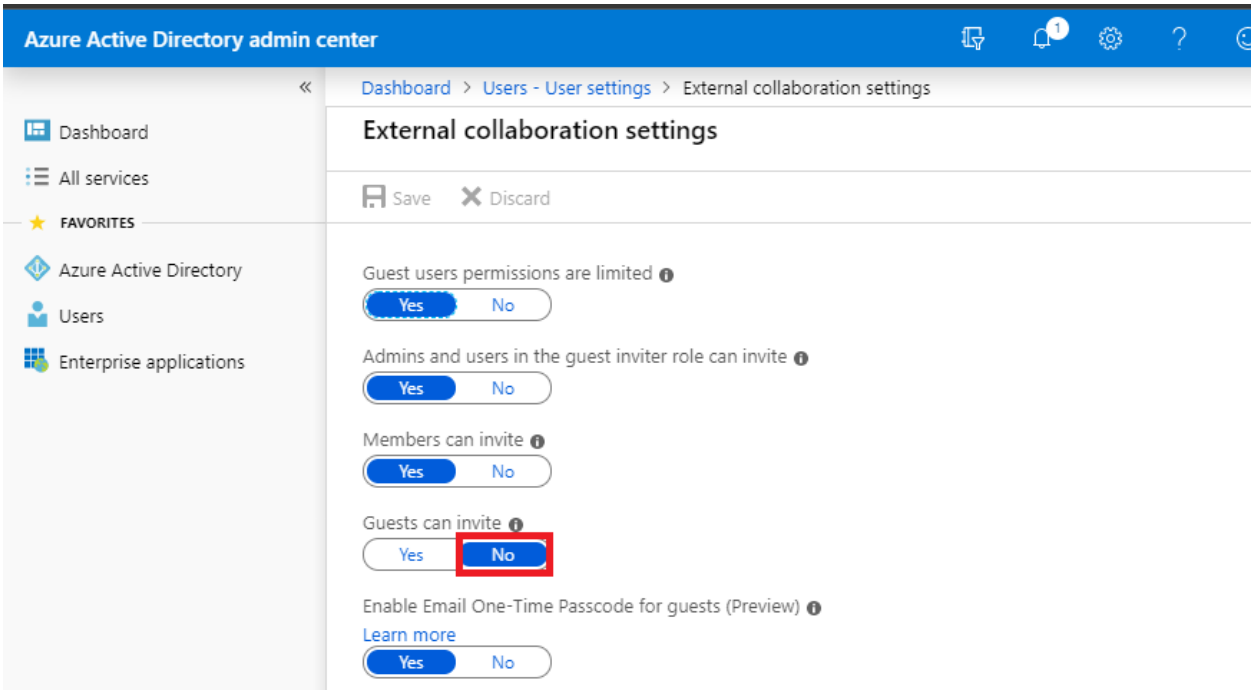


Next click on **Enterprise State Roaming**. Enable this setting for **All** users. Being able to sync settings across Windows 10 devices is supported on every Microsoft 365 subscription, including Business.



Configure optional 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**.



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.

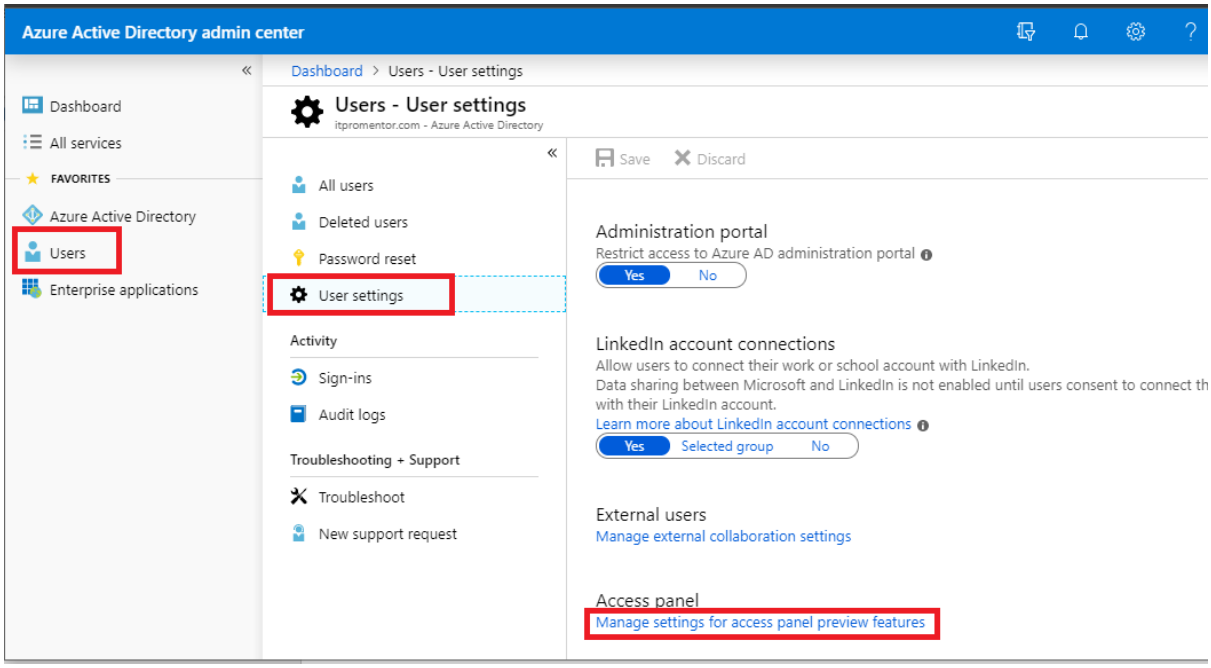
This may not always be true for every business, but it very often is the preferred configuration. In fact, most people assume the default behavior would be similar to this experience, and don't realize the opposite is on by default.

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.

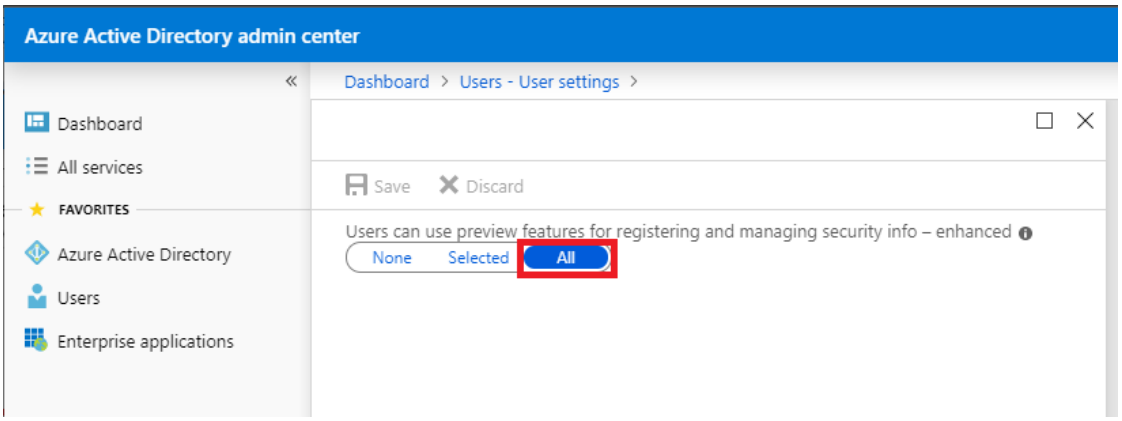
Enable combined registration of MFA and SSPR

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**.



Then, simply select **All** under **Users can use preview features…** Finally, **Save.**



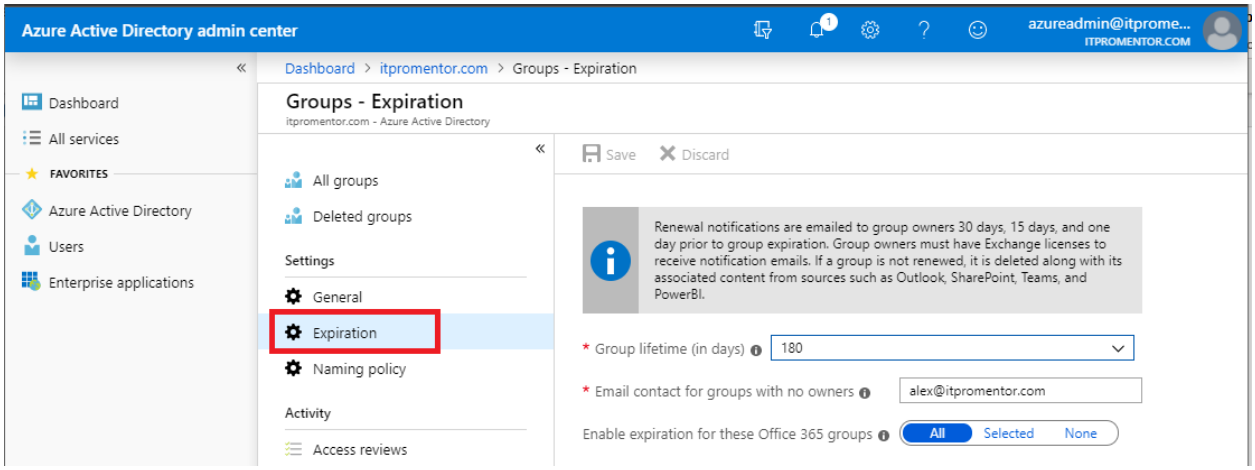
<u>Note</u>: At the time of this writing, I still find that enabling this setting will cause the registration experience to "loop" a couple of times the first time you go to set it up. Sort of annoying, but still better than two disparate registration experiences that look like websites from 10 years ago.

Configure 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).



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 retention policies, to manage Group clutter.

It is also possible to place restrictions around the naming of groups, under **Naming policy**. It 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)

There exist many other Azure AD settings which we did not cover. Again, this is meant as a baseline for best practices, and it is not intended to be comprehensive. So many options are completely up to the preference of an organization—External sharing, self-service group settings, app registration, etc.

Also keep in mind that some settings overlap with items that we can define at the service level, for example in Teams, SharePoint or OneDrive. I will be publishing separate guides detailing each major service, in time.