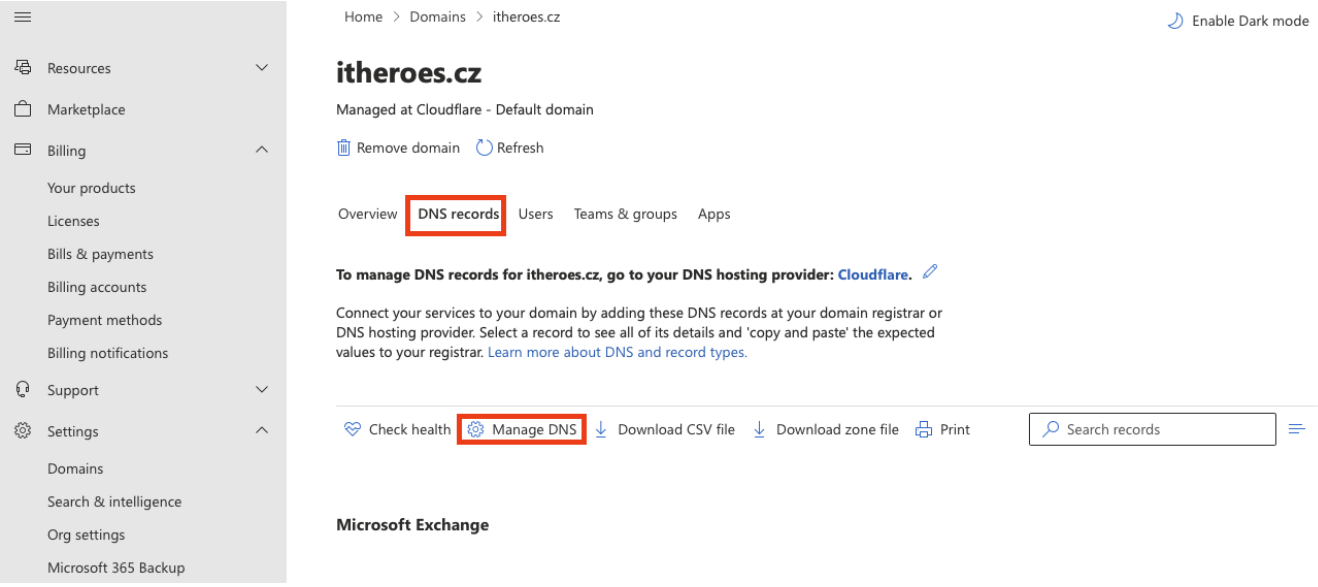
[ICT] GROUP

Nastavení DNS záznamů

Pro nastavení DKIM a SPF si otevřete
https://admin.microsoft.com/Adminportal/Home#/Domains

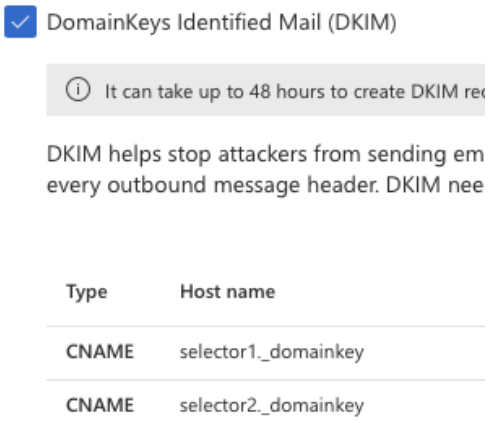
Rozklikněte si doménu, kterou chcete upravovat. Klikněte na DNS records (DNS záznamy) a poté klikněte na Manage DNS (Spravovat DNS)



Otevřete si správu domény (u koho máte doménu zaregistrovanou) a nastavte hodnoty, které vám Microsoft vygeneroval a zadejte je do pole přidat DNS záznam. Dejte si pozor, jakž typ záznamu to je!

Type	Host name	Point to address or value	TTL
MX	@	0 itheroes-cz.mail.protection.outlook.com	1 Hour
TXT	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	autodiscover	autodiscover.outlook.com	1 Hour

Poté odrolujte níže a klikněte na Advanced Options a zaškrtněte DKIM

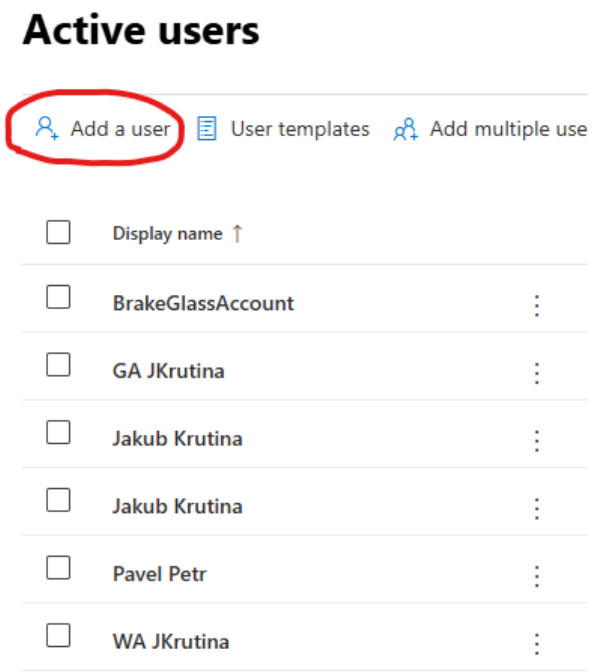


Poté co máte tyto věci nastavené, tak si vygenerujte DMARC pomocí easydmarc, nebo Dmarcian (nebo dalších služeb). DMARC vypadá přibližně takto: **v=DMARC1;p=quarantine;sp=quarantine;pct=100;rua=mailto:example@example.eu;ruf=mailto:example@example.eu;ri=86400;aspf=s;adkim=s;fo=1;**

Poté si všechno zkontrolujte přes MXTOOLBOX.

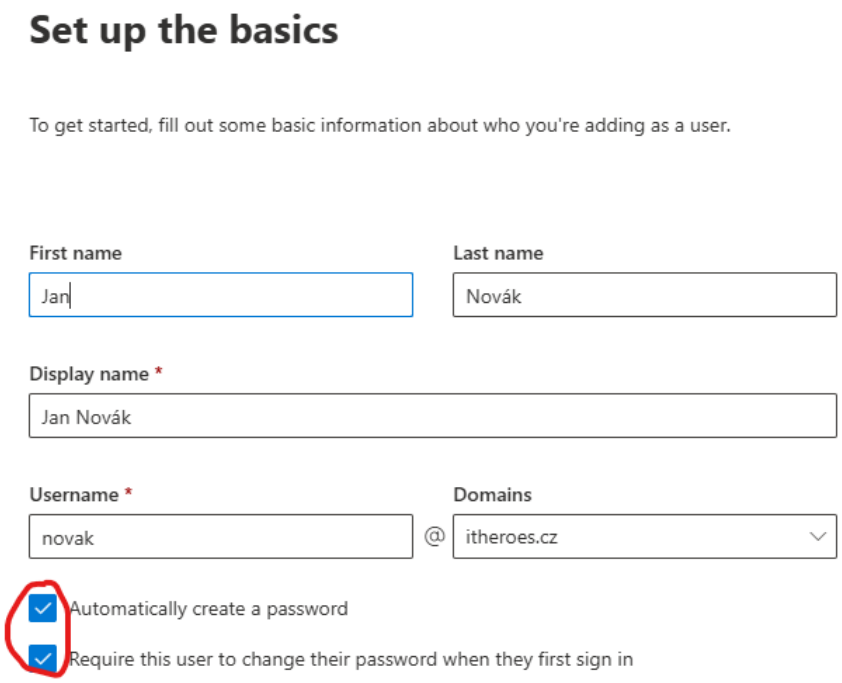
Vytváření uživatelů a administrátorů

Poté co máte nastavené DNS záznamy, se můžete vrhnout na vytváření uživatelů. Pokud už tenanta máte, a jenom se ujišťujete, že máte všechno správně nastavené, tak nepřeskakujte, i pro vás tu budou zajímavé tipy. Otevřete si Active users - Microsoft 365 admin center a klikněte na **Add a user** (Přidat uživatele)

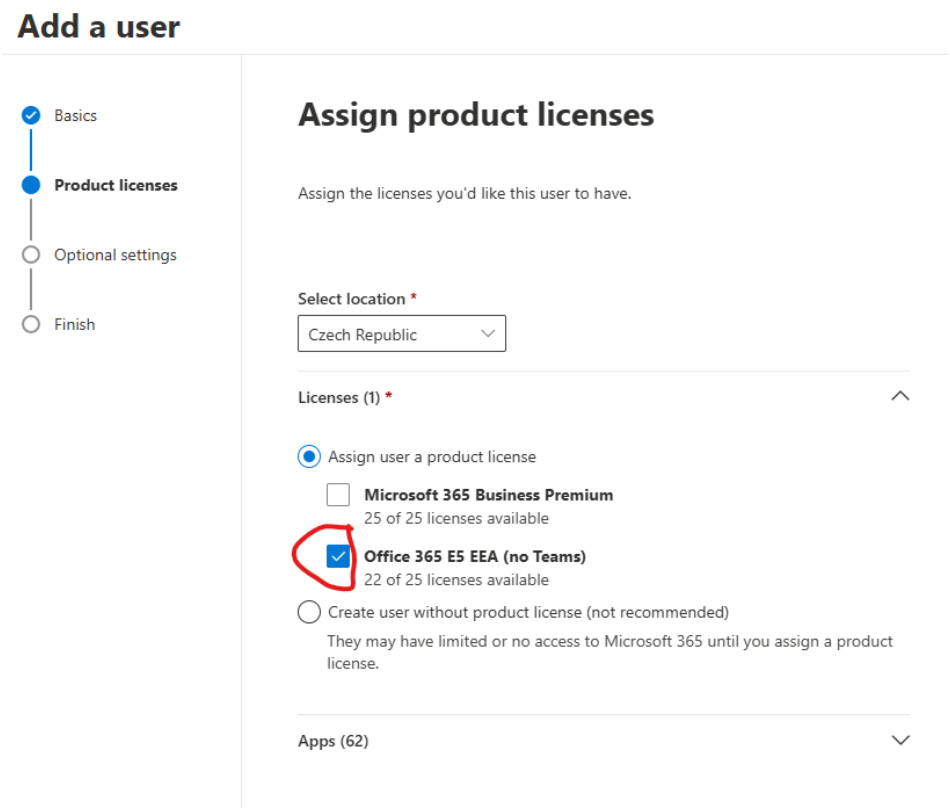


[ICT] GROUP

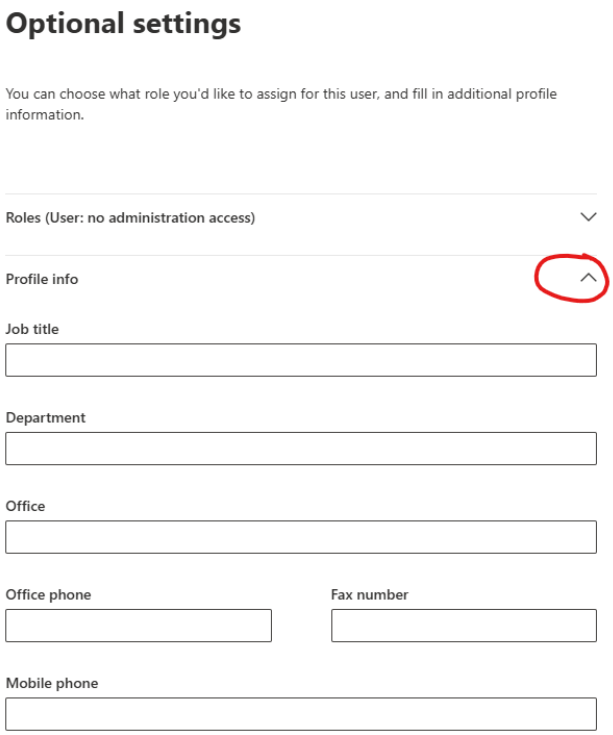
Zadejte jméno, příjmení a email, který budou používat. A nechte zaškrtnuté **Automatické vytvoření hesla** a **vynucení změnění hesla po přihlášení.**



Přidejte licenci

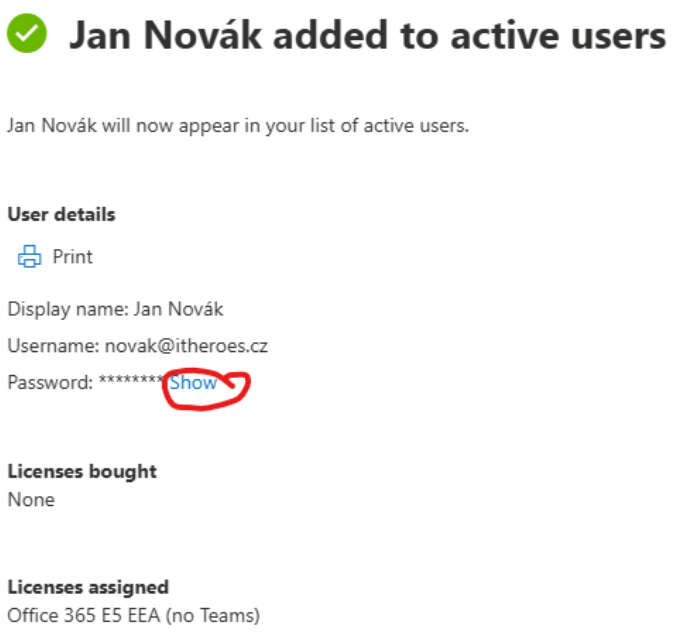


Pod sekcí **Optional settings** (Dobrovolné nastavení) je schované menu **Profile Info** (Informace o profilu), kde můžete přidat pracovní pozici, oddělení, telefonní číslo a další

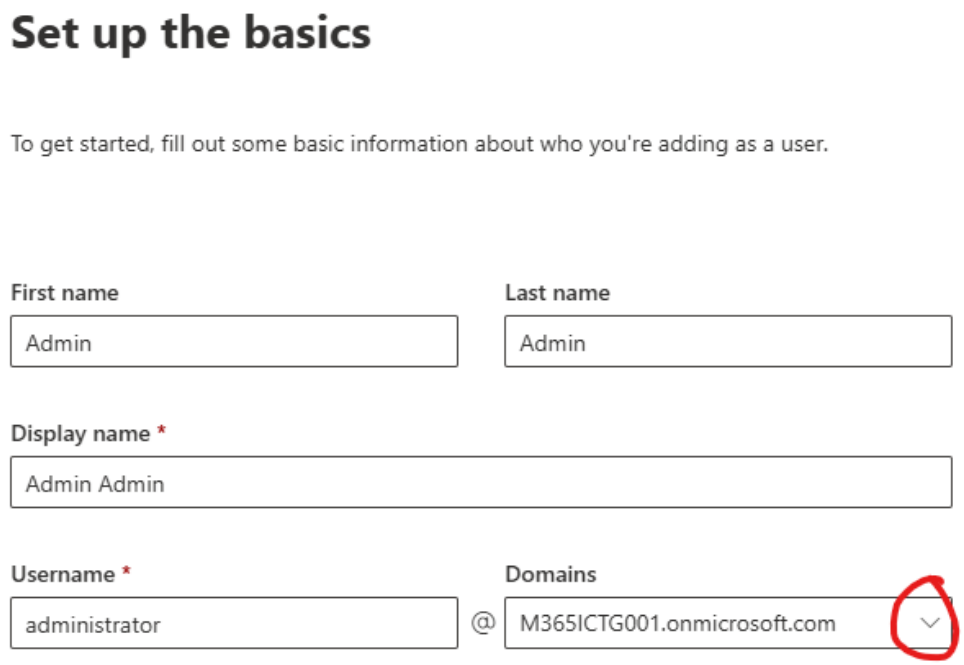


Potom dejte **dokončit**

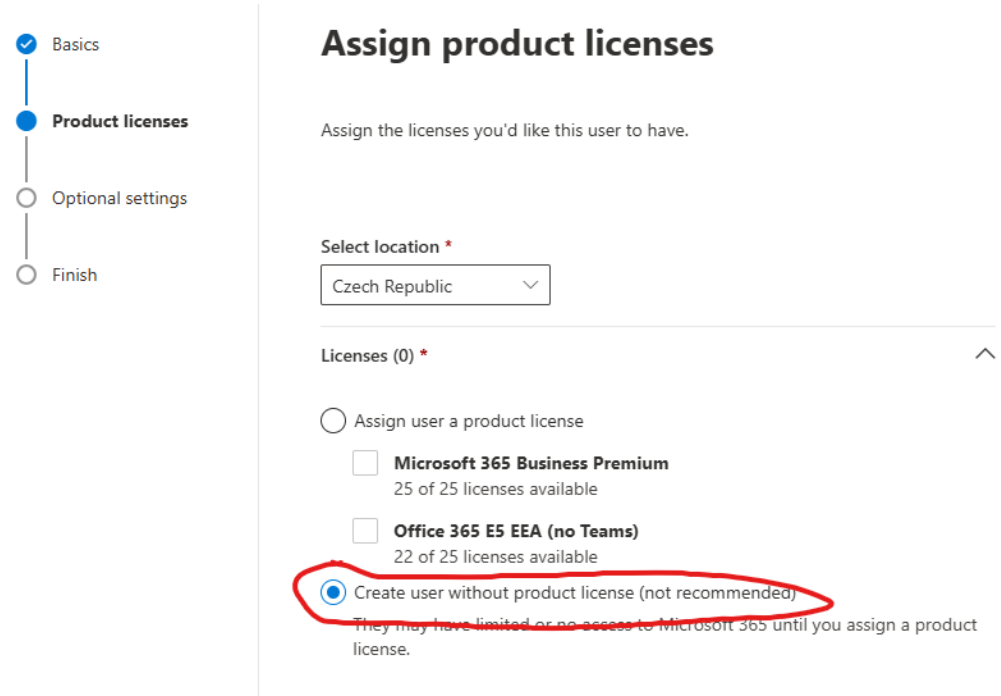
V detailu vám vyskočí informace o vytvořeném účtu. Nezapomeňte si poznamenat heslo. Nemusíte se cítit špatně, že znáte heslo daného uživatele, protože si ho při prvním přihlášení bude muset změnit.



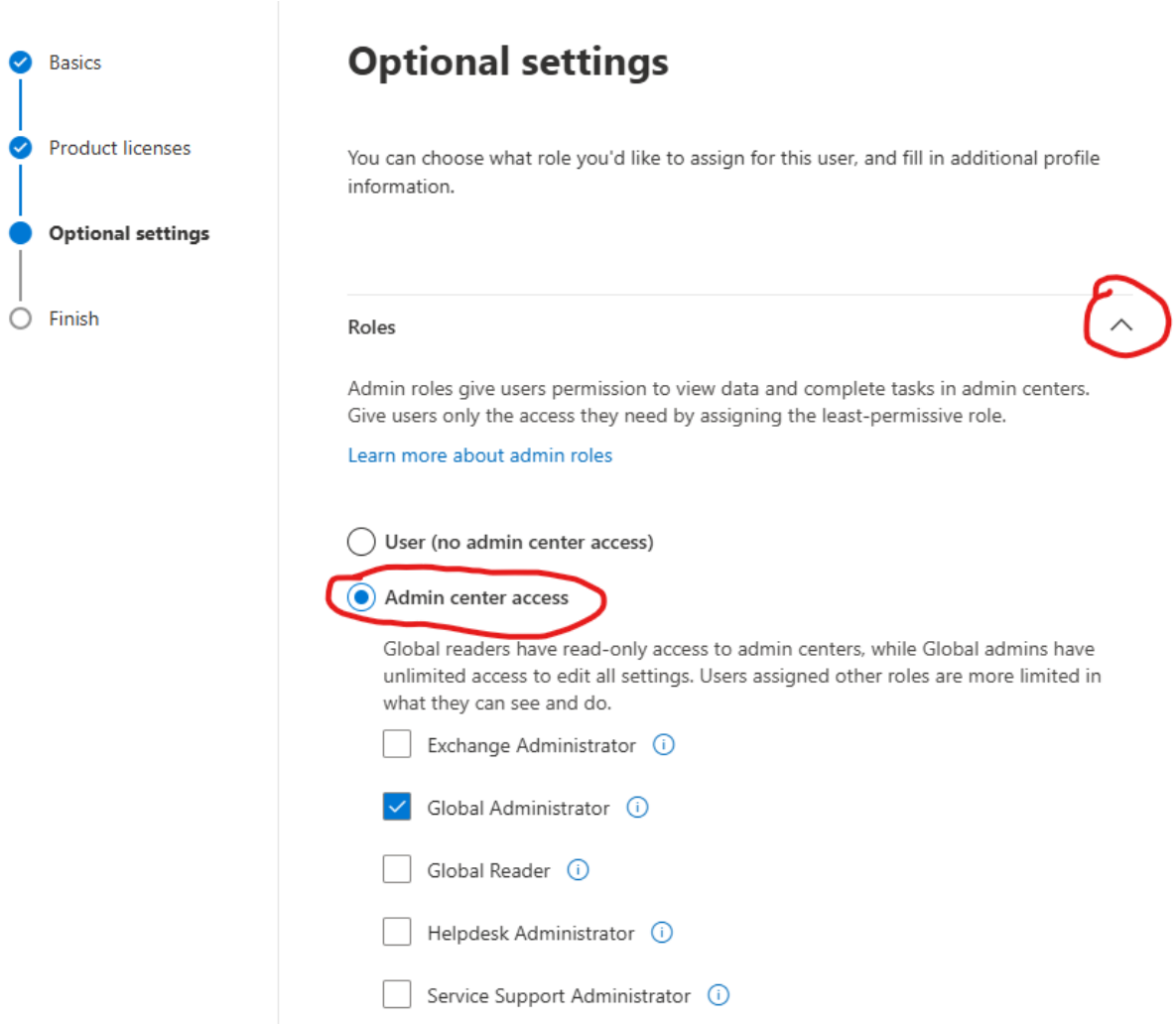
U administrátorů je proces skoro stejný až na 3 věci. Při přidávání emailu vyberte doménu onmicrosoft.com.



Při přidávání licence vyberte možnost **Create user without licence** (Vytvořit uživatele bez licence)



A v **Optional settings** (Dobrovolná nastavení) vyberte **Roles** (Role) **Admin center access** (Přístup do admin centra). Na obrázku je vidět vybraná role **Global Administrator**, která má práva na skoro vše a na co nemá, tak si je může přidat. Pod touto rolí NIKDY nepracujte!



Používání security skupin třídění

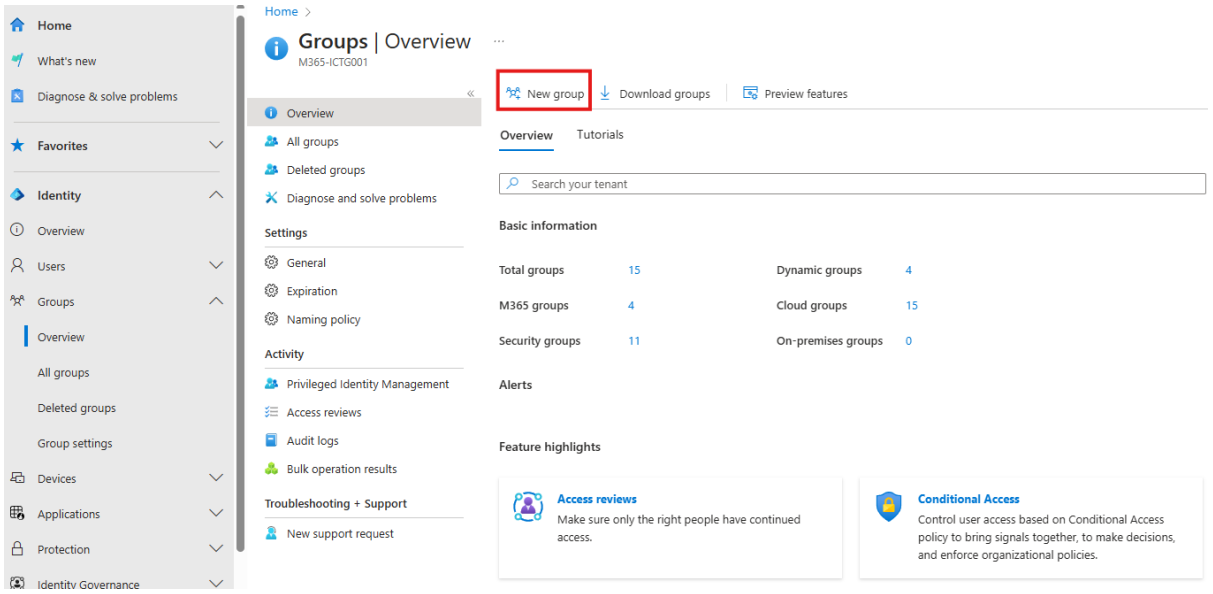
Ať už vám to přijde, jakkoliv otravné, tak udělat si systém v nastavení M365 je absolutně kritické. Nastavení v portálech je hrozně moc a většina věcí se dá nastavit na několika místech. Proto všechno, co děláte musíte označit, jakoukoliv skupinu lidí nebo zařízení zařadit do tzv. security skupin. U nich si nastavte jmennou konvenci ať se v tom neztratíte.

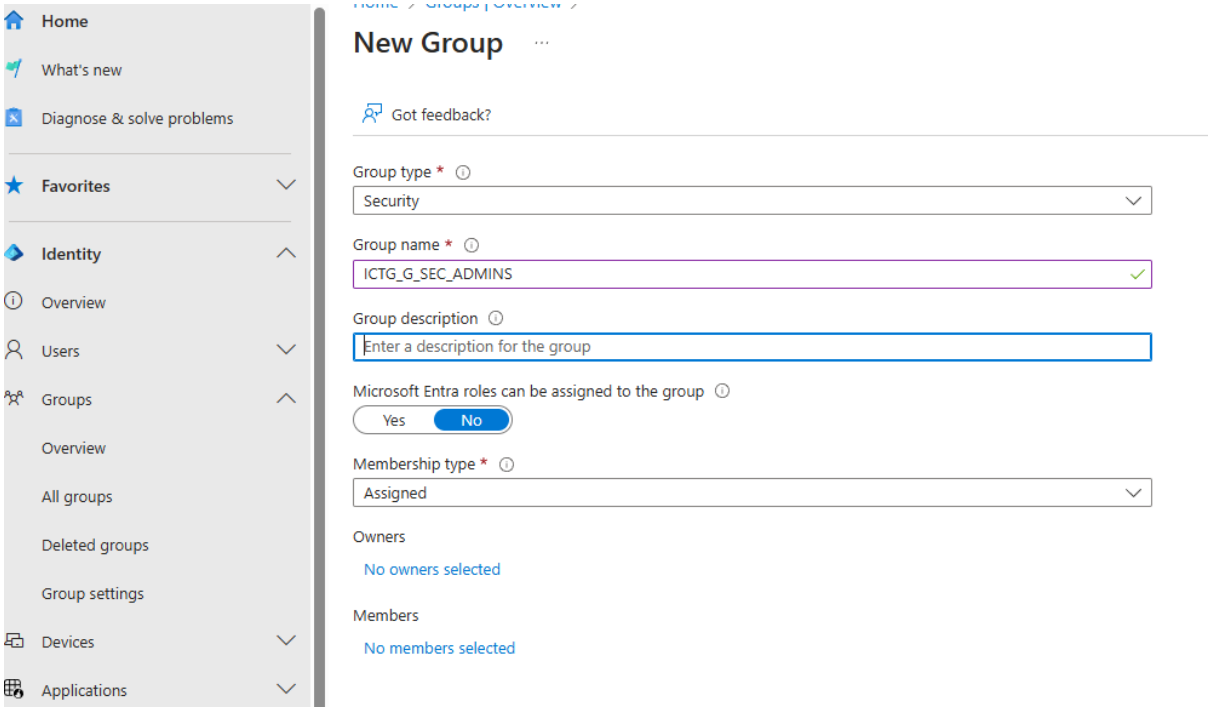
Jak vytvořit security skupinu.

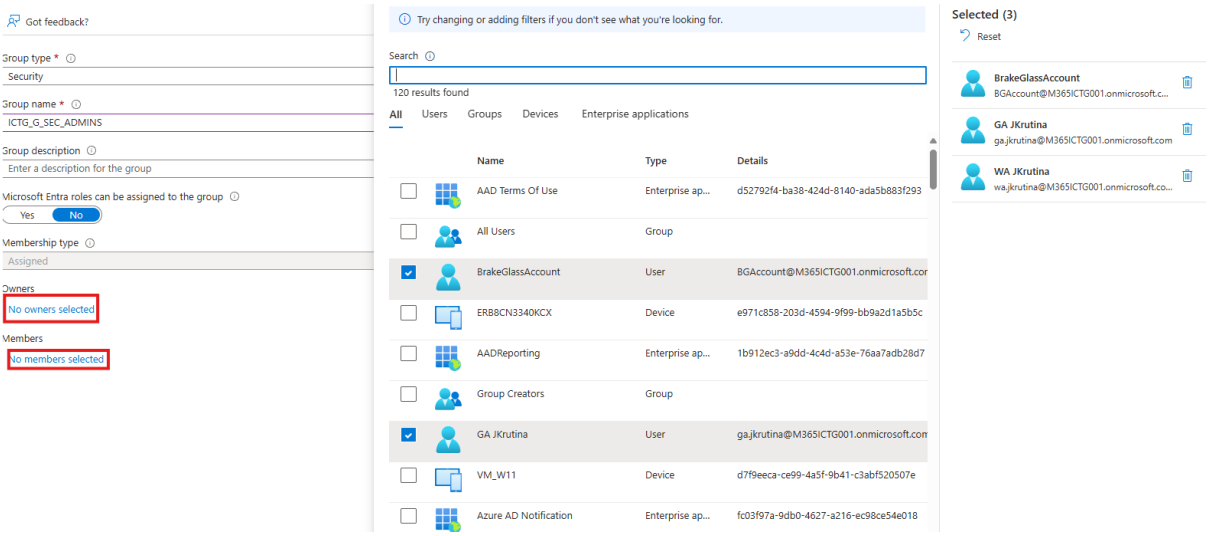
Jde to z více míst, ale já vám ukážu jak na to z Microsoftem doporučované https://entra.microsoft.com/.

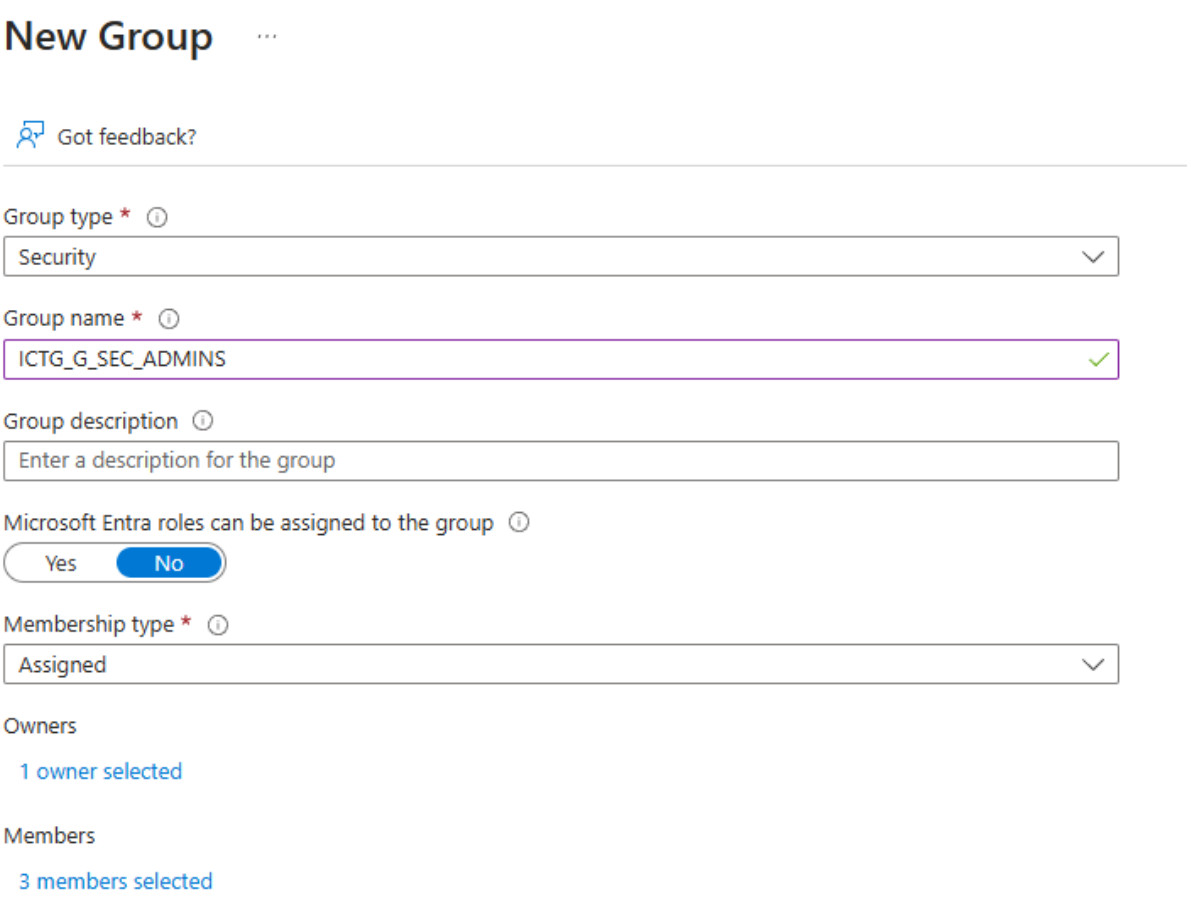
Otevřete si Groups - Microsoft Entra admin center

Jak security, tak i M365 skupiny můžou být ve dvou „módech“ assigned (Přidělená)do té musíte uživatele přidělit sami. Tento typ se hodí pro skupiny, které se buď nemění vůbec nebo se mění velmi málo. Druhý mód je dynamic (dynamická), ta se ještě dělí na dynamic user a dynamic device. U tohoto typu skupiny můžete udělovat členství automaticky podle zadaných parametrů. Teď si ukážeme, jak udělat assigned skupinu pro administrátory a dynamickou skupinu pro zařízení značky HP.









Teď si vytvoříme dynamickou skupinu pro HP zařízení.

[ICT] GROUP

New Group ...

Got feedback?

Group type * ⓘ

Security

Group name * ⓘ

ICTG_G_SEC_DEV_HPDEVICE

Group description ⓘ

Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ

Yes No

Membership type * ⓘ

Assigned

Assigned

Dynamic User

Dynamic Device

No members selected

Group type * ⓘ

Security

Group name * ⓘ

ICTG_G_SEC_DEV_HPDEVICE

Group description ⓘ

Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ

Yes No

Membership type * ⓘ

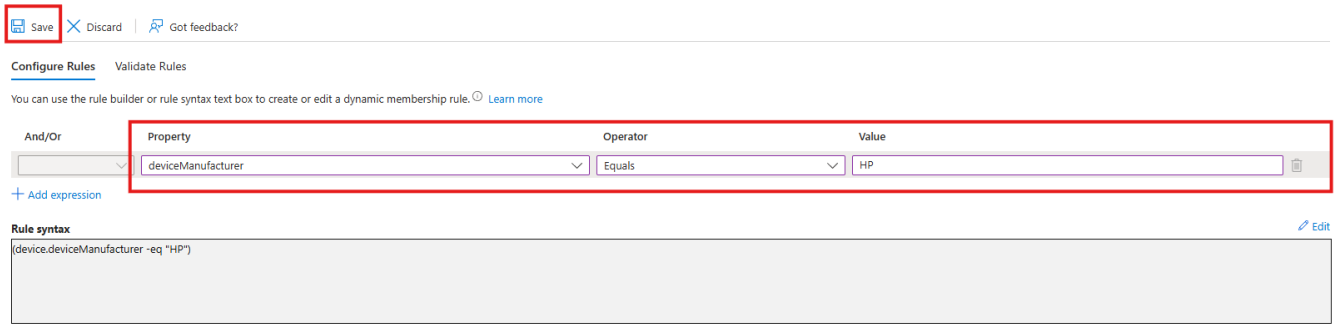
Dynamic Device

Owners

No owners selected

Dynamic device members * ⓘ

Add dynamic query



Propsání do dynamických skupin může trvat 15 až 30 minut i u menších tenantů proto nespěchej opravovat hned.

U dynamických skupin se meze nekladou, proto vám doporučuji s tím trošku pohrát a zeptat se Chat GPT, který v tomto pseudo jazyce psát umí.

User, device a group settings

Jak praví citát od J. M. Jurana: 80 % výsledků vychází z 20 % příčin. Na část z těch 20 % se dneska podíváme. Tato malá a jednoduchá nastavení vám velmi usnadní život a uchrání vás před alespoň nějakou částí útoků, a to bych řekl, že za tak 5–15 min nastavování stojí. Users - Microsoft Azure

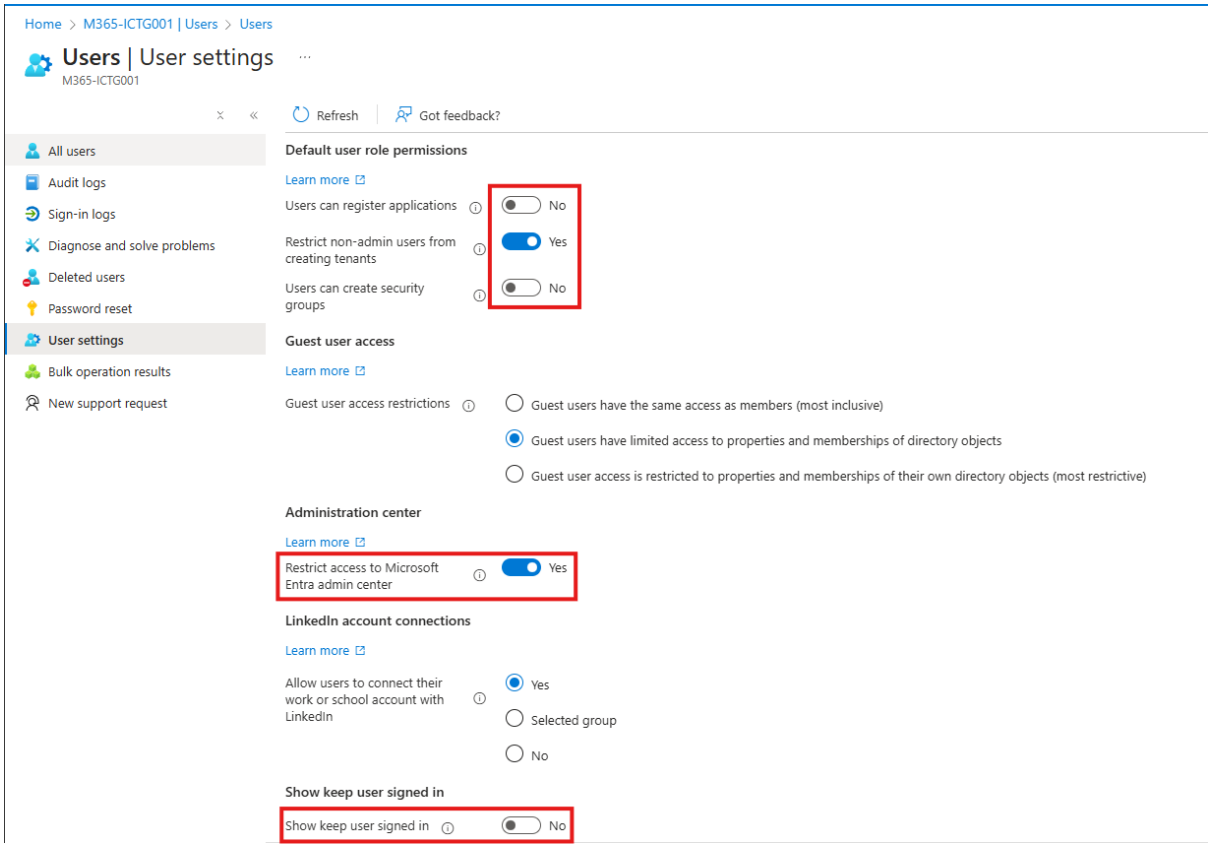
Users can register applications chcete mít vypnuté vždy, krom toho, kdy by vaši uživatelé vytvářeli aplikace v Azure prostředí.

Restrict non-admins users from creating tenants zakazuje uživatelům vytvářet tenanty ve vašem tenantu. Pokud z nějakého důvodu vaši uživatelé potřebují vytvářet podtenanty, tak to asi nechte zapnuté, ale ještě jsem nenašel důvod proč to nechat zapnuté, proto u nás je to vždycky vypnuté.

Users can create security groups by dávalo uživatelům možnost vytvářet security skupiny, které ale, jak jsem vysvětloval minulý týden, jsou spíš pro administraci na admin straně, a proto je zbytečné dávat uživatelům tuto možnost.

Restrict access to Microsoft Entra admin center zajišťuje, že všichni ne administrátoři nemají přístup do admin portálů M365. Tohle je velmi důležité nastavení, protože v krajním případě nepouští útočníka s normálním účtem do těchto portálů, a tím mu nedává přístup k citlivým informacím.

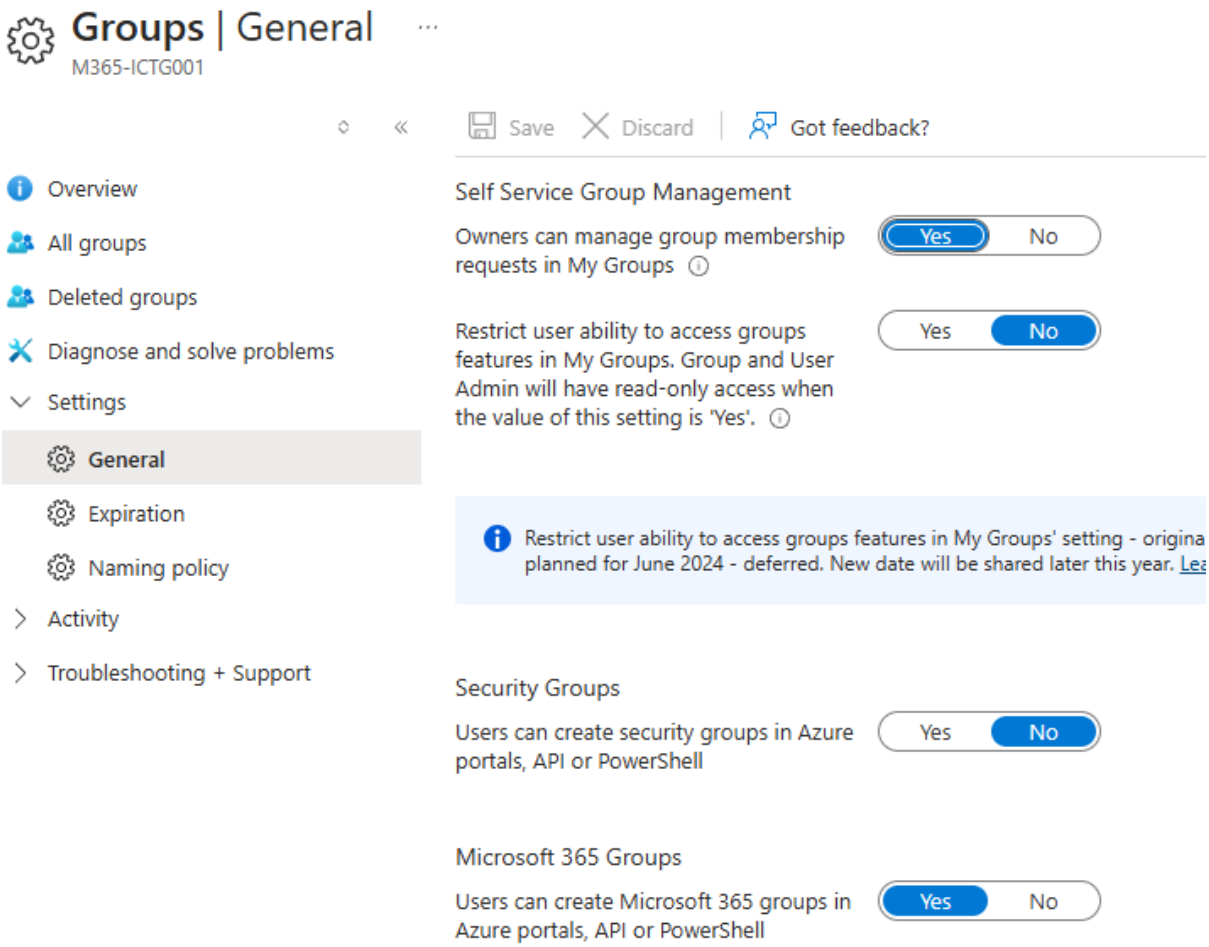
Show keep user signed in toto nastavení zobrazuje uživatelům možnost zaškrtnou „zůstat přihlášen“ okno. Tím se cookie s přihlášením uloží na disk, což může být problematické, kdyby byl počítač zavirovaný.



[ICT] GROUP

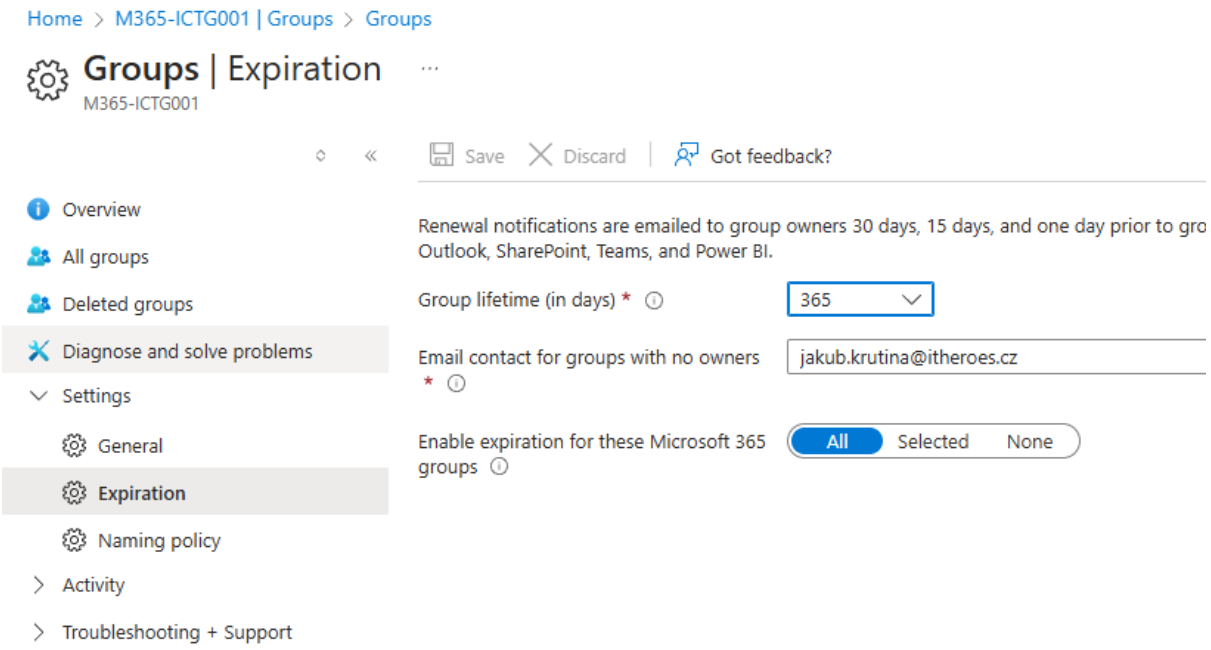
Nastavení skupin – základní nastavení skupin je velmi jednoduché a asi nepotřebuje vysvětlení, krom vyváření M365 skupin. Když vypnete toto zaškrtávátko, tak uživatelé nebudou schopni vytvářet týmy v Teams, ani jako administrátoři. Jediné, kde bude možné vytvářet týmy bude Teams admin centre

Groups - Microsoft Azure

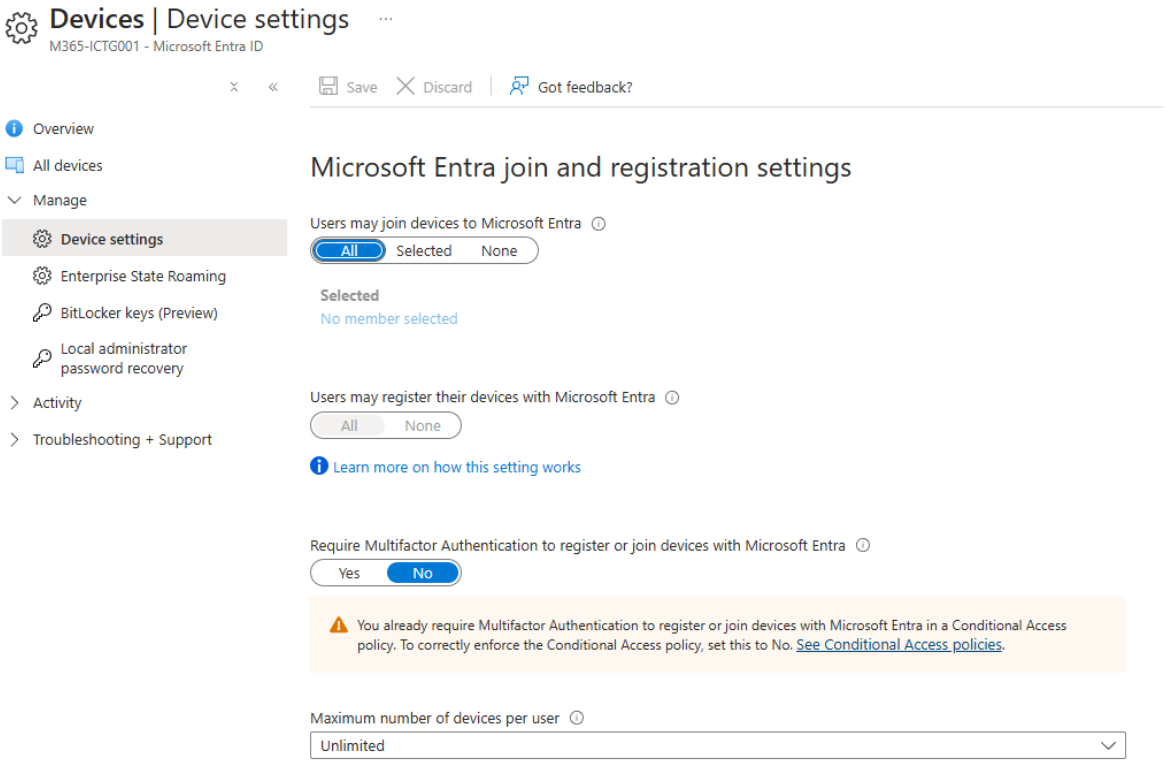


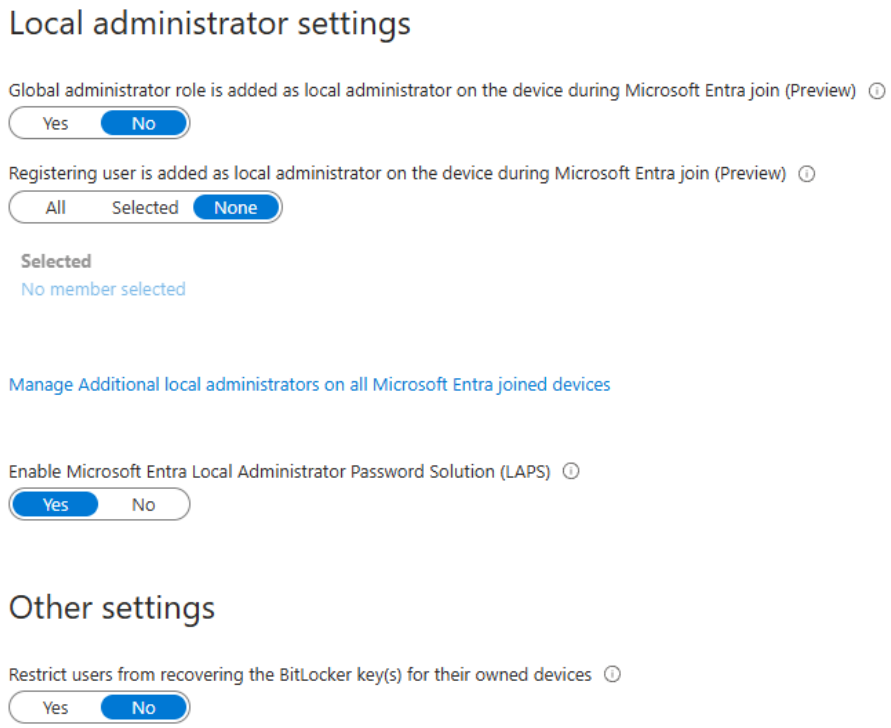
Ta zajímavější pasáž je expirace skupin. Ta může být velmi důležitá, ale také vám může dost uškodit. Hlavní věc je nastavit e-mail kontakt na někoho kdo ve firmě zůstane, ideálně vy samy. Toto nastavení je proto, aby skupiny bez vlastníka po vypršení expirace mohly být obnovené. Normálně přijde e-mail vlastníkovy skupiny o tom, jestli chce obnovit skupinu nebo ne, u skupin bez vlastníka přijde tomuto kontaktu.

Groups - Microsoft Azure



Nastavení zařízení – tyto nastavení můžou vypadat v celku otevřeně, ale mám nastavené jiné politiky, které zajišťují, že si do tenanta nemůže přidat zařízení jenom tak někdo. Proto pokud plánujete pokračovat s tímto návodem, tak není potřeba toho moc měnit až na **Local administrator settings**, kde všechno vypněte. Do počítačů se jako administrátoři dostanete přes workstation admin účty.





[ICT] GROUP

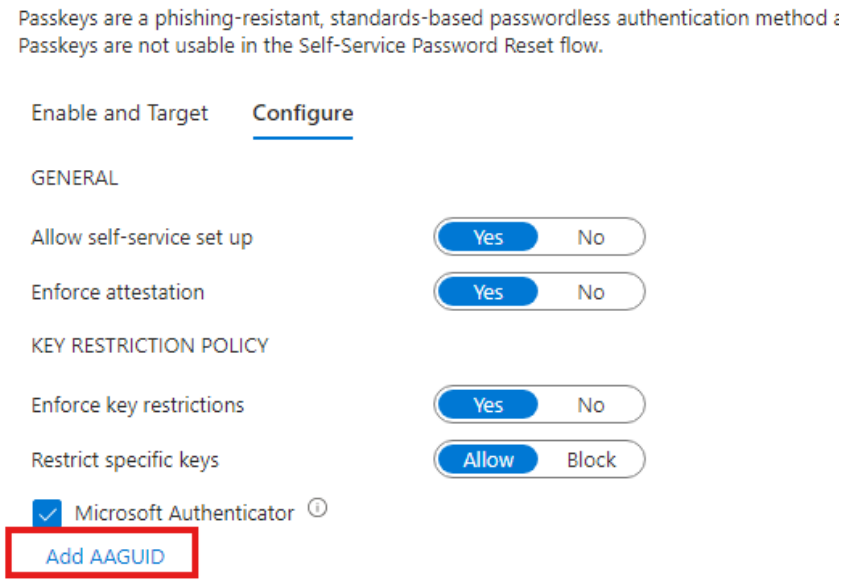
Zabezpečení uživatelských účtů

V dnešním díle téhle obsáhlé kuchařky se podíváme na zabezpečení uživatelů nebo tedy lépe řečeno jejich účtů. Protože za ně vystupovat nemůžete a stát za zády jim také nemůžete, tak je dobré je nějak chránit, většinou hlavně před nimi samotnými. První věc, na kterou se podíváme je nastavení **Authentication methods.**
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods/fromNav/

Zde povolíme všechny silné metody autentifikace (Email OTP samozřejmě používat můžete, ale já ho osobně nemusím).

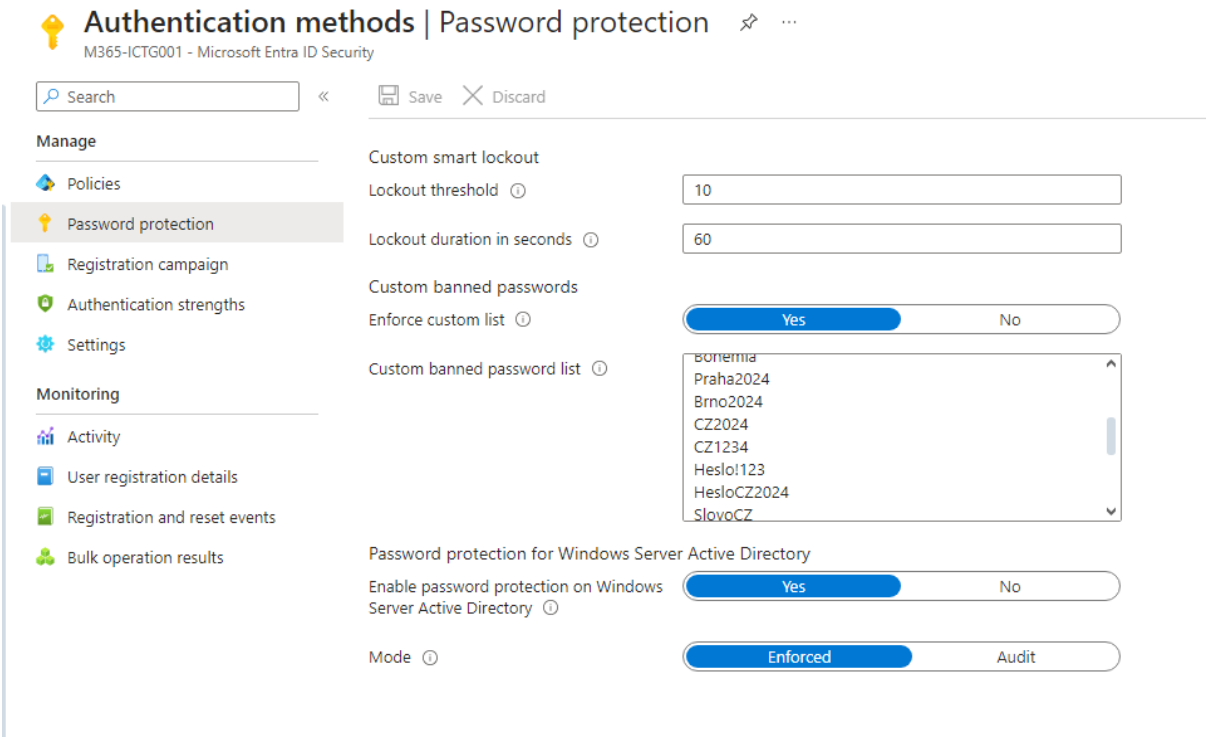
Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)	All users	Yes
Third-party software OATH tokens	All users	Yes
Voice call		No
Email OTP		No
Certificate-based authentication		No
QR code (Preview)		No

Nezapomeňte si přidat všechny stávající FIDO2 klíče, které používáte do nastavení FIDO2.



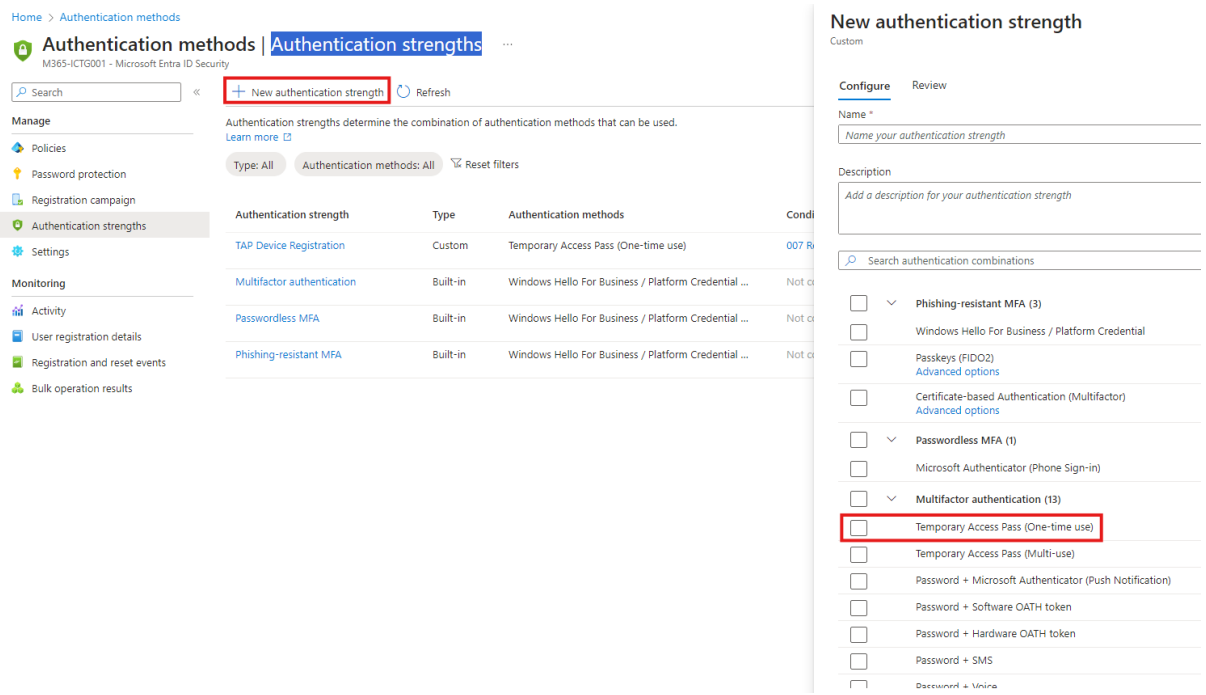
Další, na co se podíváme je **Password Protection**. Toto je velmi zajímavá věc, která vám umožňuje nastavit list zablokovaných hesel, můžete jich mít až 1000, velká a malá písmena se nezohledňují a rovnou blokuje substituce jako je 0 za o nebo 5 za s. Toto vám umožňuje vyhnout se velké části slovníkových útoků. Abyste se neupsali, tak na vygenerování hesel, které zakážete použijte ChatGPT. (ChatGPT dotaz pro inspiraci: Ahoj snažím se zabezpečit svoji firmu pomocí Password protection v Microsoft Entra ID. Budu od tebe potřebovat pomoct vygenerovat list 1000 jednoduchých hesel, které by lidi mohli v mojí firmě „Jméno firmy“ použít. Lokalizuj tyto hesla pro českou republiku a neřeš velká a malá písmena a substituce). Otevřete si

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtection/fromNav/



Pozor na **Enable password protection on Windows Server Active Directory** je možné, že bude kolidovat s **Group policy** v AD. Nemělo by, ale Windows se občas zblázní.

A pro dnešek na závěr se podíváme na **Authentication strengths** a rovnou si jednu vytvoříme, tu potom použijeme na připojování zařízení do systému Entra ID. Otevřete si https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AuthStrengths/fromNav/

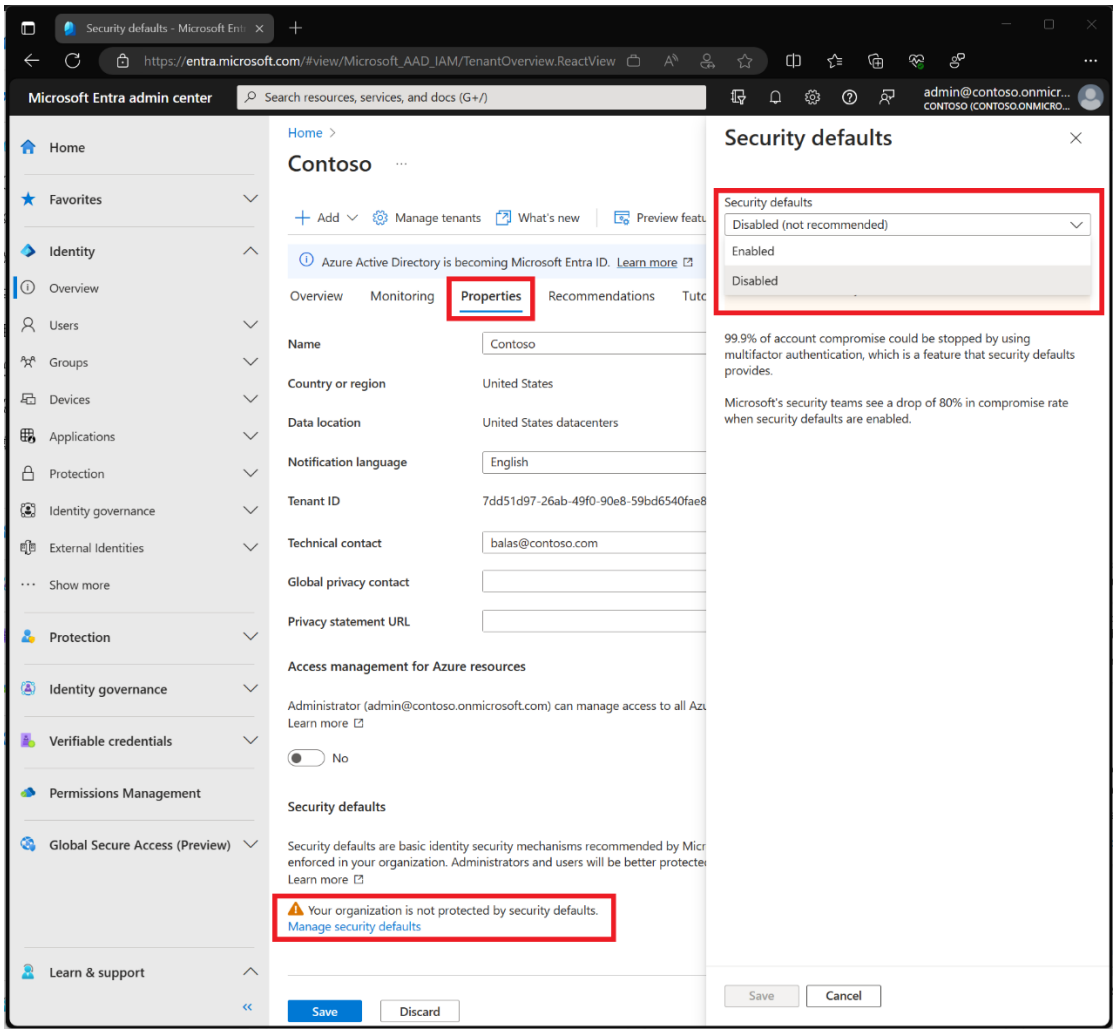


Samozřejmě můžete použít i multi-use TAP (Temporary Access Pass). Potom stačí jenom dát vytvořit a máte hotovo!

[ICT] GROUP

Conditional Access Policies!

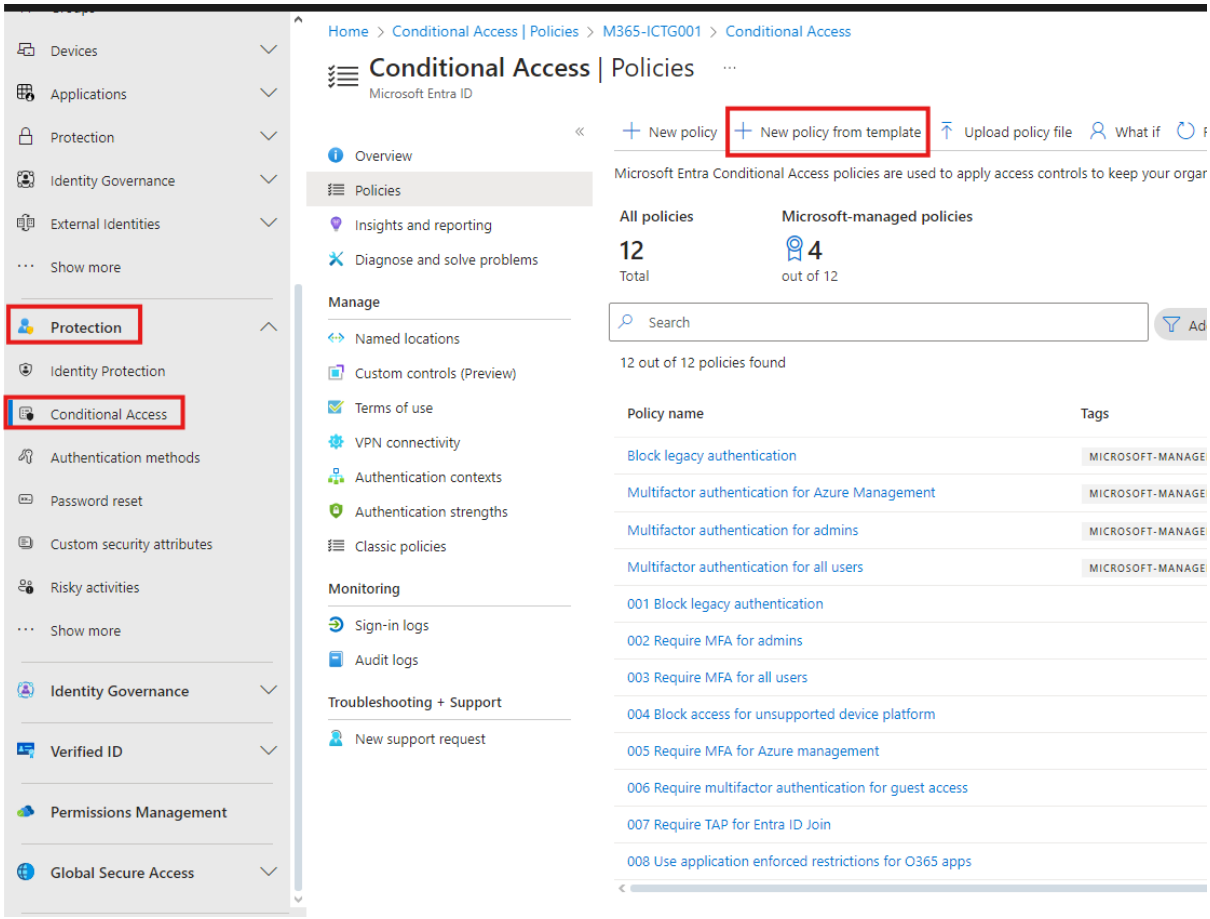
Conditional Accass Policies neboli **CAP** jsou hlavním ochranným prvkem po silných a unikátních heslech, a proto pokud máte tu možnost, tak si je rozhodně nastavte.
V dnešní článku si ukáže prvních pár, v příštím článku si ukážeme zbytek. Velmi důležitá věc, než začneme, buďte s implementací **CAP** opatrní a mějte vždy alespoň jeden účet, který je ze všech politik vyjmutý a je **Globální Administrátor!!!** První věc, co musíte udělat před nastavením **CAP** je vypnout tzv. **Security defaults.** Takto to vypadá, když je máte vypnuté. Můžete si je vypnout zde.
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView/initialValue//tabId//recommendationResourceId//fromNav/Identity

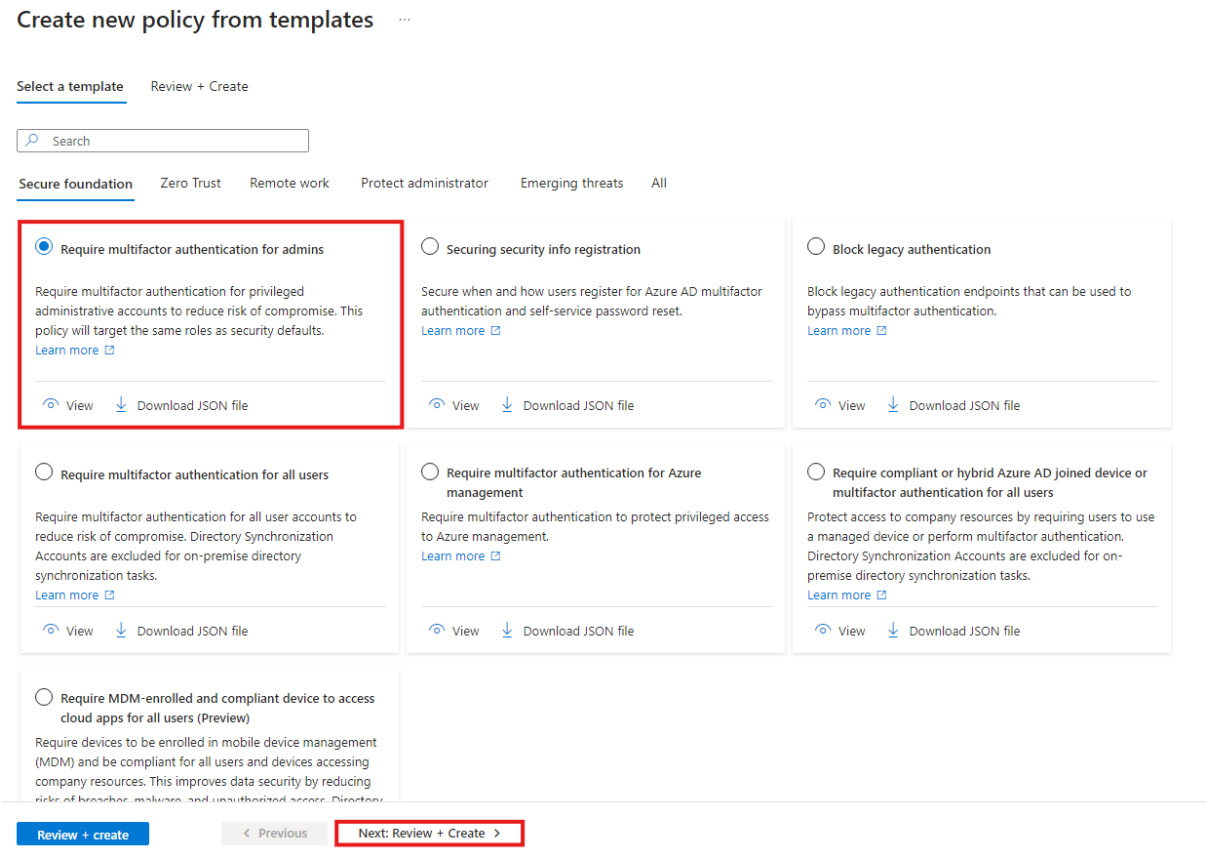


Teď na nastavení **CAP**! První věc, kterou nastavíme je **require MFA for admin** (vynucení MFA pro administrátory) a použijeme na to už předvytvořenou šablonu od Microsoftu. Otevřete si portál **Entra**, přejděte k **protection** a pod tím **Conditional Access**.

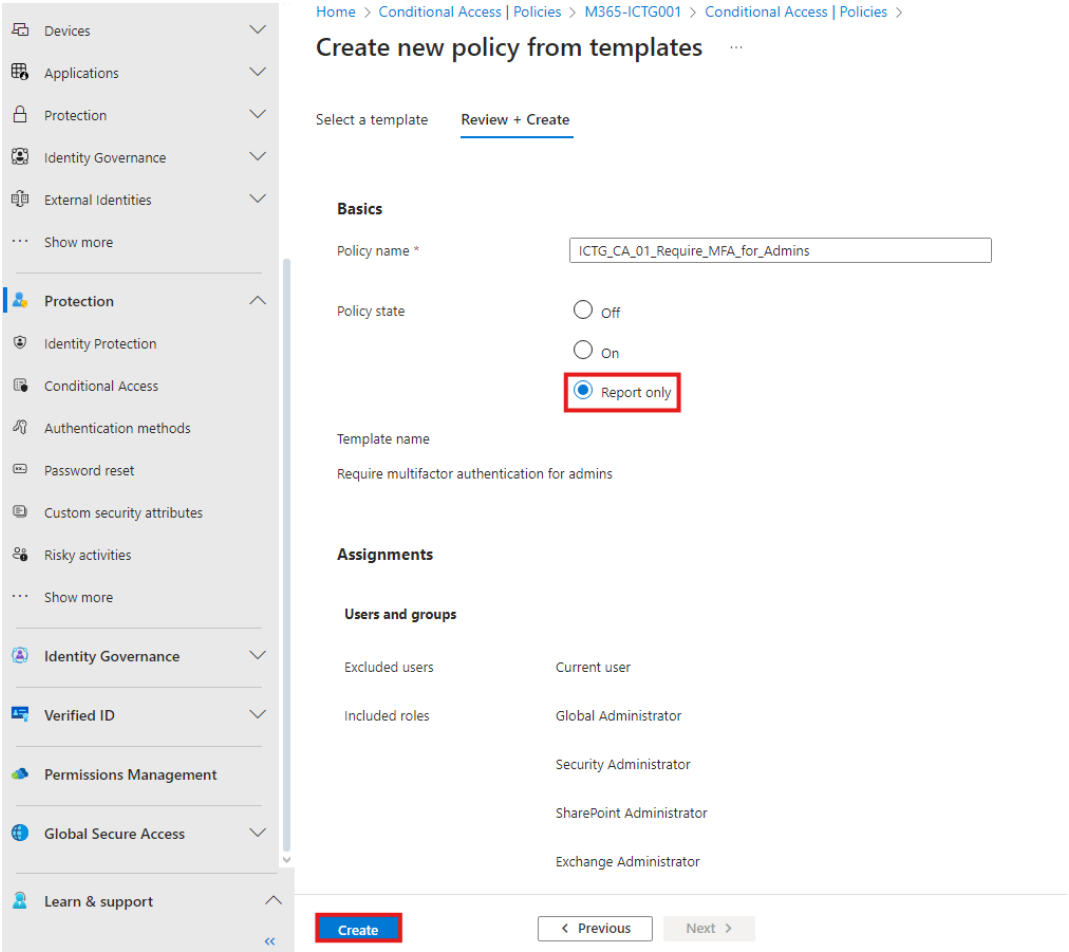
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies/fromNav/

Poté klikněte na **New policy from template.**

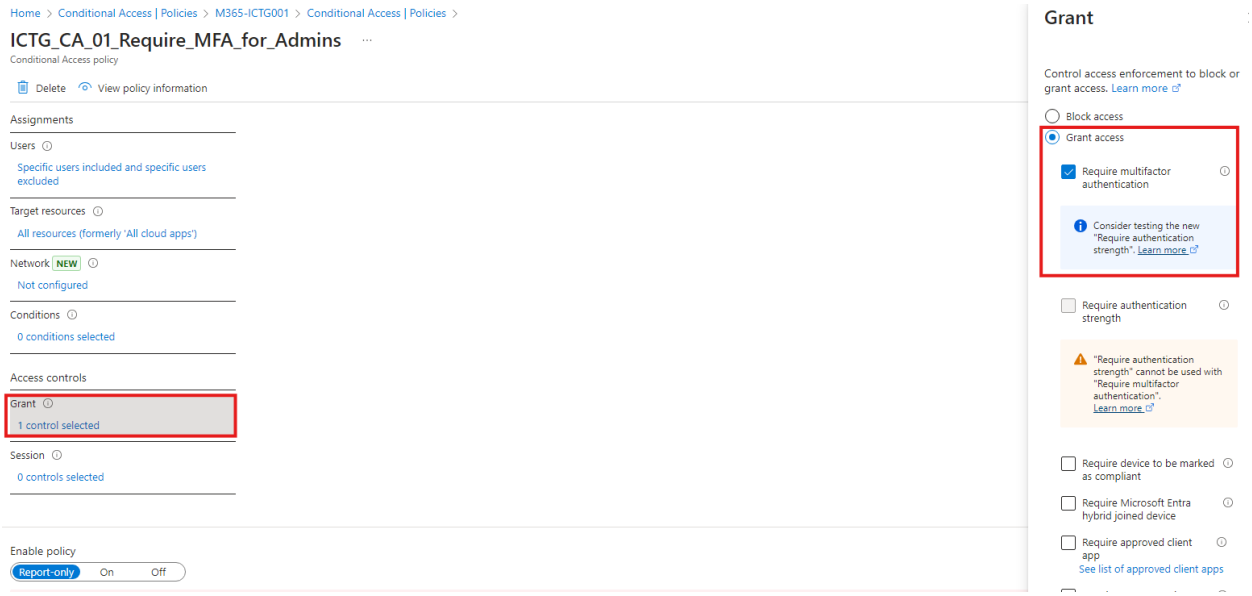




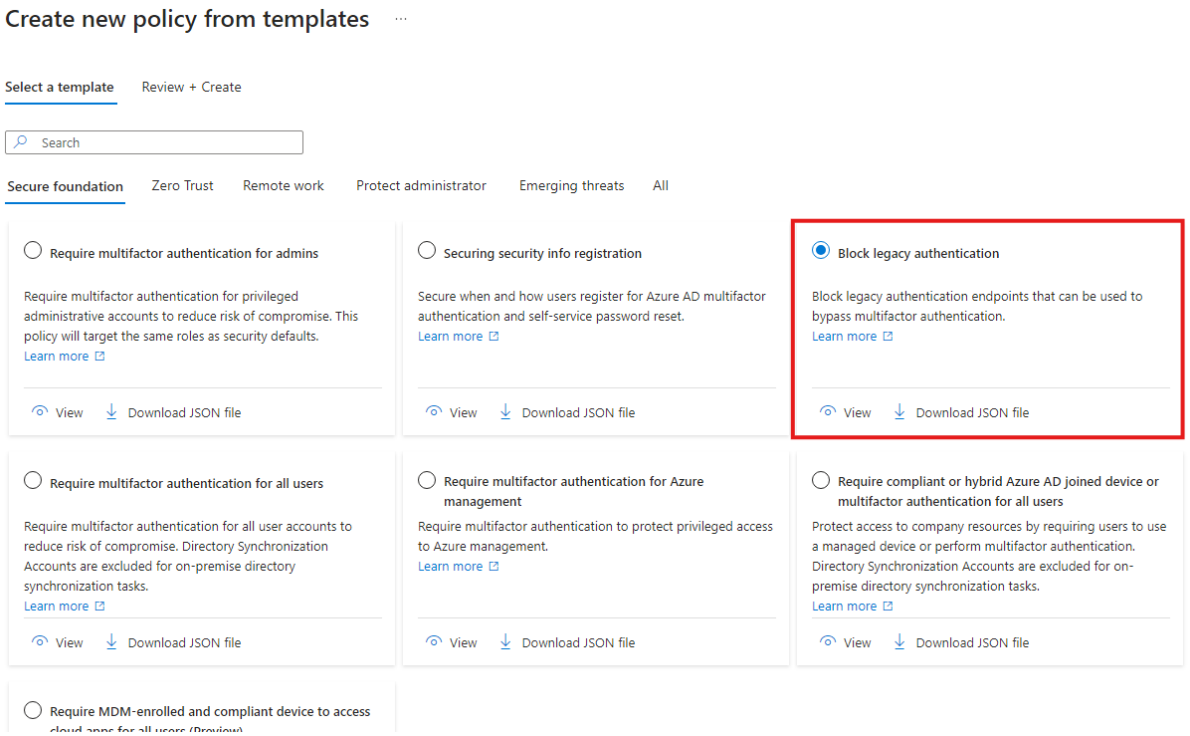
Zezačátku nechte politiky v módu **Report Only**, zjednoduší vám to doladění a testování. Taky silně doporučuji nastavit si jmennou konvenci u **CAP** a přidat do jména číslo politiky, velmi vám to usnadní řešení problémů.



Rozklikněte si politiku a klikněte na **Users.** Do **Exclude** dejte skupinu/y nebo uživatele, kteří mají být vyřazeni. To znamená ten jeden **Global Administrator** účet. Tato politika se bude vztahovat na vybrané administrátorské role a nebude se vztahovat na vyřazený účet. Pod tím v **Target resources** vidíme, že se bude vztahovat na **All cloud apps**. Potom dlouho nic a až u **Access Control** pod záložkou **Grant** vidíme, že je vynucené více faktorové ověřování. Jedna důležitá věc, kterou bych rád zmínil je, že politiky se můžou vztahovat, jak na zařízení, tak na uživatele, ale ne zároveň. Nesmí se míchat!

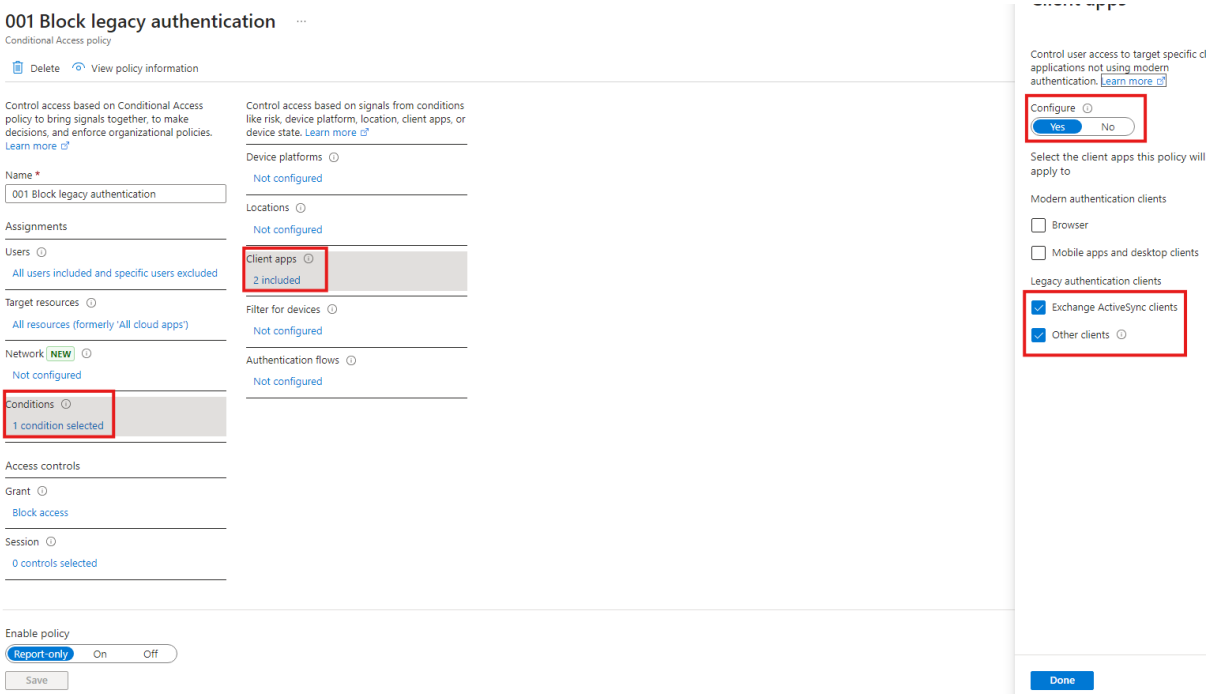


Teď přejdeme k další politice, a to je **Block Legacy Authentication.**



Zase ji pojmenujte a nechte v módu **Report Only**. Toto nastavení mám zapnuté pro všechny uživatele vyjma dvou skupin, ve kterých mám účet poslední záchrany a vyřazené uživatele. Zase mám nastavené na **All cloud apps.** Kde se ale nastavení mění je u **Conditions**, kde mám nastavené blokování zastaralých autentizačních klientů, jako je **SMTP**, **POP**, **IMAP** a další. Pokud máte nějaká zařízení, která se přes profil ověřují u **Entra ID** pomocí některého z těchto protokolů, tak je přidejte do **Exclude.**

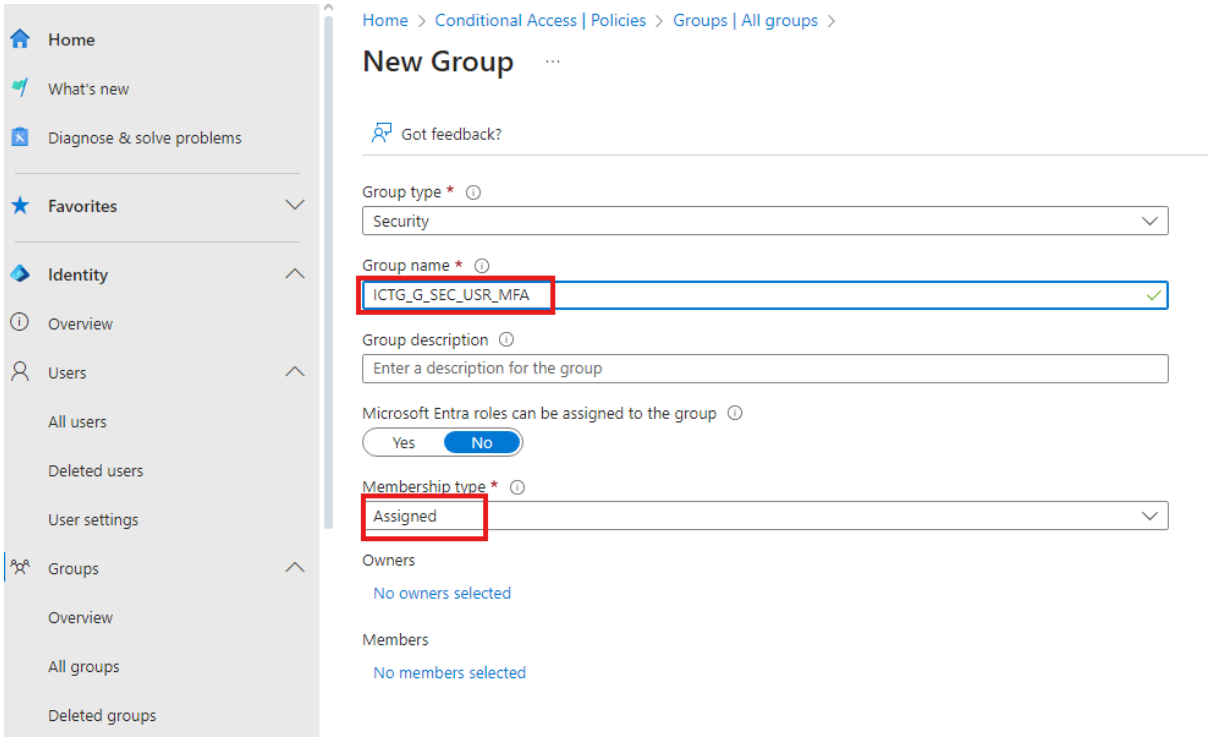
[ICT] GROUP



Conditional Access Policies část druhá!

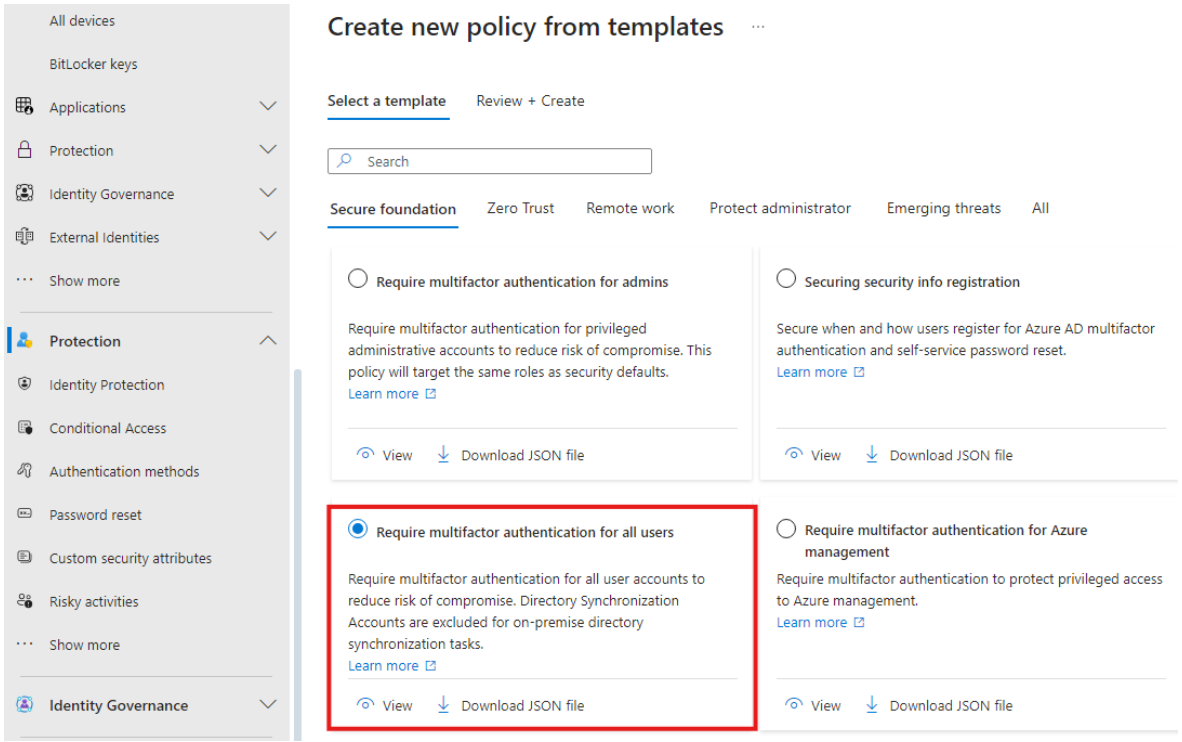
V dnešním článku si projedeme další část **CAP**, které doporučuji jako základní nastavení pro kohokoliv s **Business Premium** tenantem. Samozřejmě kreativitě se meze nekladou a pokud něco specifického budete potřebovat povolit nebo zablokovat, tak to přes **CAP** skoro určitě půjde. Další politika, kterou si nastavíme je **Require MFA for all users**. Tato politika může být a nejspíš bude složitá nastavit, pokud vaši zaměstnanci nejsou s technikou moc kamarádi, přesto je ale nesmírně důležitá a zabrání skoro všem útokům. Proto pokud máte více zaměstnanců, tak si implementaci rozdělte do menších částí, ať vás nezahltí velká spousta požadavků typu: co to po mě chce, proč to po mě chce, a na co je to potřeba. Ze zkušenosti přijdou a 5 najednou se zvládnou dá, ale 50 rozhodně ne!!!

Pro nastavení této politiky si prvně tedy vytvoříme **security** skupinu, do které budeme manuálně přidávat uživatele (ano je to pakárna, ale řešit všechny najednou je za mě horší). Skupinu vytvoříme v portálu **Entra**, pod záložkou **Identy** a **Groups**. Skupinu nezapomeňte pojmenovat podle vaší konvence.
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AddGroupBlade



Teď si do skupiny přidáme uživatele, na které chceme cílit jako první. Jenom rychlá odbočka, všechny ve skupině nechte a nikoho, kromě lidí, co u vás už nepracují, z ní nevyndávejte, protože po tom co do ní dostanete všechny, tak ze skupiny můžete udělat dynamickou. Zpátky k vytváření politiky. Otevřete si v **Entra** portálu **CAP** a zvolte šablonu **Require multifactor authentication for all users**.

https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/CaTemplates.ReactView



[ICT] GROUP

Create new policy from templates ...

Select a template | Review + Create

Basics

Policy name * ICTG_CA_03_Require_MFA_for_users

Policy state

- ○ Off
- ○ On
- ◉ Report only

Template name

Require multifactor authentication for all users

Assignments

Users and groups

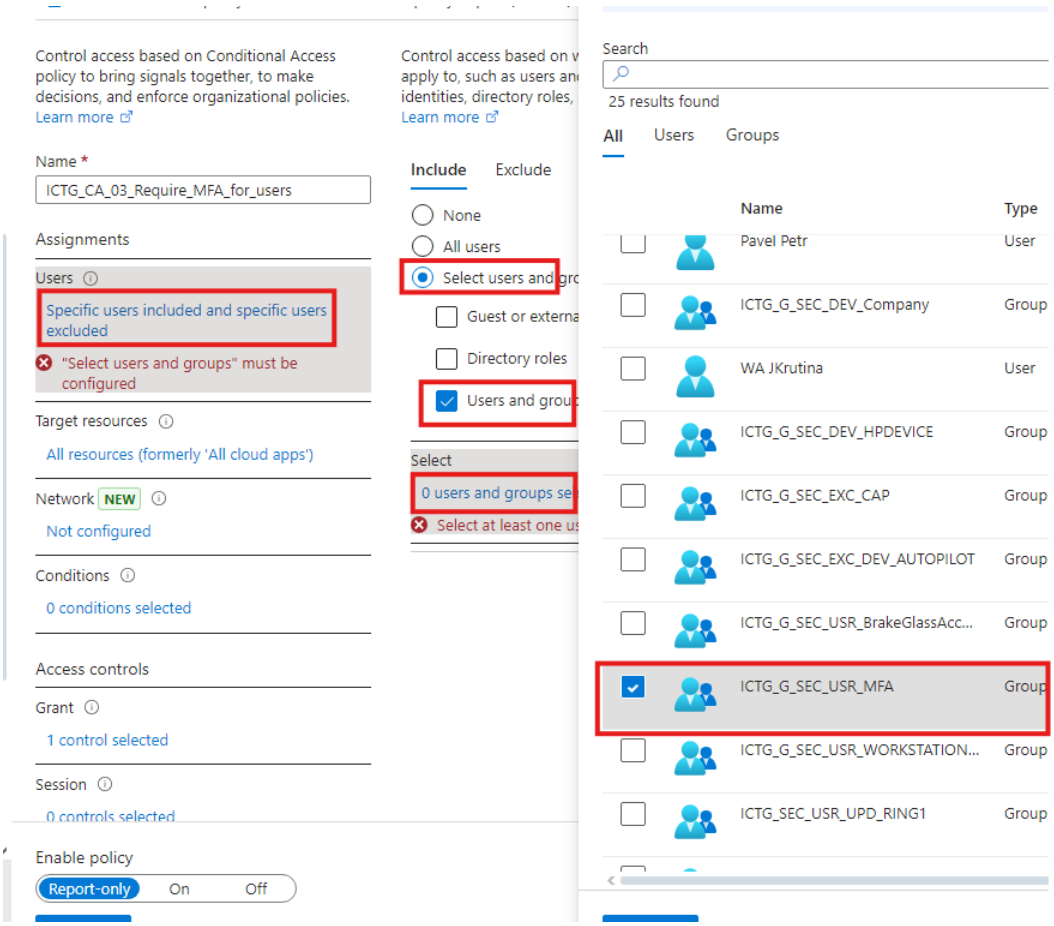
Included users	All users
Excluded users	Current user
Excluded roles	Directory Synchronization Accounts

Cloud apps or actions

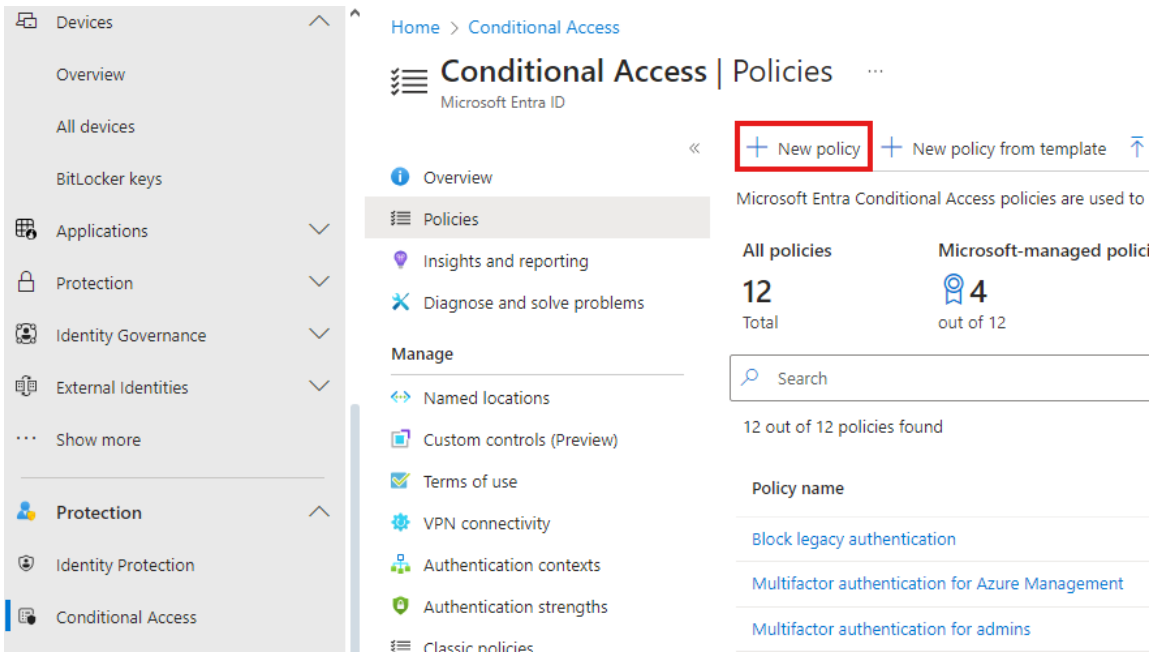
Create | < Previous | Next >

[ICT] GROUP

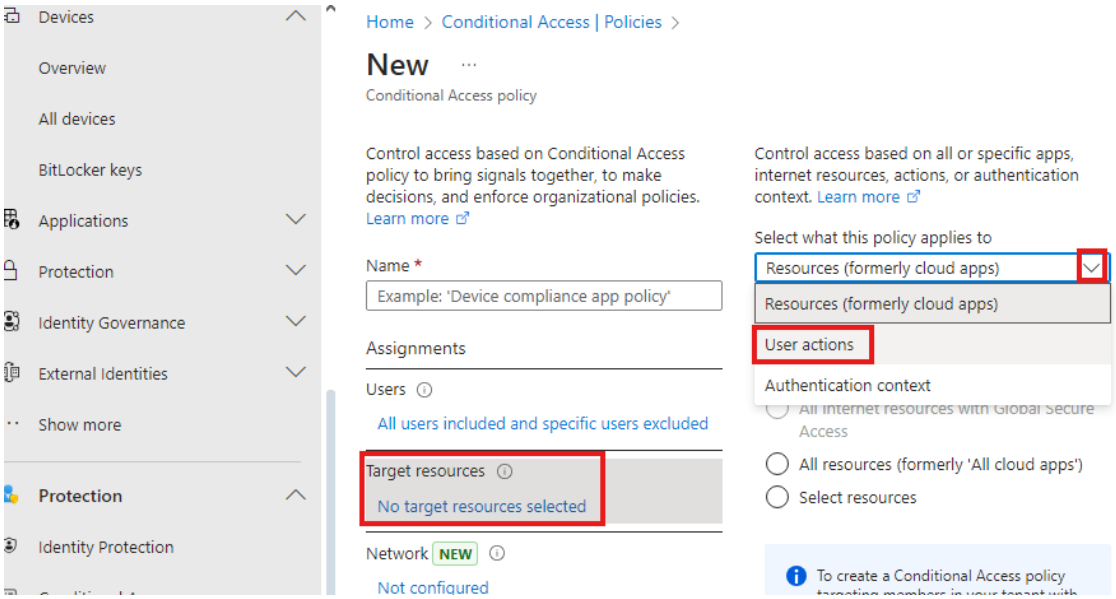
Teď si politiku otevřete, vyberete **users,** poté **Select users and groups, Users and groups** a nakonec přidejte svoji skupinu, kterou jsme vytvořili v předchozím kroku. Poté už stačí jenom vyndat přes **Exclude** účty záchrany a máte hotovo!

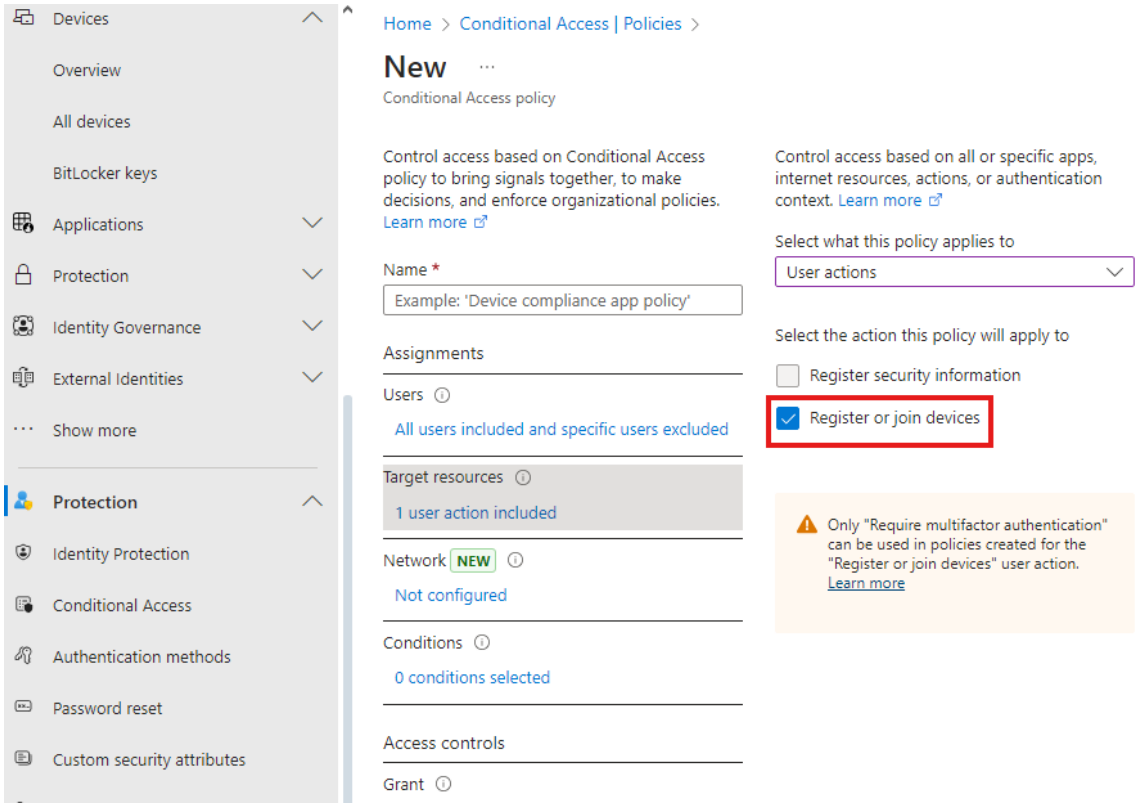


Teď si vytvoříme politiku, díky které bude vynucený **TAP** pro připojení zařízení k **Entra ID**. V menu, kde jste doteď vytvářeli politiky přes šablony si teď vytvoříme politiku, na kterou šablona není.



Zacílíme ji na všechny uživatele a vyhodíme z ní účty záchrany a vyřazené uživatele, jako u všech skupin a poté jdeme na konfiguraci. Rozklikneme si **Target resources** a vybereme, že se politiky budou aplikovat na **User actions** a v tomto menu na **Register or join a device**.





Poté už stačí jen přejít do sekce **Grant,** kde zaškrtnete **Require authentication strength** a zde vybere TAP.

Pak už stačí jen uložit v **Report-only** módu a máte to.