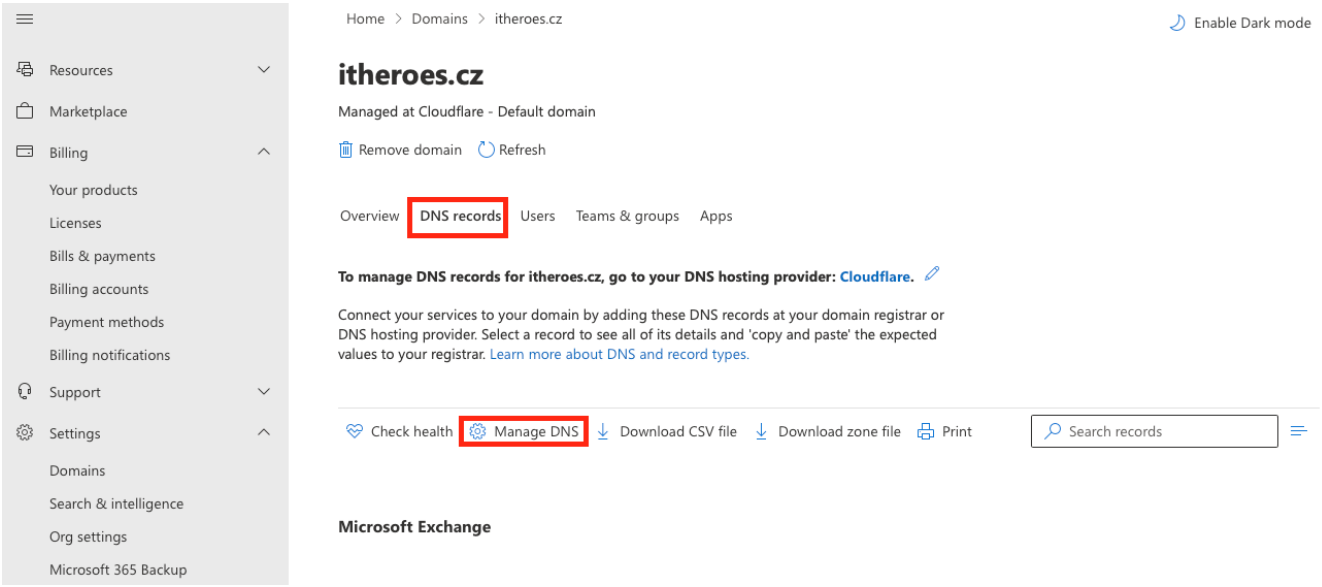
[ICT] GROUP

Admin Centrum

Nastavení DNS záznamů

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

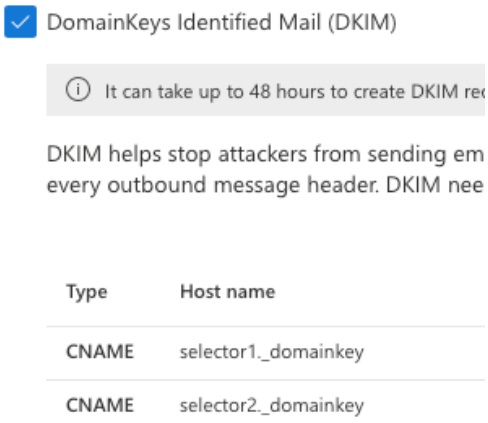
Rozklikněte si doménu, kterou chcete upravovat. Klikněte na DNS records (DNS záznamy) a poté klikněte na Manage DNS (Spravovat DNS)



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

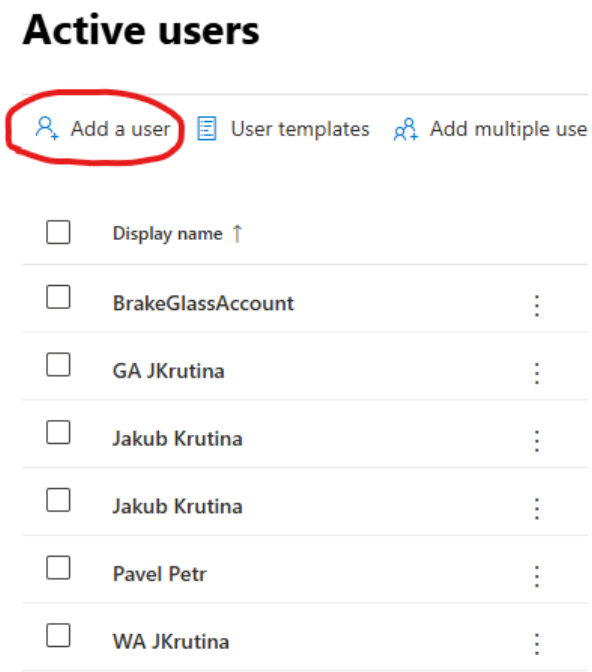


Poté co máte tyto věci nastavené, tak si vygenerujte DMARC pomocí easydmarc, nebo Dmarcian (nebo dalších služeb). DMARC vypadá přibližně takto: **v=DMARC1;p=quarantine;sp=quarantine;pct=100;rua=mailto:example@example.eu;ruf=mailto:example@example.eu;ri=86400;aspf=s;adkim=s;fo=1;**

Poté si všechno zkontrolujte přes MXTOOLBOX.

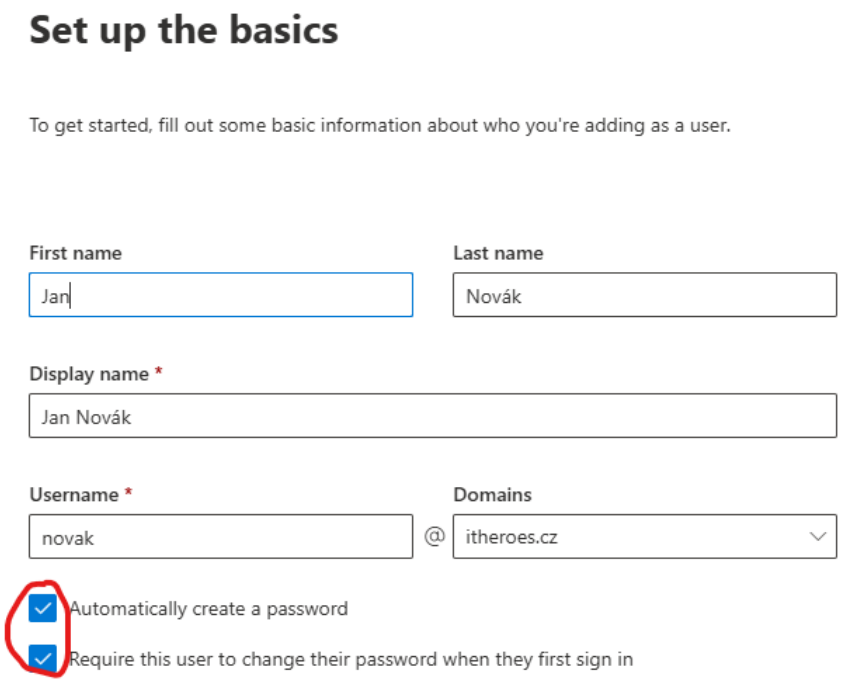
Vytváření uživatelů a administrátorů

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)

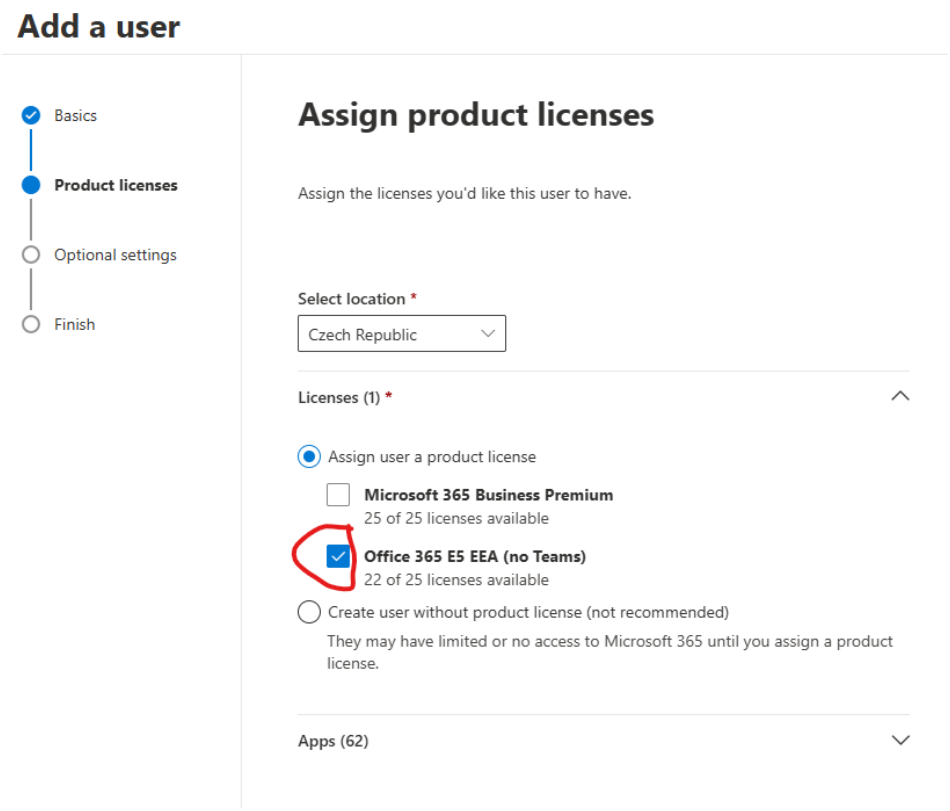


[ICT] GROUP

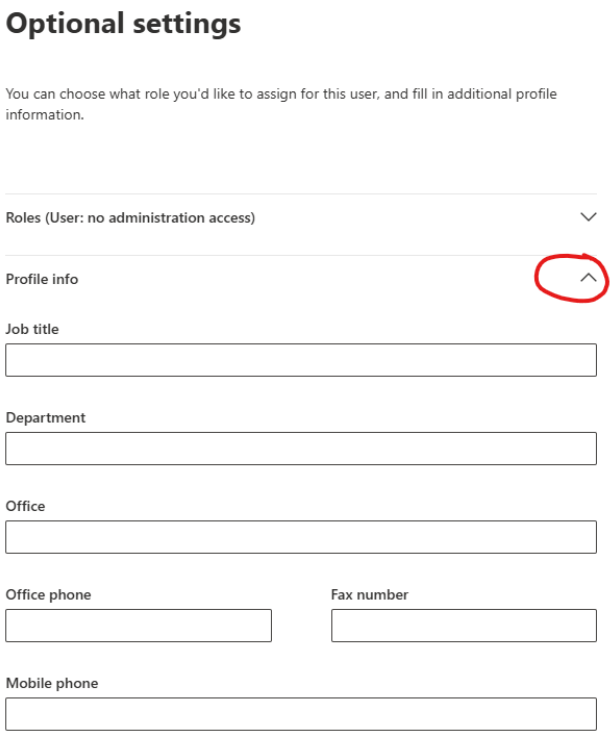
Zadejte jméno, příjmení a email, který budou používat. A nechte zaškrtnuté **Automatické vytvoření hesla** a **vynucení změnění hesla po přihlášení.**



Přidejte licenci

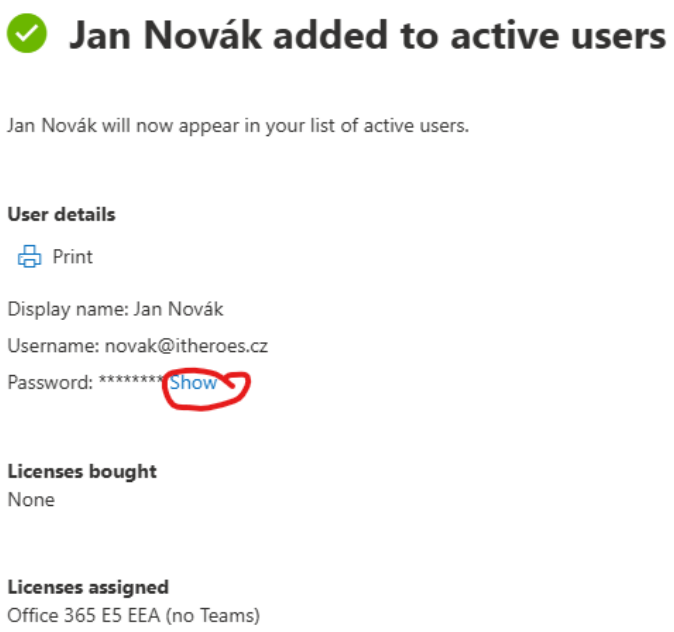


Pod sekcí **Optional settings** (Dobrovolné nastavení) je schované menu **Profile Info** (Informace o profilu), kde můžete přidat pracovní pozici, oddělení, telefonní číslo a další

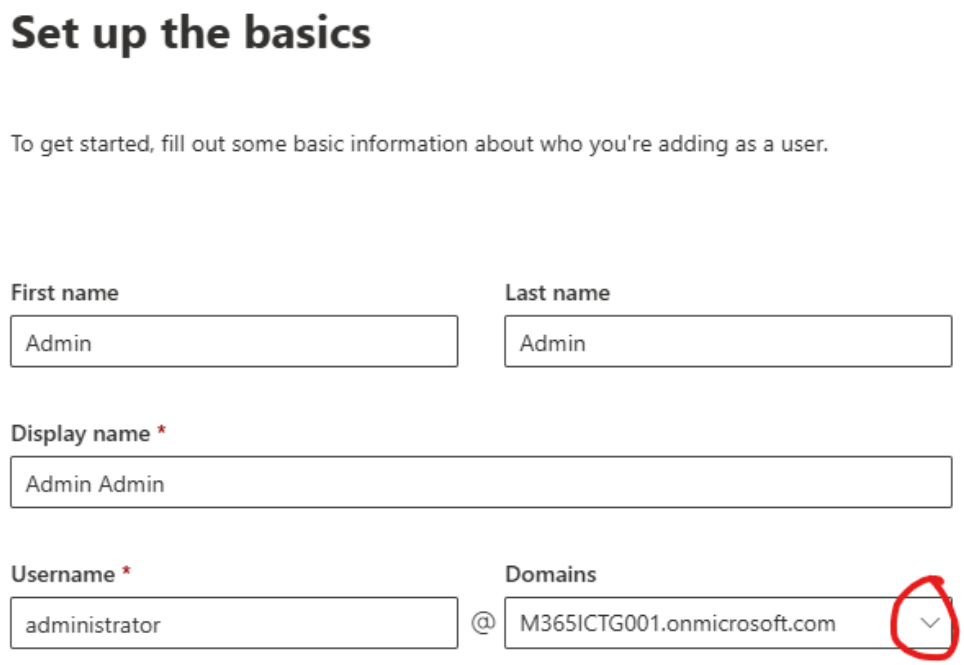


Potom dejte **dokončit**

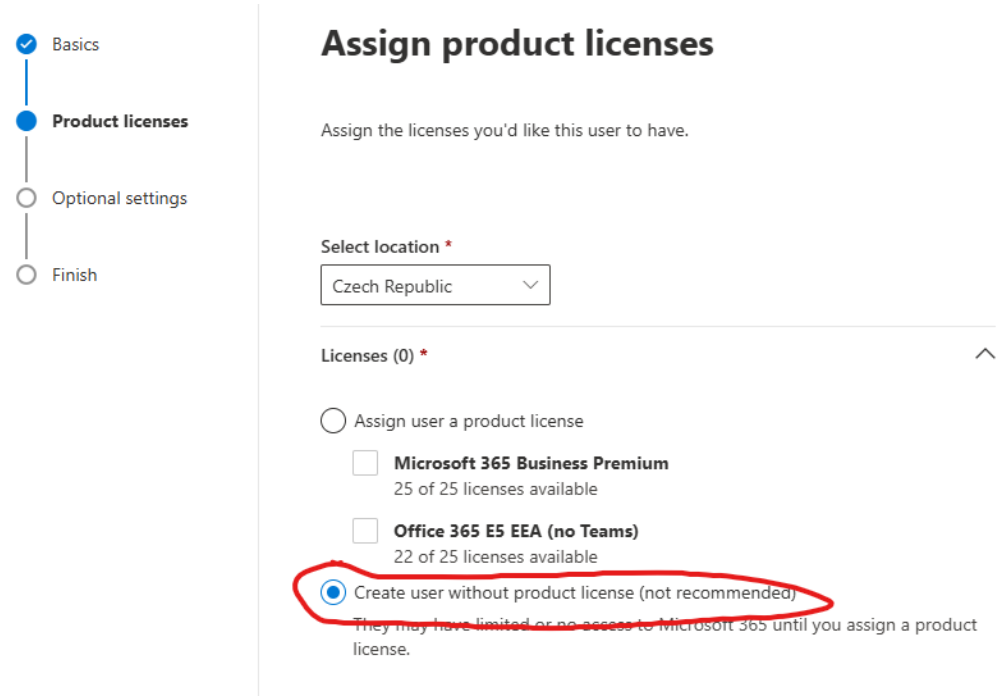
V detailu vám vyskočí informace o vytvořeném účtu. Nezapomeňte si poznamenat heslo. Nemusíte se cítit špatně, že znáte heslo daného uživatele, protože si ho při prvním přihlášení bude muset změnit.



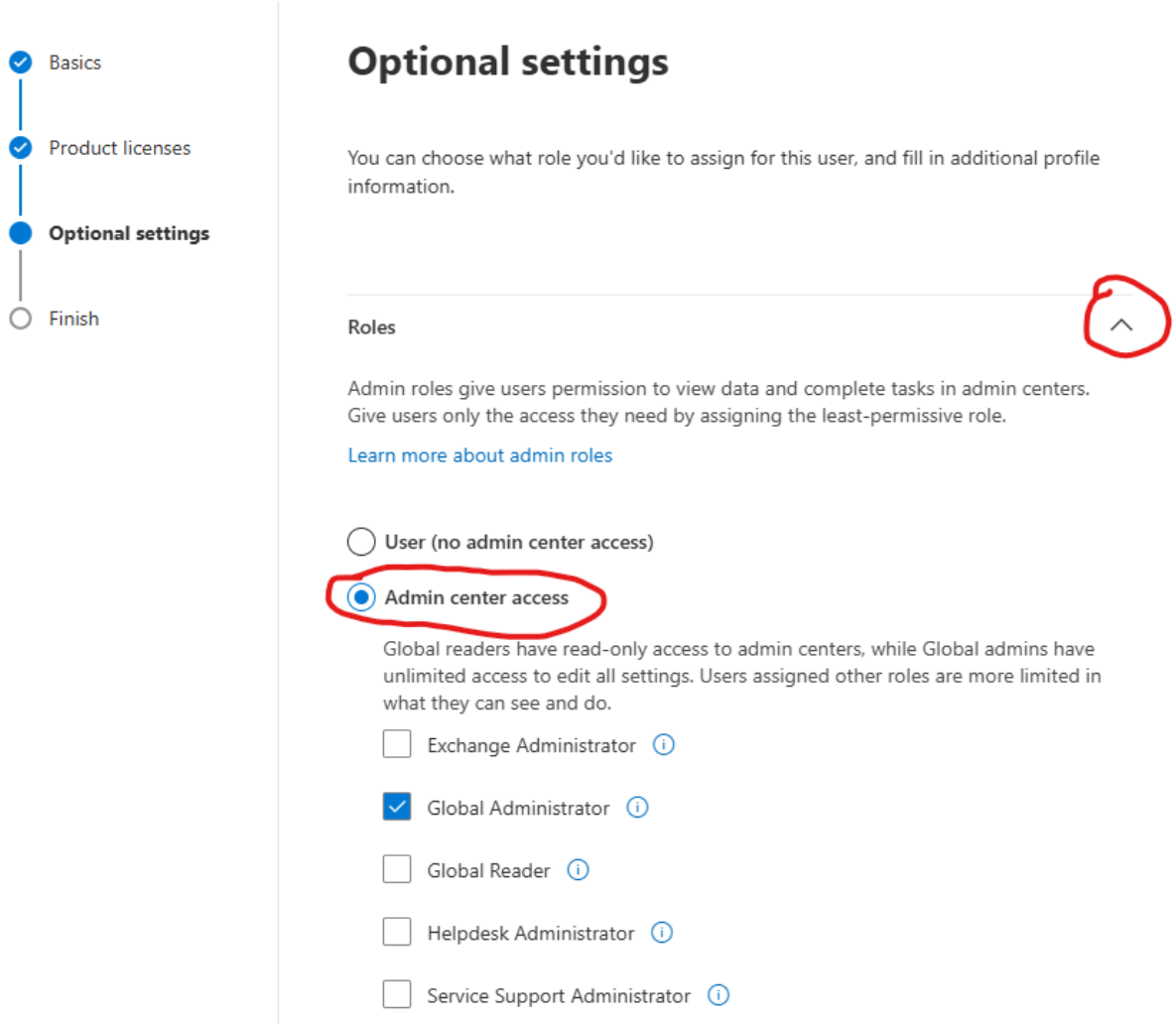
U administrátorů je proces skoro stejný až na 3 věci. Při přidávání emailu vyberte doménu onmicrosoft.com.



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

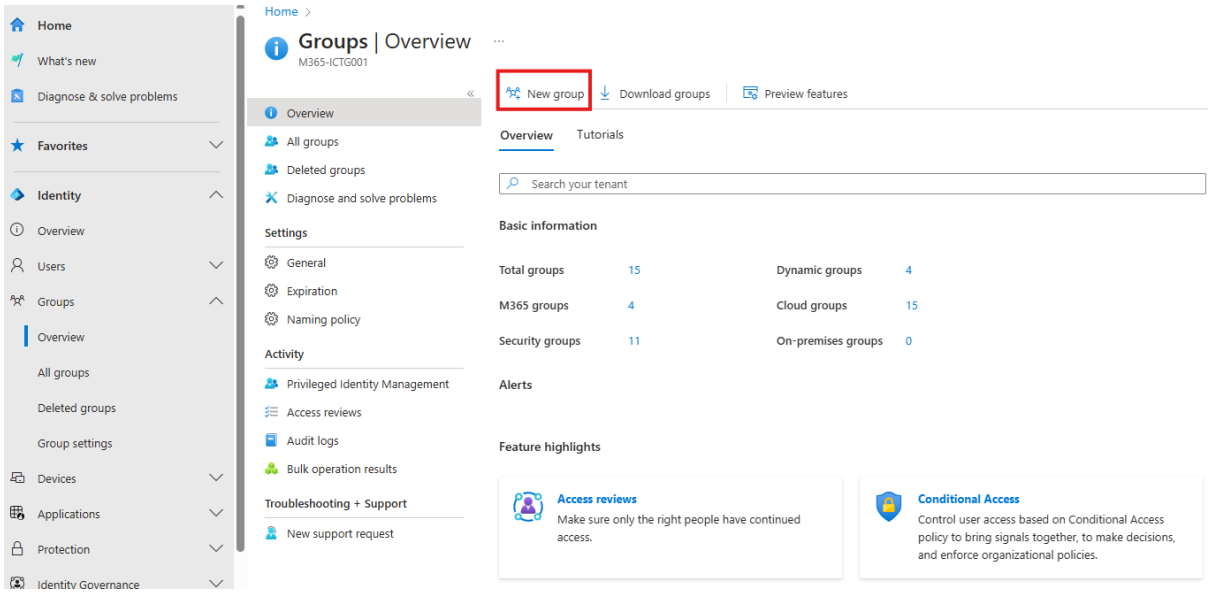
Ať už vám to přijde, jakkoliv otravné, tak udělat si systém v nastavení M365 je absolutně kritické. Nastavení v portálech je hrozně moc a většina věcí se dá nastavit na několika místech. Proto všechno, co děláte musíte označit, jakoukoliv skupinu lidí nebo zařízení zařadit do tzv. security skupin. U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

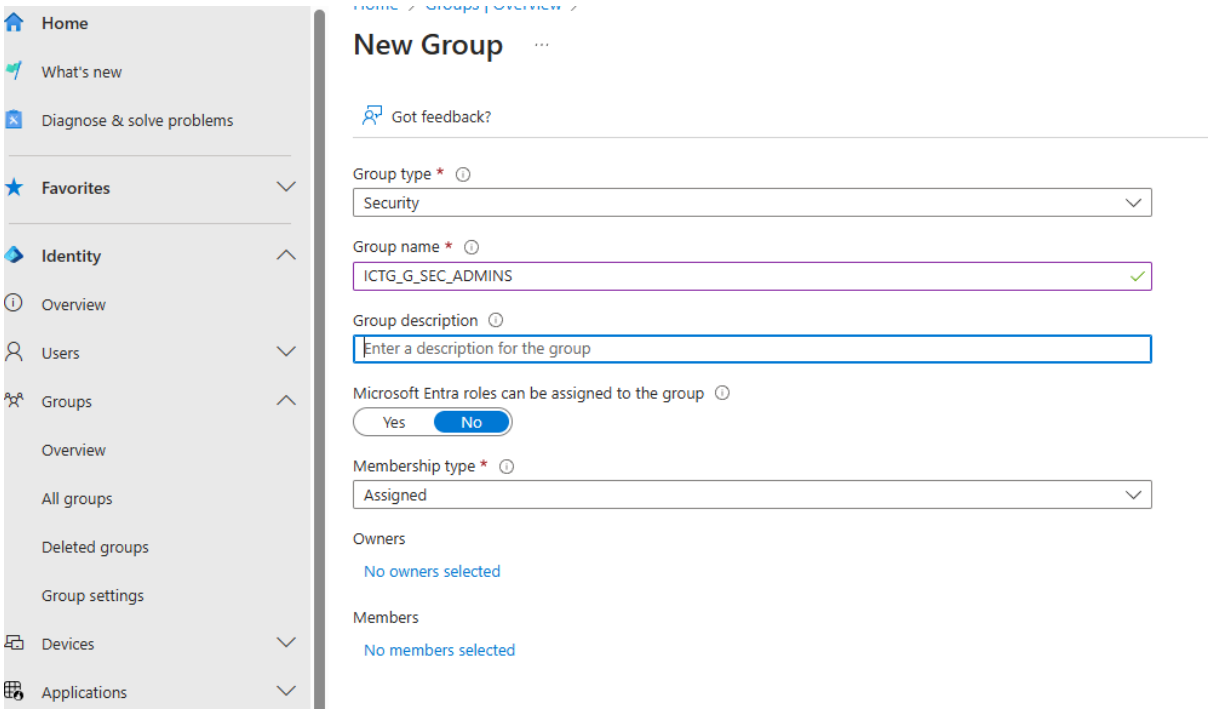
Jak vytvořit security skupinu.

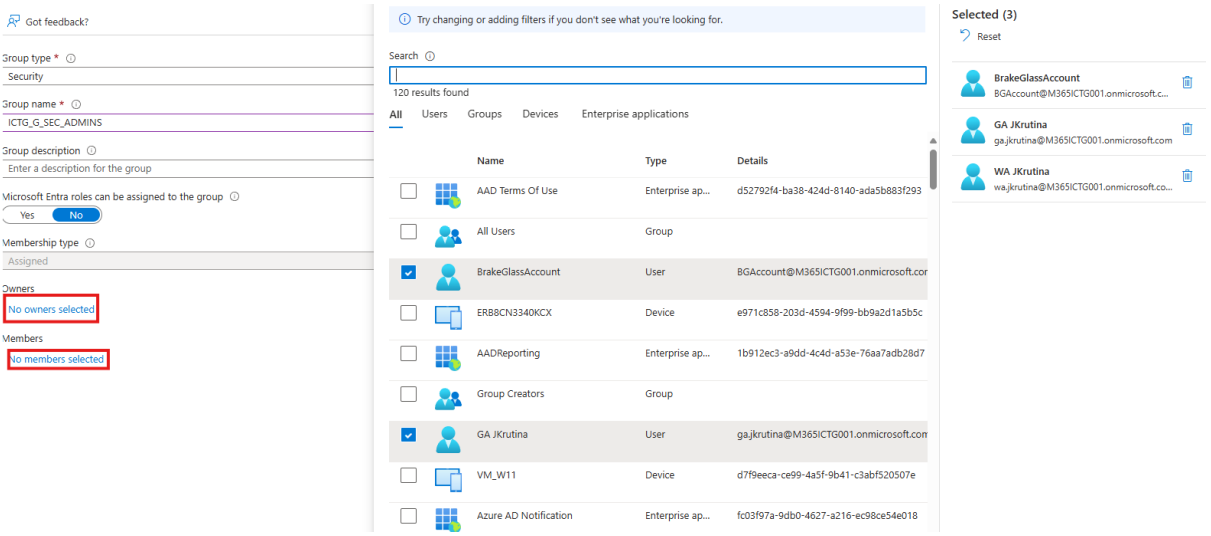
Jde to z více míst, ale já vám ukážu jak na to z Microsoftem doporučované https://entra.microsoft.com/.

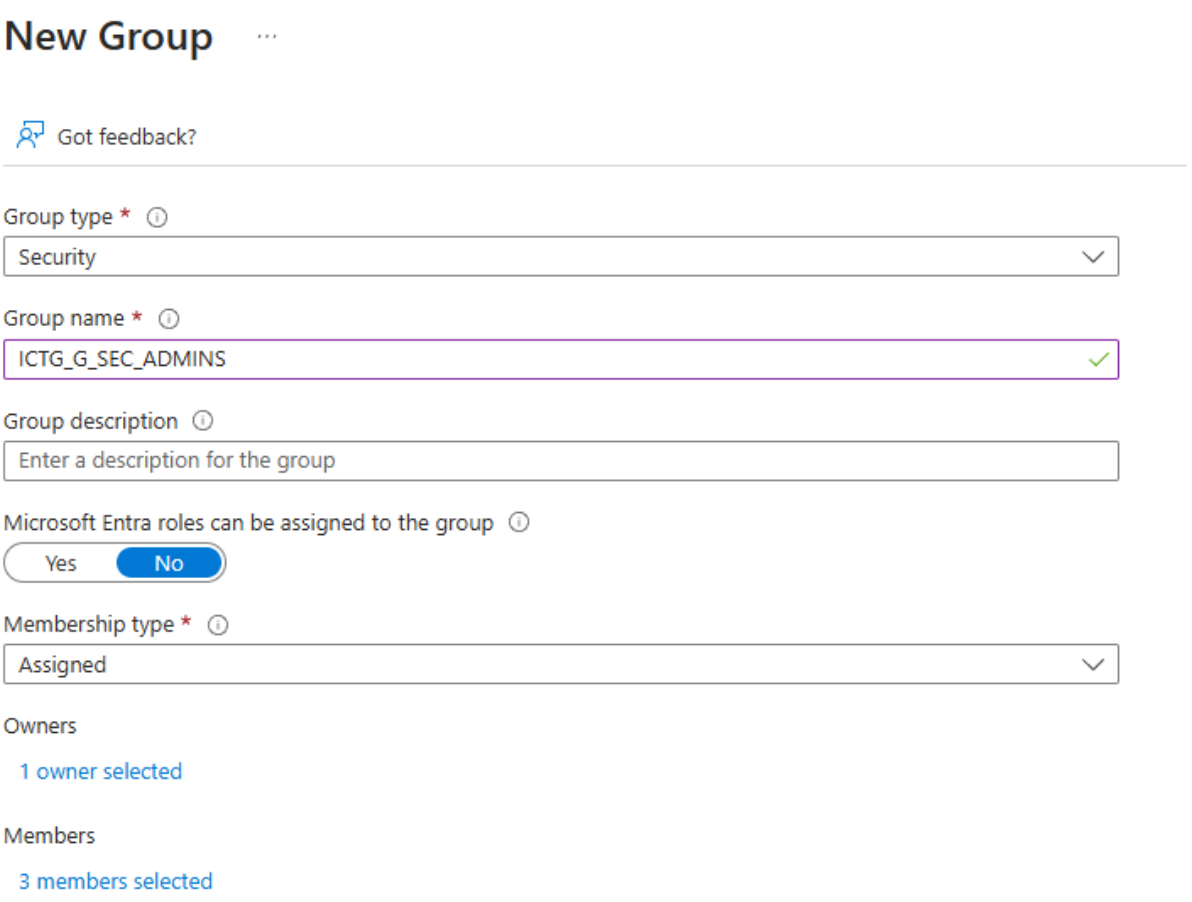
Otevřete si Groups - Microsoft Entra admin center

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 * ⓘ

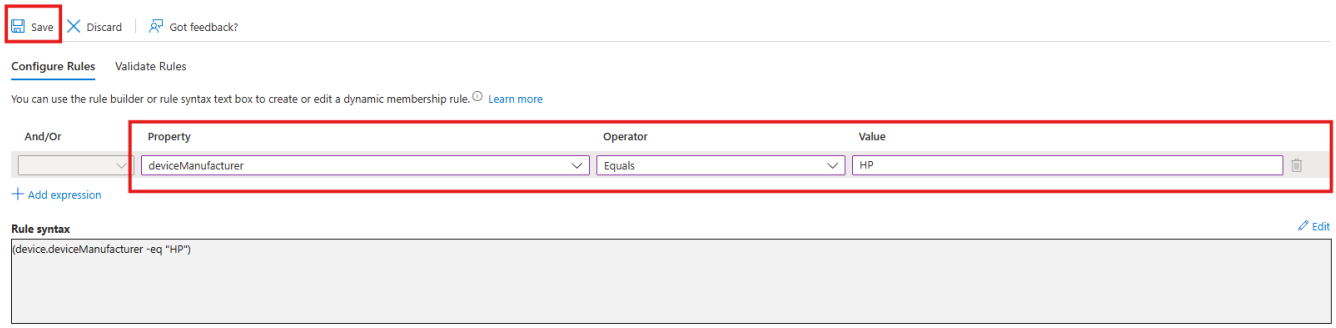
Dynamic Device

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.

Entra

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

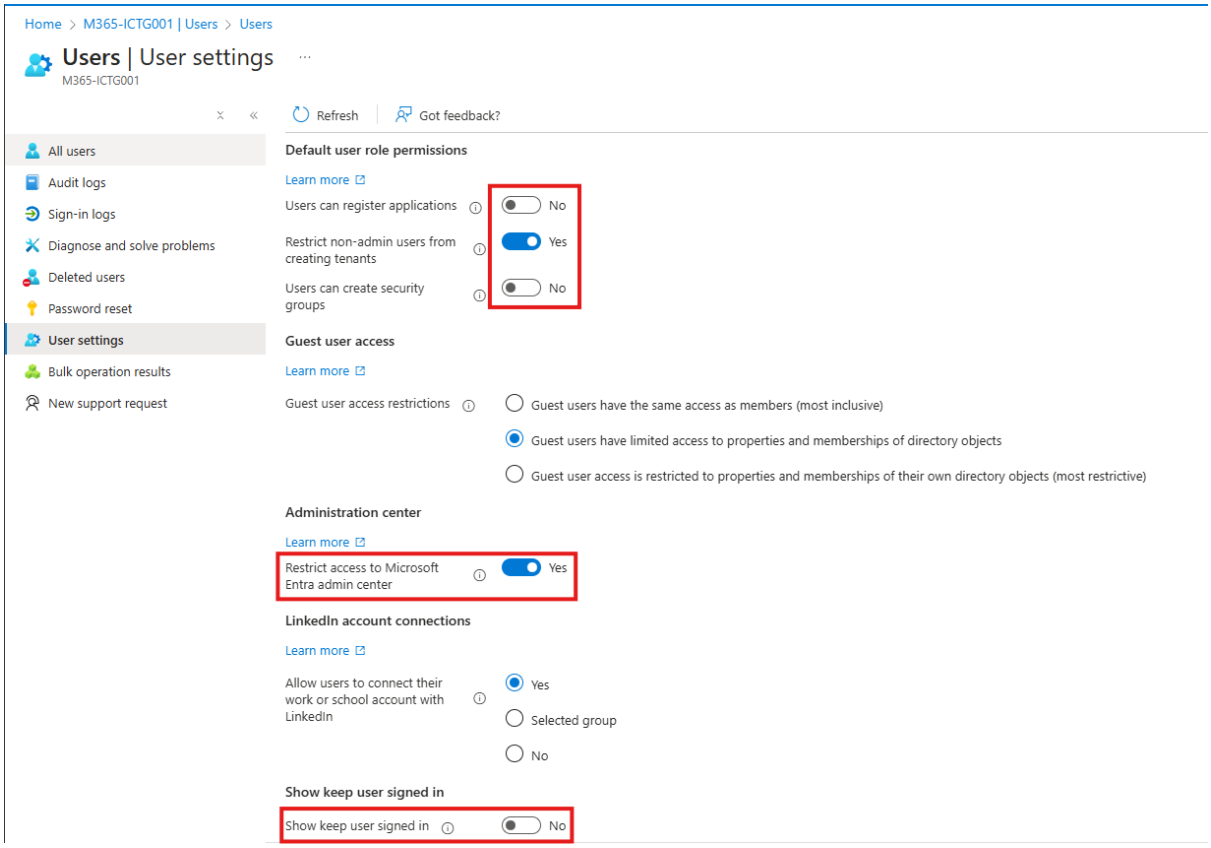
Users can register applications chcete mít vypnuté vždy, krom toho, kdy by vaši uživatelé vytvářeli aplikace v Azure prostředí.

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.

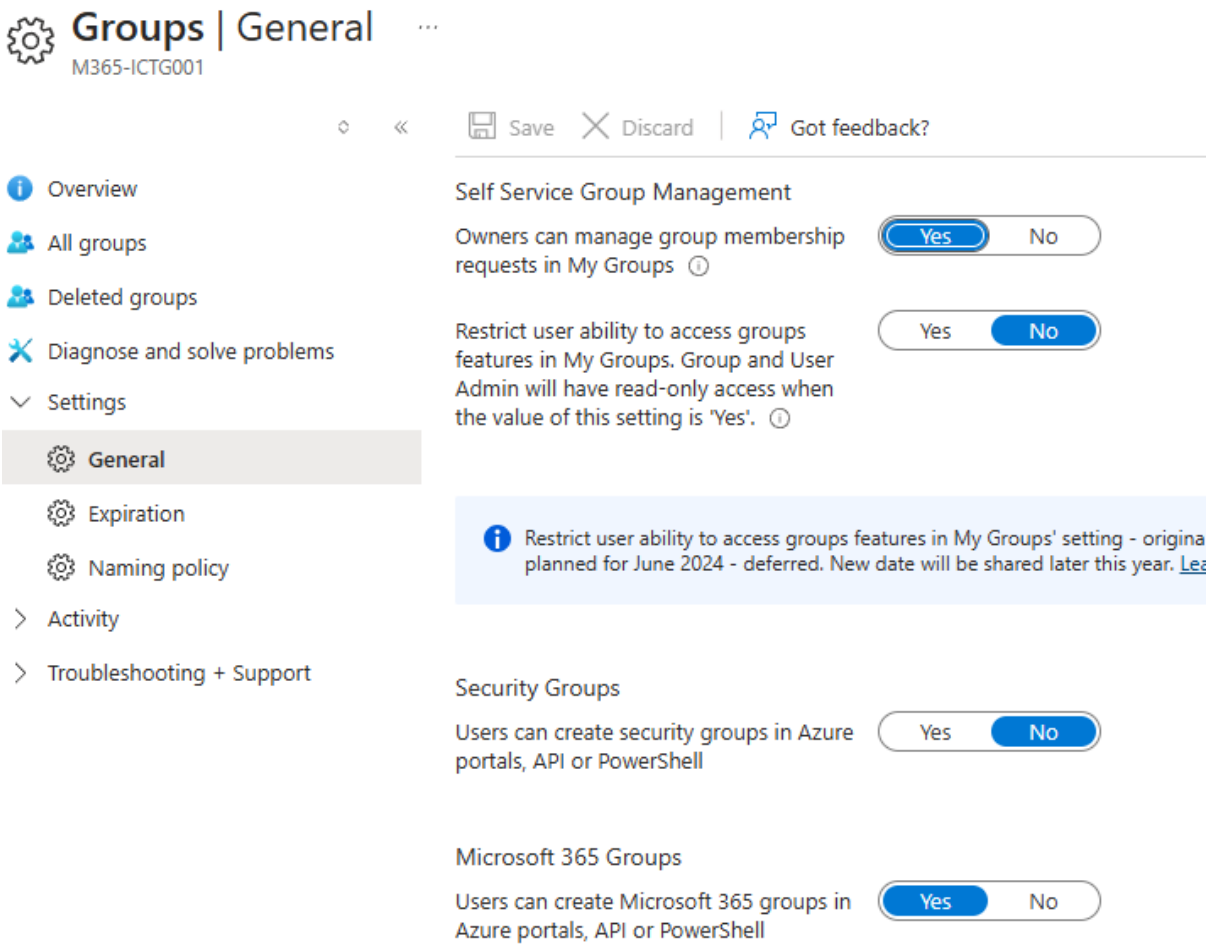
Show keep user signed in toto nastavení zobrazuje uživatelům možnost zaškrtnou „zůstat přihlášen“ okno. Tím se cookie s přihlášením uloží na disk, což může být problematické, kdyby byl počítač zavirovaný.



[ICT] GROUP

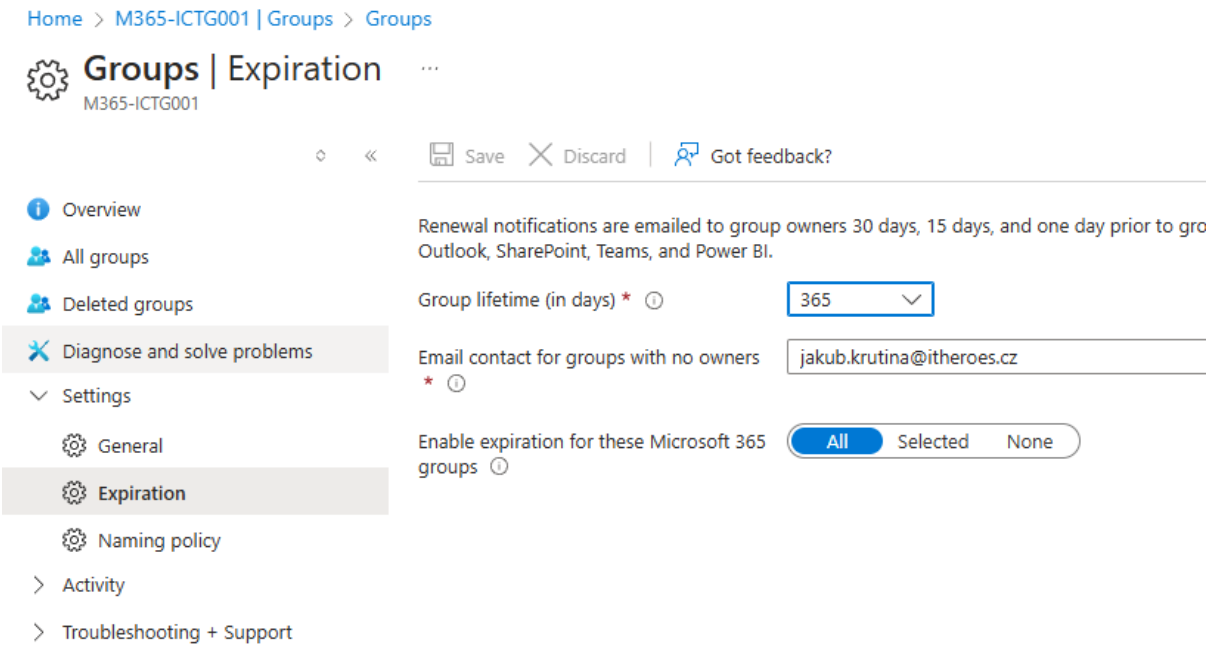
Nastavení skupin – základní nastavení skupin je velmi jednoduché a asi nepotřebuje vysvětlení, krom vyváření M365 skupin. Když vypnete toto zaškrtávátko, tak uživatelé nebudou schopni vytvářet týmy v Teams, ani jako administrátoři. Jediné, kde bude možné vytvářet týmy bude Teams admin centre

Groups - Microsoft Azure

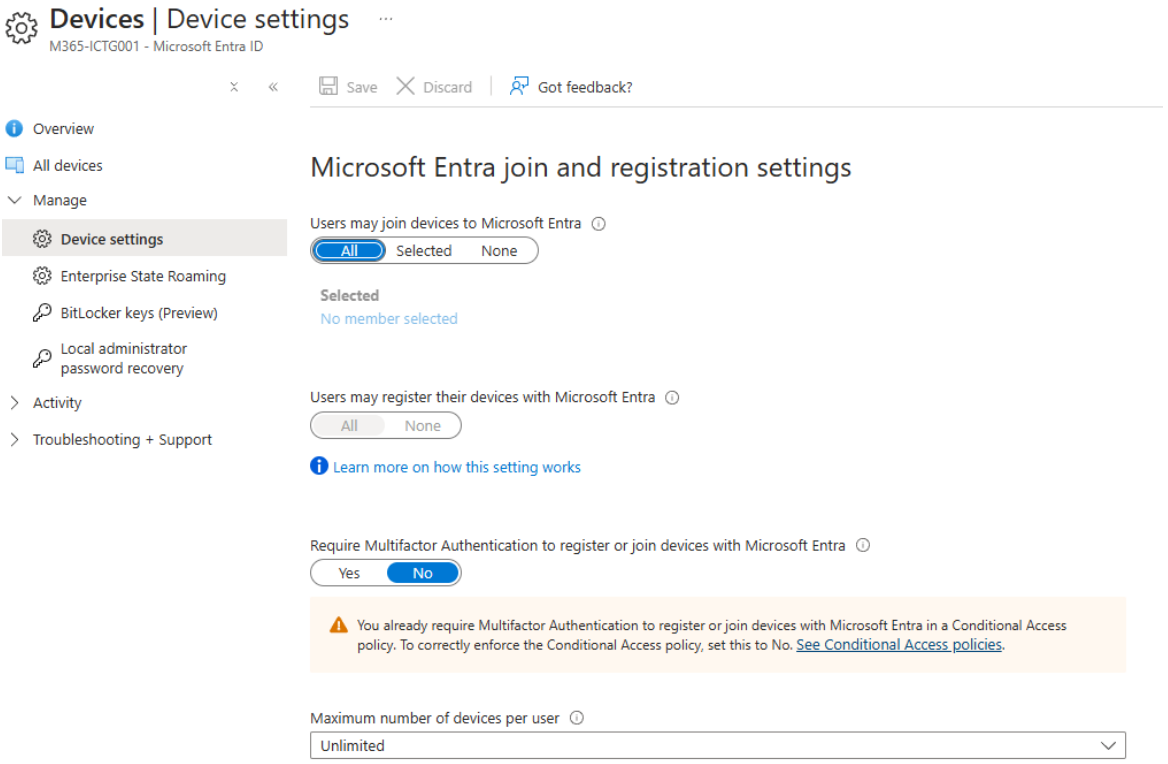


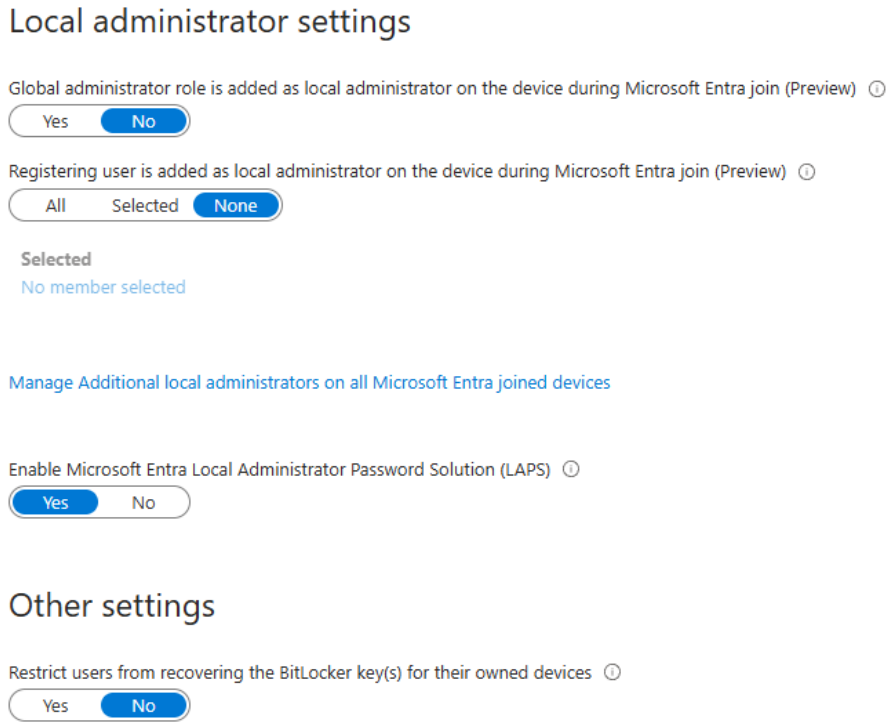
Ta zajímavější pasáž je expirace skupin. Ta může být velmi důležitá, ale také vám může dost uškodit. Hlavní věc je nastavit e-mail kontakt na někoho kdo ve firmě zůstane, ideálně vy samy. Toto nastavení je proto, aby skupiny bez vlastníka po vypršení expirace mohly být obnovené. Normálně přijde e-mail 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

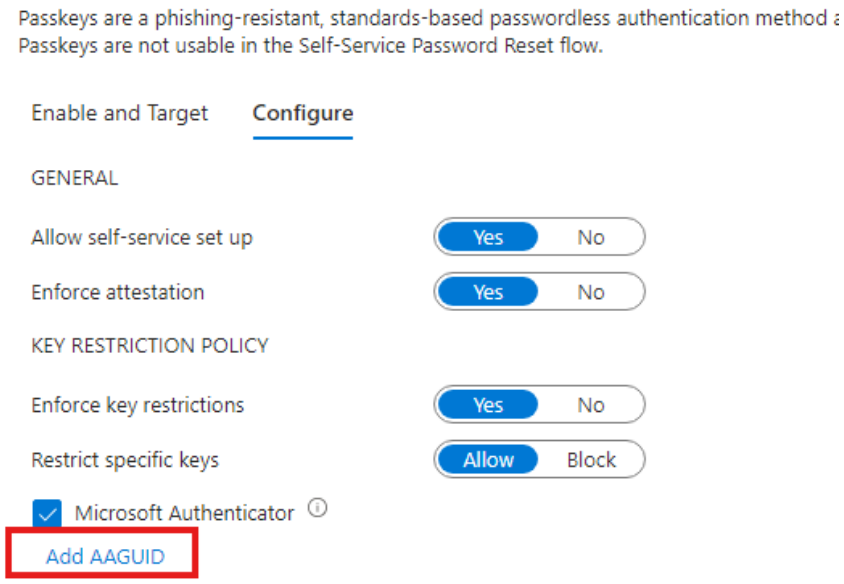
Zabezpečení uživatelských účtů

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).

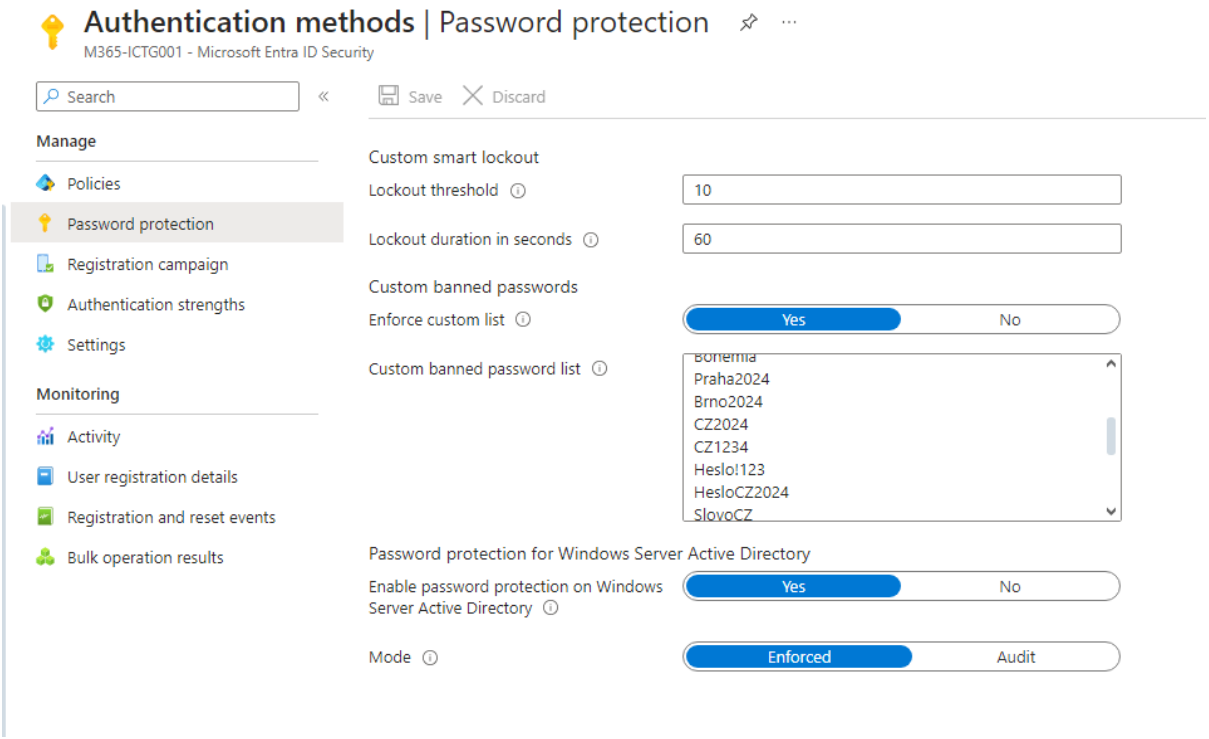
Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)	All users	Yes
Third-party software OATH tokens	All users	Yes
Voice call		No
Email OTP		No
Certificate-based authentication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

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



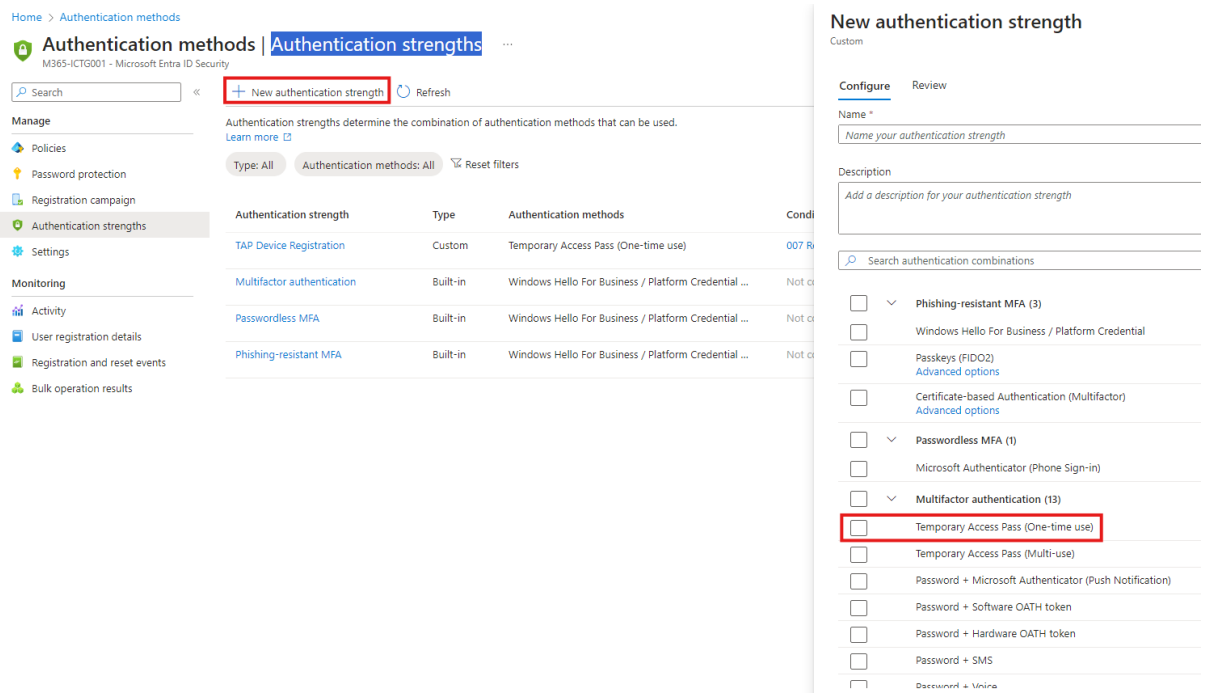
Další, na co se podíváme je **Password Protection**. Toto je velmi zajímavá věc, která vám umožňuje nastavit list zablokovaných hesel, můžete jich mít až 1000, velká a malá písmena se nezohledňují a rovnou blokuje substituce jako je 0 za o nebo 5 za s. Toto vám umožňuje vyhnout se velké části slovníkových 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/

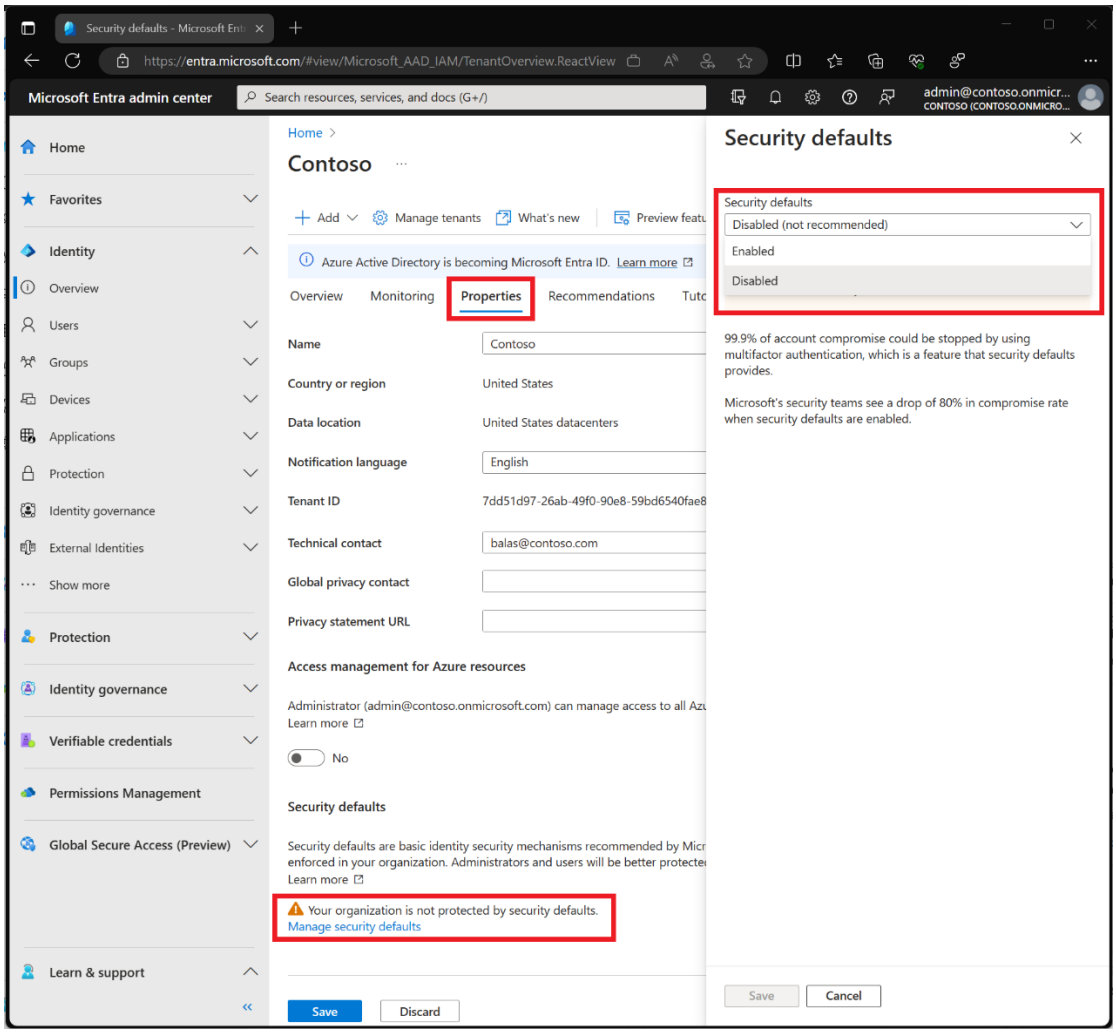


Samozřejmě můžete použít i multi-use TAP (Temporary Access Pass). Potom stačí jenom dát vytvořit a máte hotovo!

[ICT] GROUP

Conditional Access Policies!

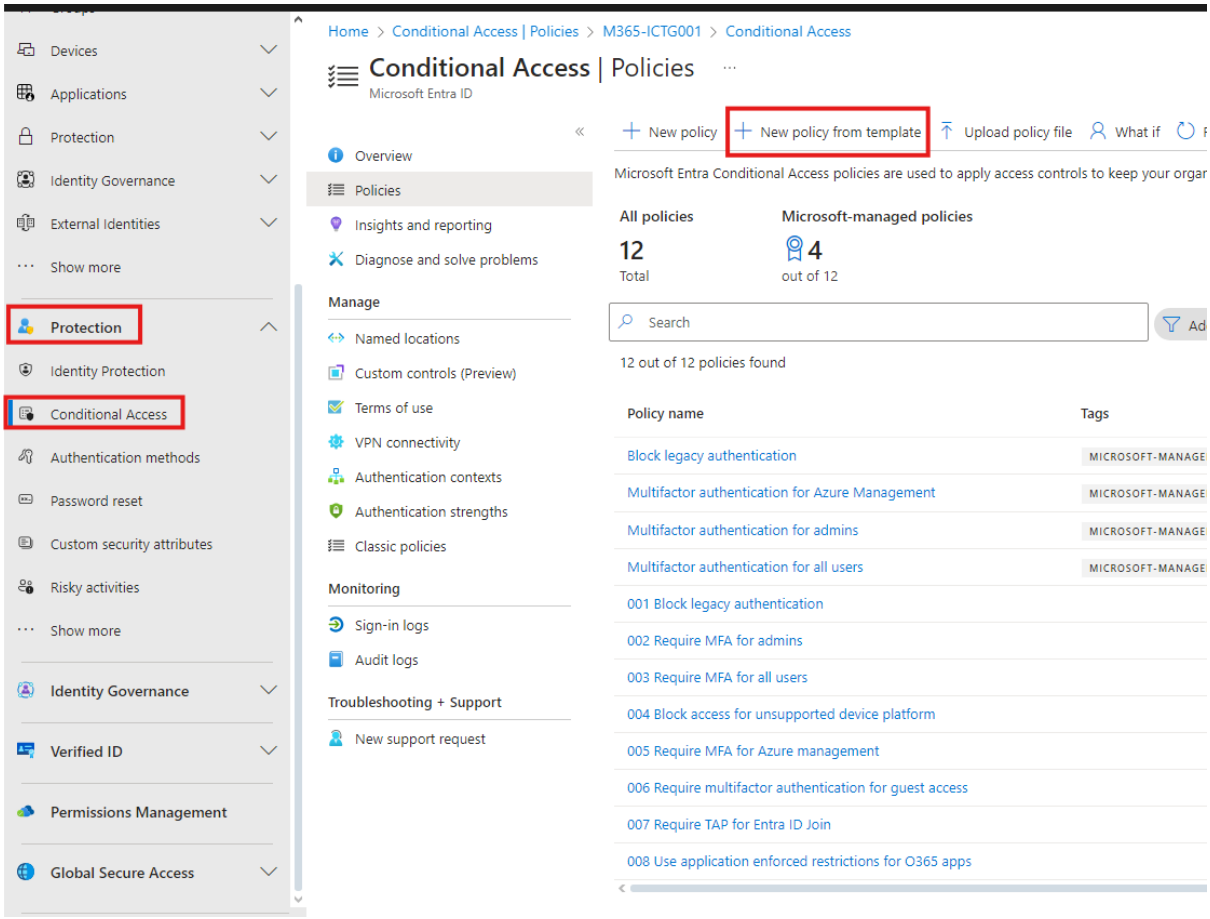
Conditional Accass Policies neboli **CAP** jsou hlavním ochranným prvkem po silných a unikátních heslech, a proto pokud máte tu možnost, tak si je rozhodně nastavte.
V dnešní článku si ukáže prvních pár, v příštím článku si ukážeme zbytek. Velmi důležitá věc, než začneme, buďte s implementací **CAP** 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

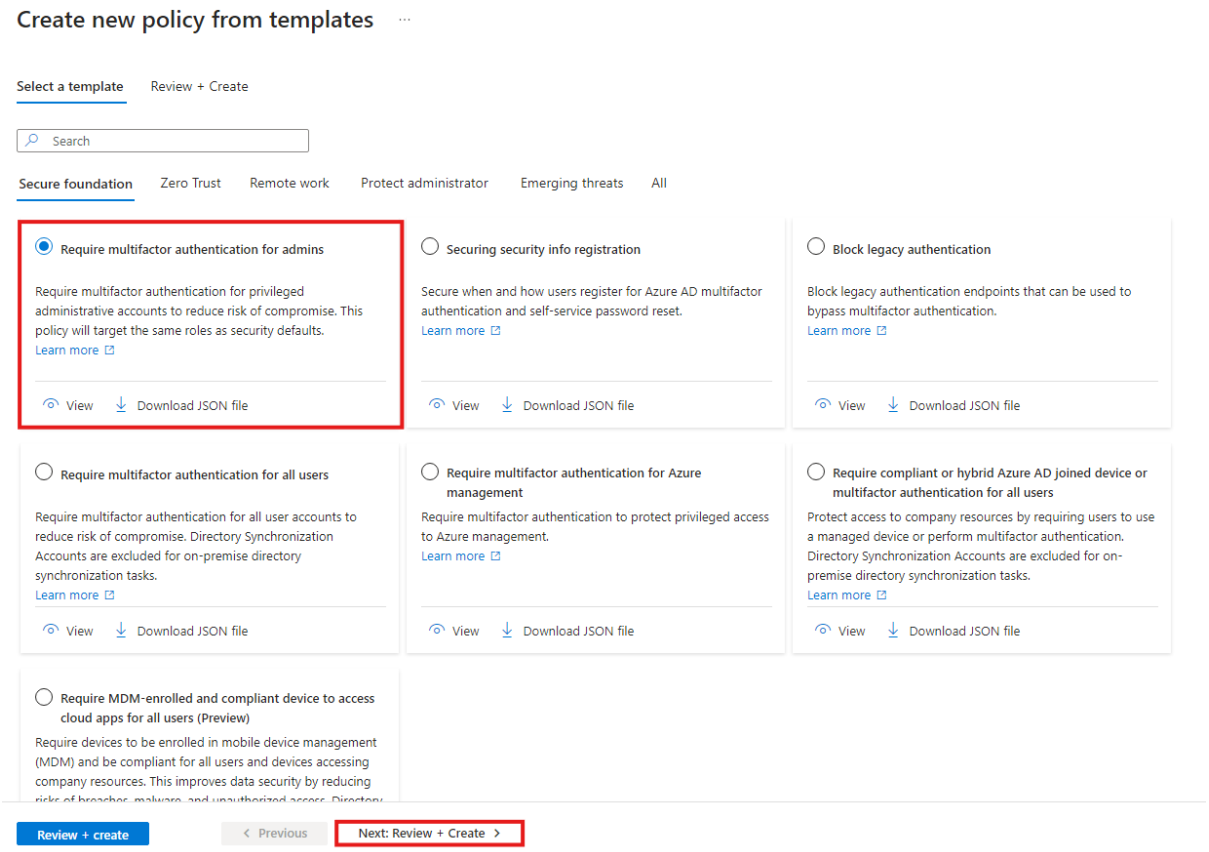


Teď na nastavení **CAP**! První věc, kterou nastavíme je **require MFA for admin** (vynucení MFA pro administrátory) a použijeme na to už předvytvořenou šablonu od Microsoftu. Otevřete si portál **Entra**, přejděte k **protection** a pod tím **Conditional Access**.

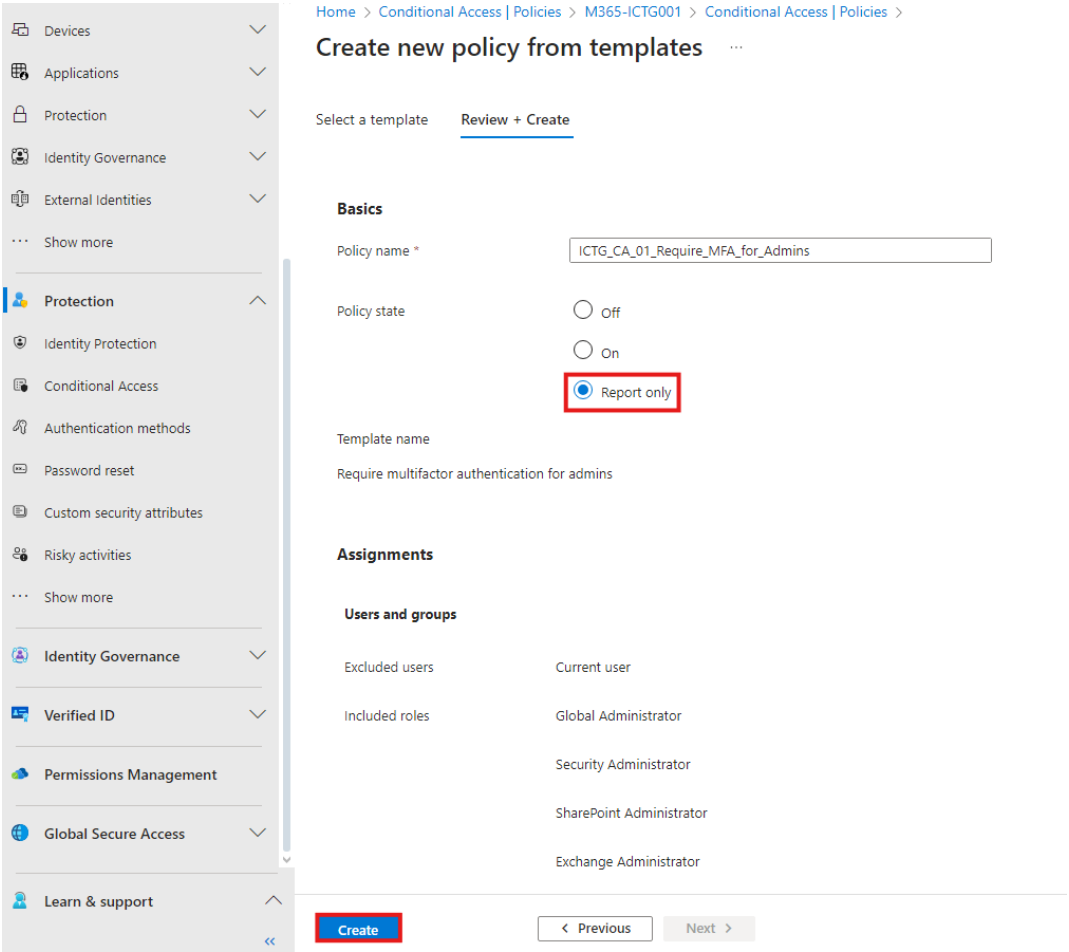
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies/fromNav/

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

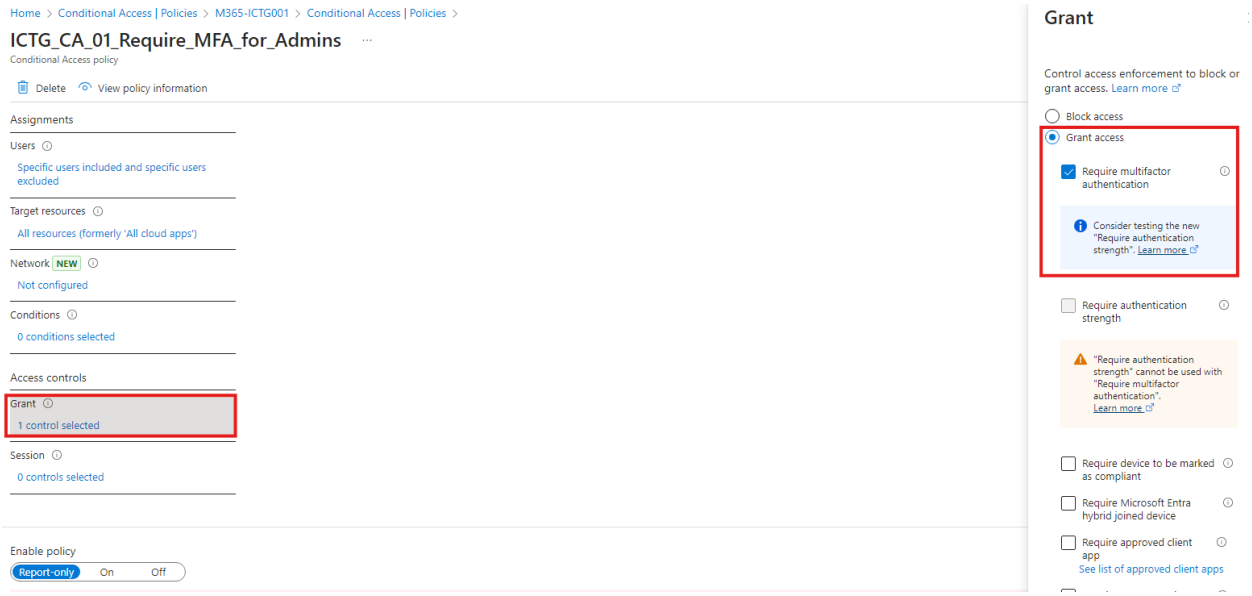




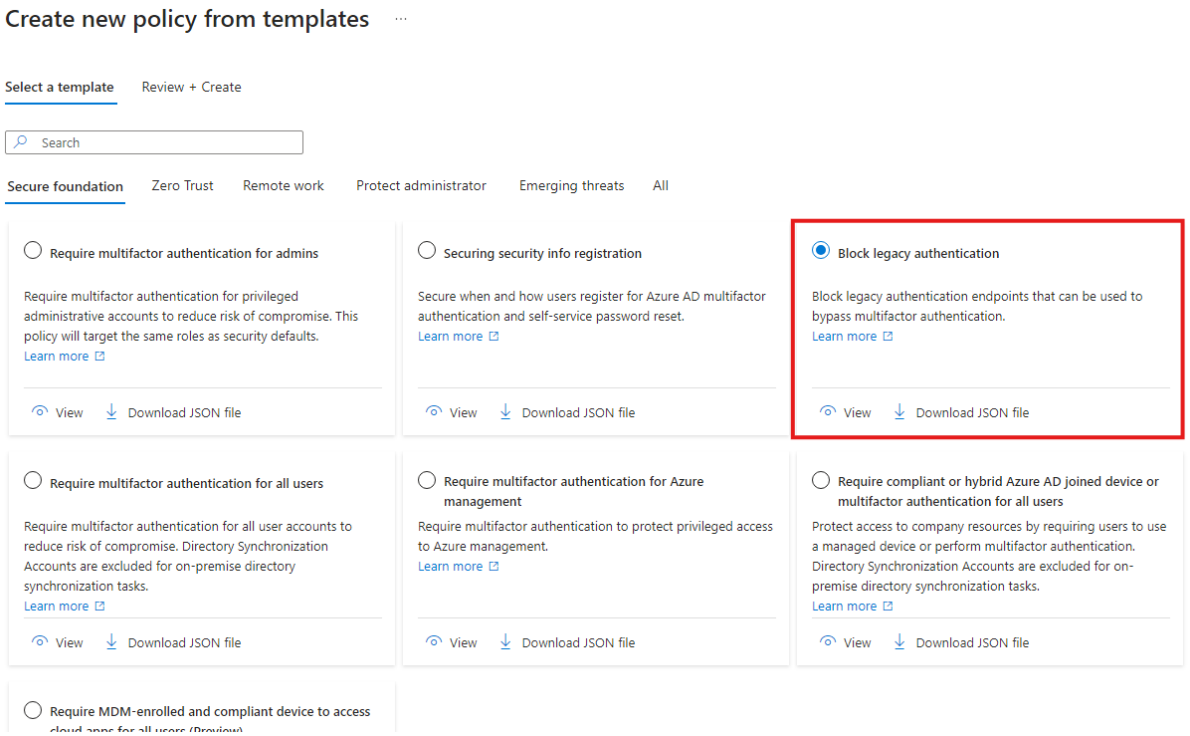
Zezačátku nechte politiky v módu **Report Only**, zjednoduší vám to doladění a testování. Taky silně doporučuji nastavit si jmennou konvenci u **CAP** a přidat do jména číslo politiky, velmi vám to usnadní řešení problémů.



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!

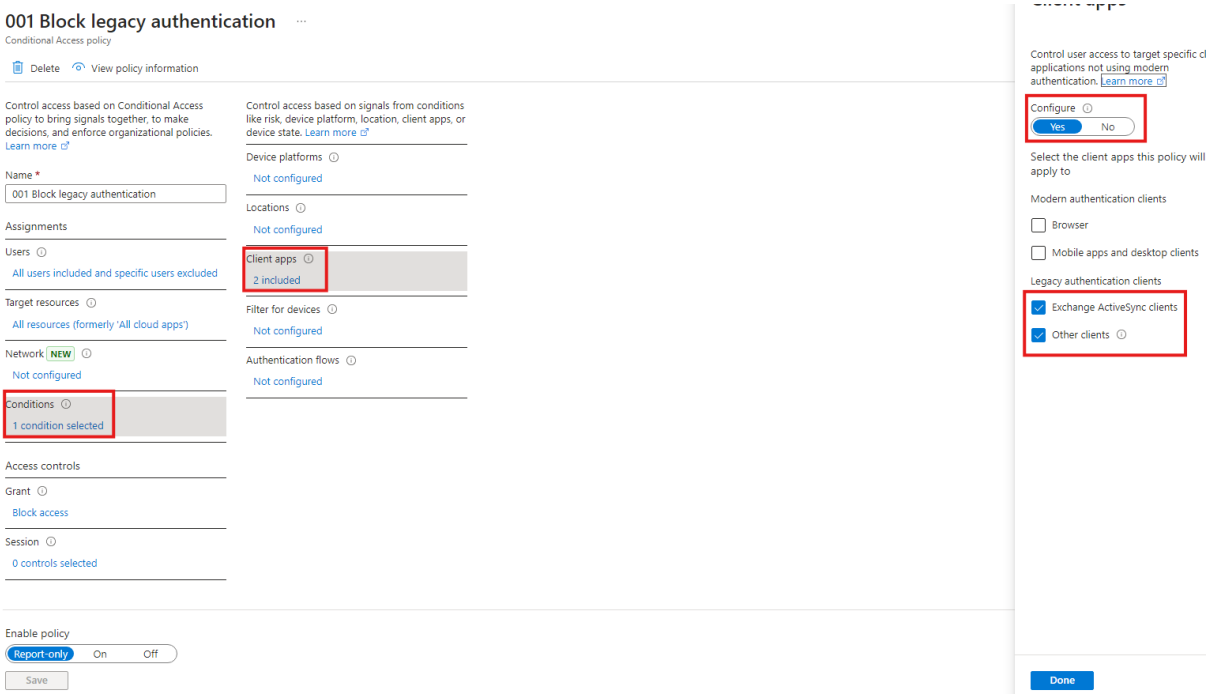


Teď přejdeme k další politice, a to je **Block Legacy Authentication.**



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.**

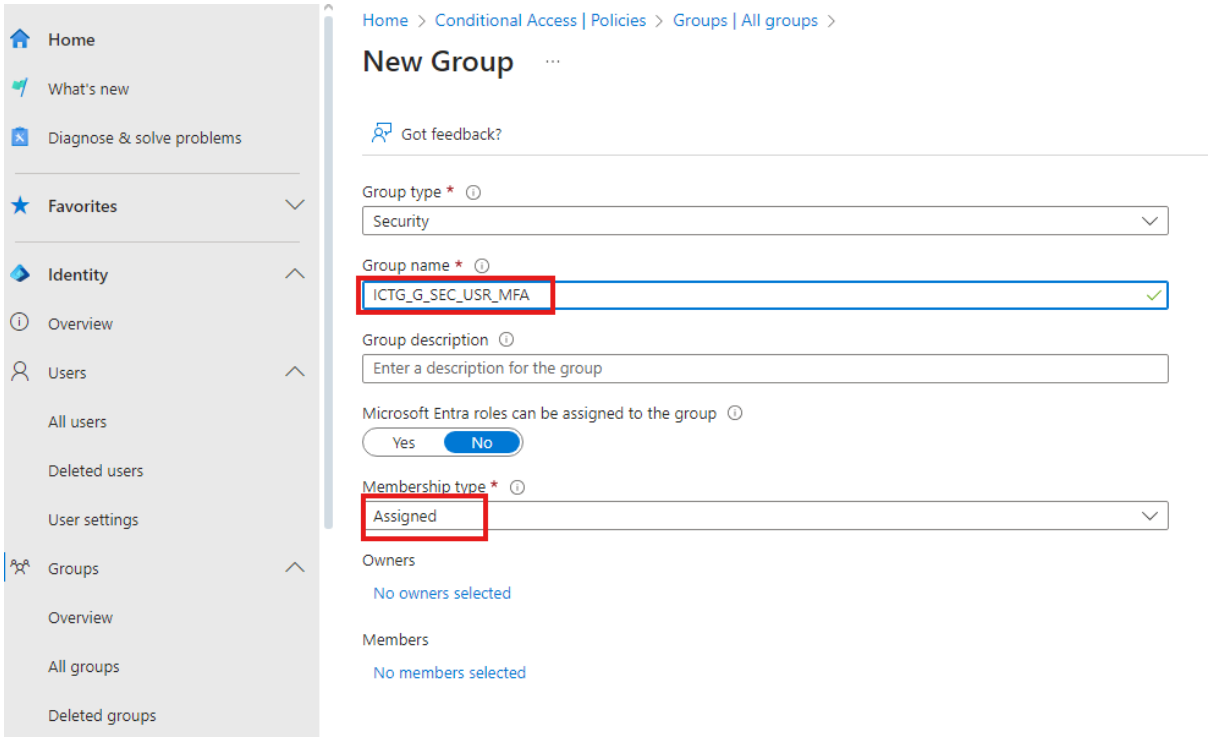
[ICT] GROUP



Conditional Access Policies část druhá!

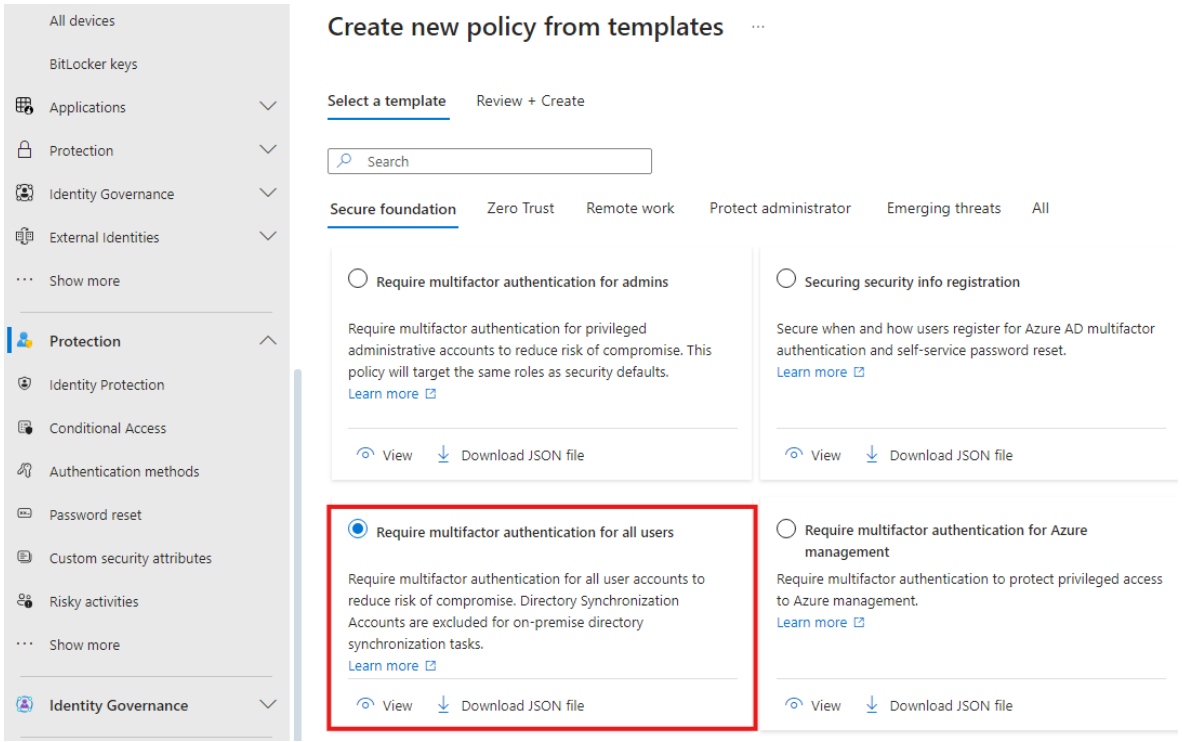
V dnešním článku si projedeme další část **CAP**, které doporučuji jako základní nastavení pro kohokoliv s **Business Premium** tenantem. Samozřejmě kreativitě se meze nekladou a pokud něco specifického budete potřebovat povolit nebo zablokovat, tak to přes **CAP** skoro určitě půjde. Další politika, 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

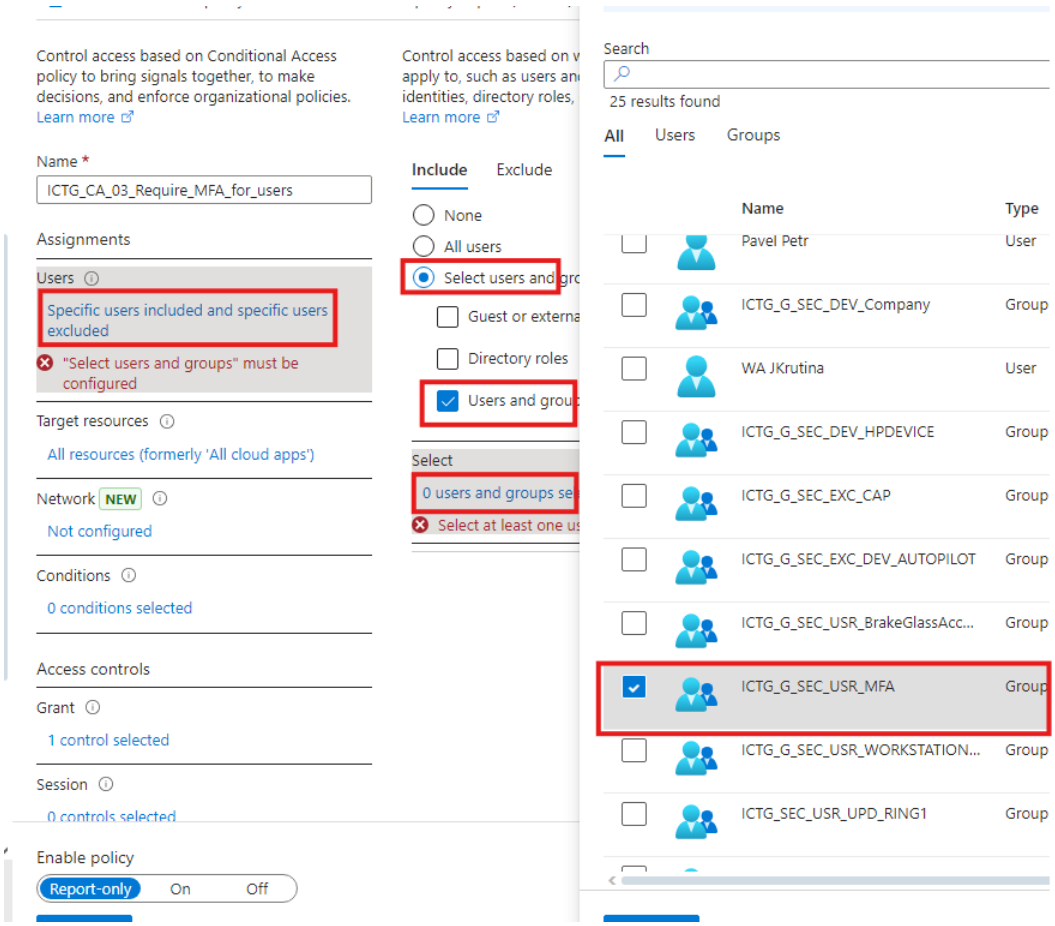
Users and groups

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

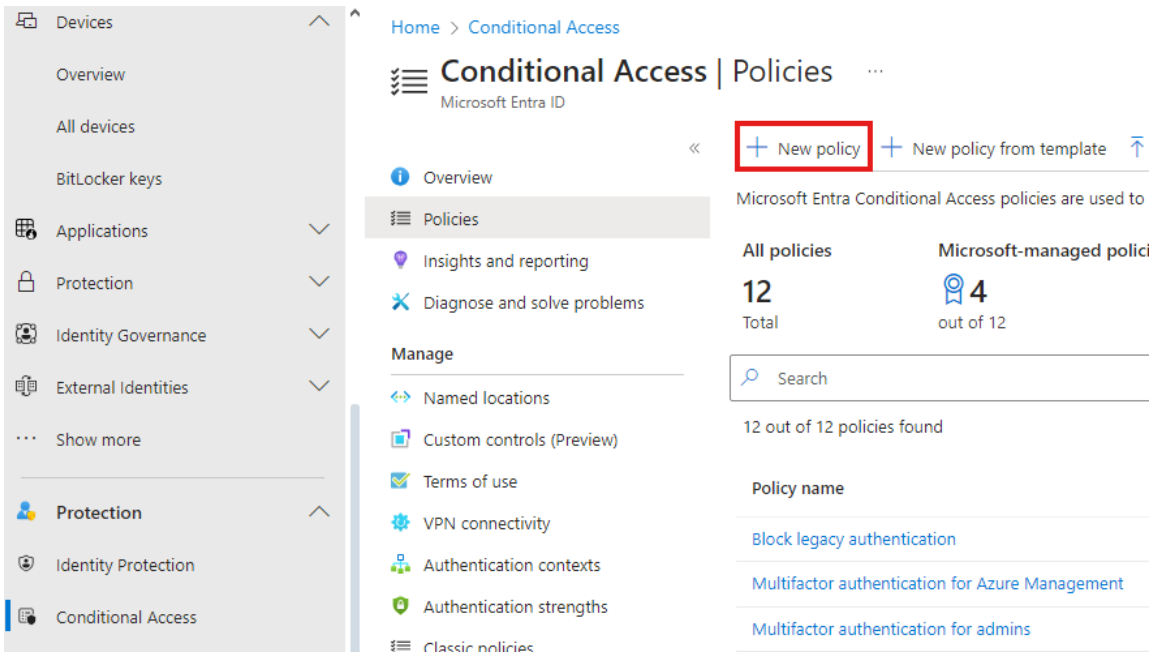
Cloud apps or actions

Create | < Previous | Next >

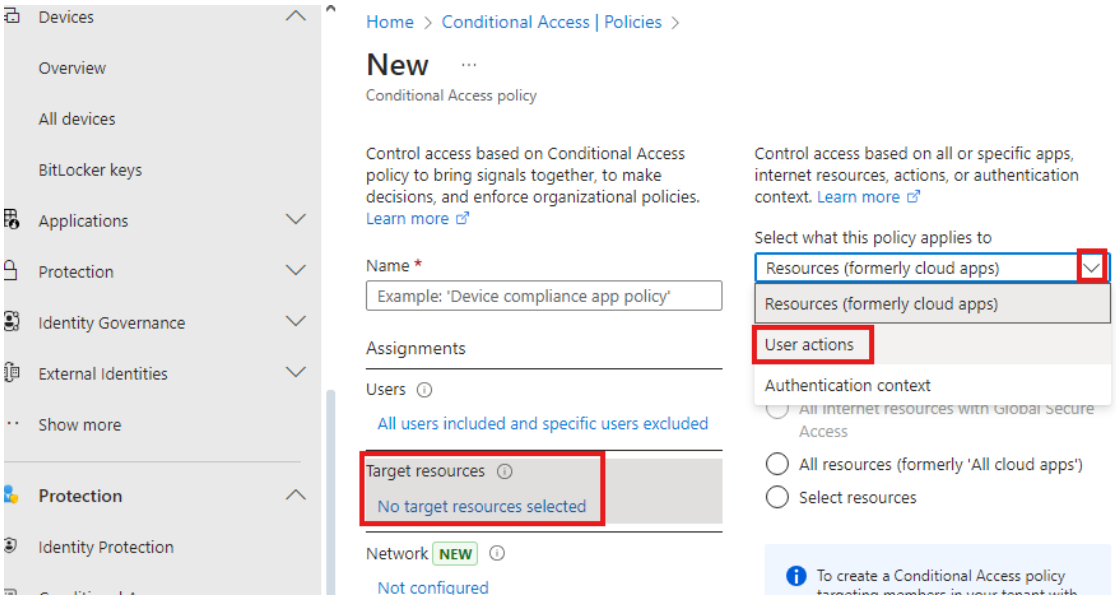
Teď si politiku otevřete, vyberete **users,** poté **Select users and groups, Users and groups** a nakonec přidejte svoji skupinu, kterou jsme vytvořili v předchozím kroku. Poté už stačí jenom vyndat přes **Exclude** účty záchrany a máte hotovo!

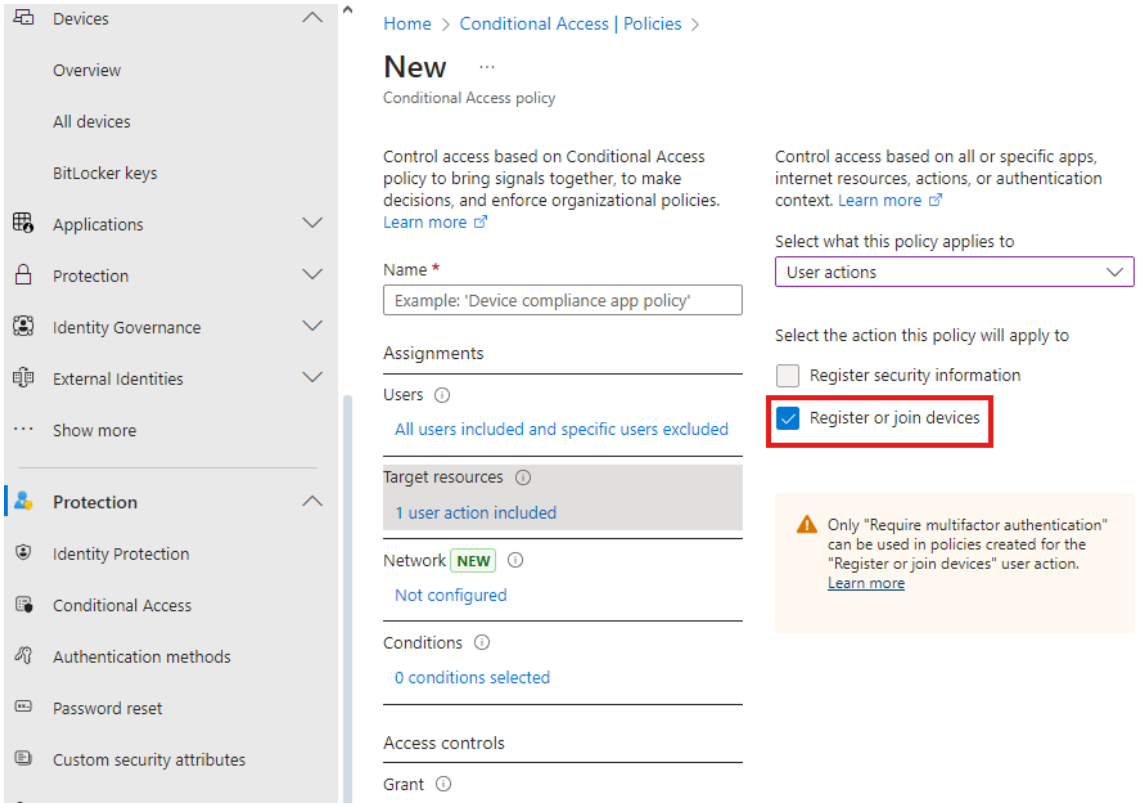


Teď si vytvoříme politiku, díky které bude vynucený **TAP** pro připojení zařízení k **Entra ID**. V menu, kde jste doteď vytvářeli politiky přes šablony si teď vytvoříme politiku, na kterou šablona není.



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.

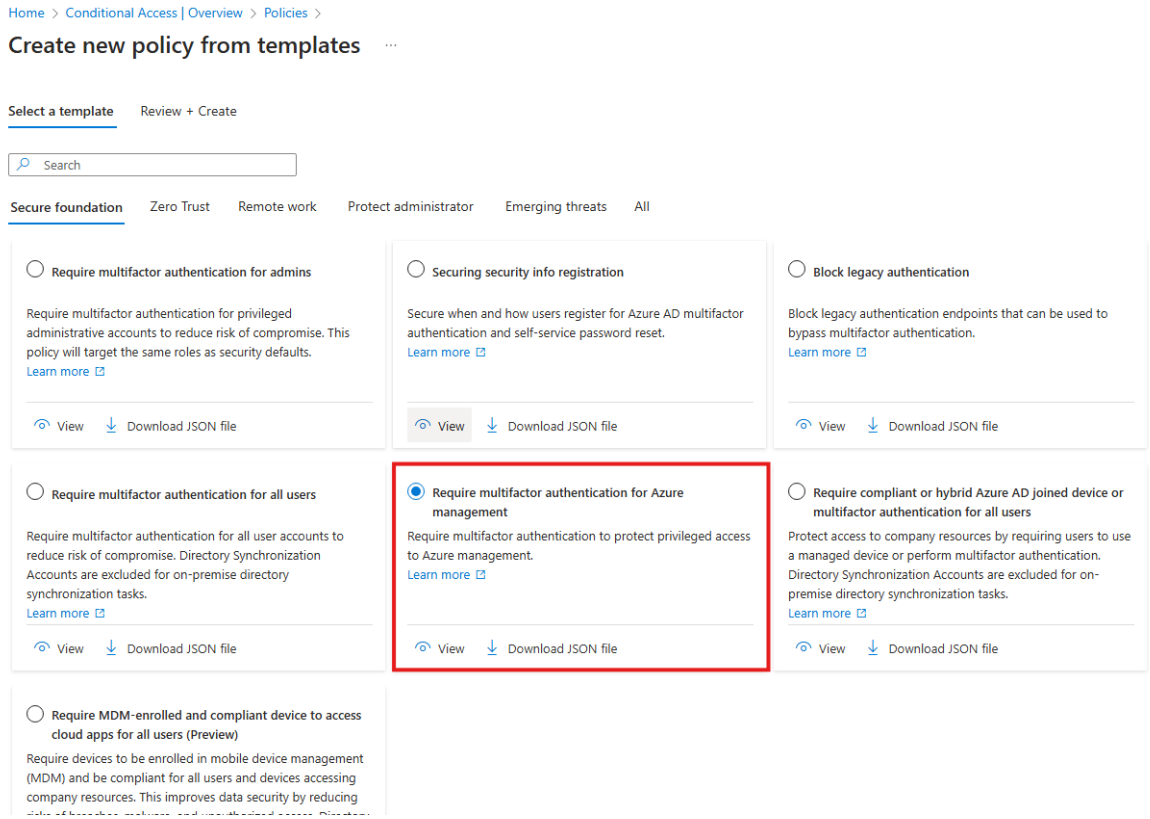
Pak už stačí jen uložit v **Report-only** módu a máte to.

[ICT] GROUP

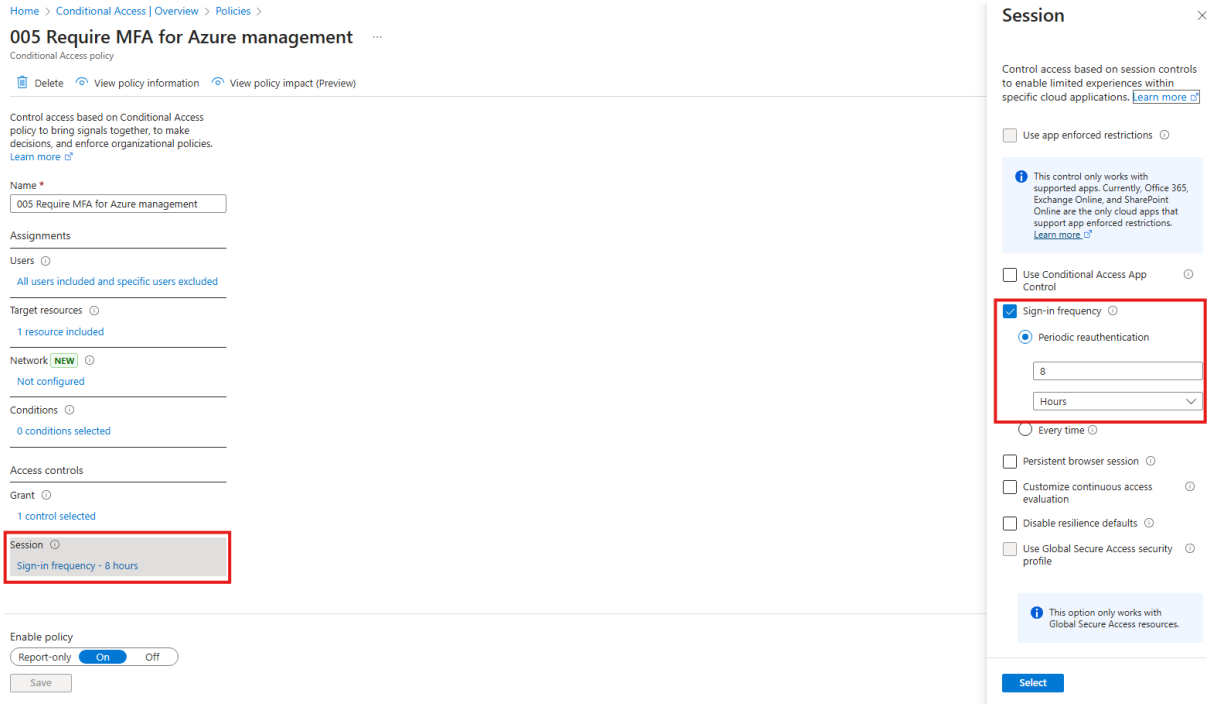
Conditional Access Policies poslední část!!!

Bylo to dlouhé tažení, ale jsme na konci mého základního doporučení. Dbejte na slovo základní, protože s **CAP** je možné si opravdu vyhrát. V dnešním článku si teda probereme poslední 3 politiky, které budou zahrnovat vynucení více faktorového ověřování pro tzv. **Azure management**, který zahrnuje všechny správce virtuální infrastruktury v **Azure**, vynucení více faktorového ověřování u externistů a hostovských účtů a vynucení používání Microsoft aplikací pro přístup k firemním datům a účtům. Všechny politiky je možné vytvořit z katalogu od Microsoftu, takže je projedeme trochu rychleji.

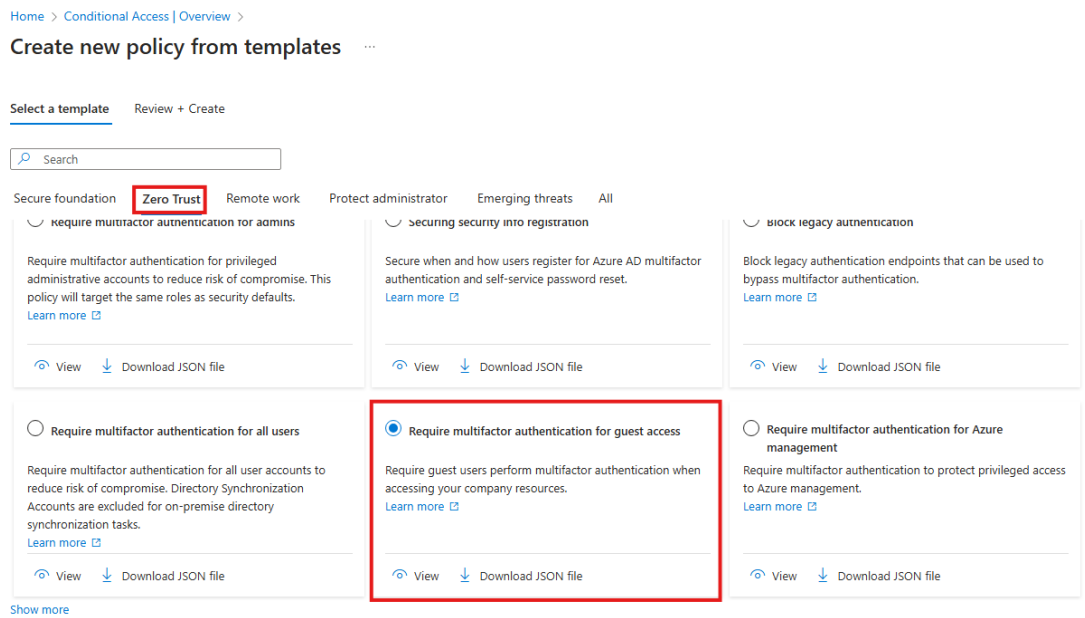
Pro nastavení **MFA** pro **Azure management** stačí jít do **New policy from template** a vybereme **Require multifactor authentication for Azure management**. Poté stačí upravit název a můžete politiky vytvořit.



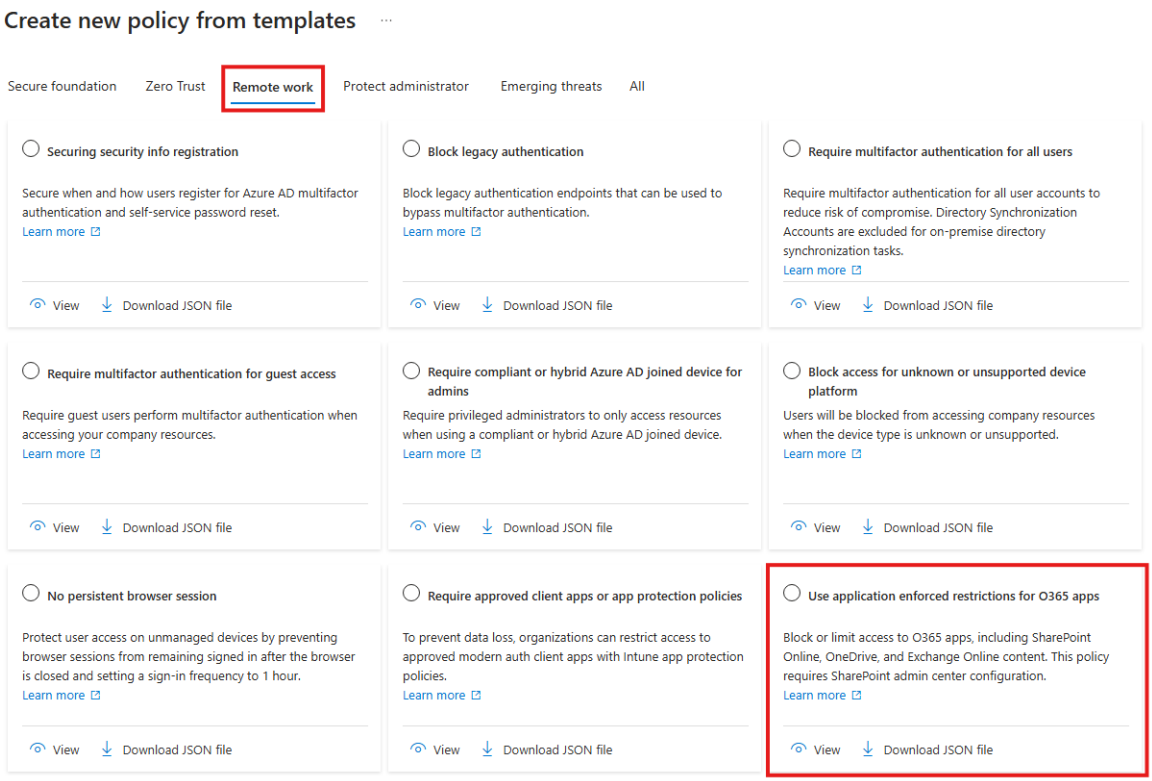
Poté si politiku rozklikneme a odebereme z ní pod kolonkou **Users Exclude** náš účet poslední záchrany. Pak ještě silně doporučuji nastavit maximální dobu přihlášení na 8 hodin.



Jako další si nastavíme vynucení více faktorového ověřování pro externisty. Zase si otevřete **Create new policy from templates** a pod kolonkou **Zero Trust** vyberte **Require multifactor authentication for guest access**. Poté stačí znovu jen vyhodit pomocí **Exclude** účet poslední záchrany a máte hotovo!



A jako posední se podíváme na vynucení používání Microsoft aplikací, jako je Outlook, pro přístup k firemním datům a účtům. Toto nastavení, ač může vypadat jako v celku restriktivní, tak řeší velkou část synchronizačních problémů, protože Microsoft aplikace se se sebou synchronizují lépe než třeba s Apple mail aplikací. Pro vytvoření takovéto politiky nám znovu stačí se podívat do **Create new policy from template** a poté pod kolonkou **Remote work** najdete šablonu s názvem **Use application enforced restrictions for O365 apps**.



Poté vyndejte z politiky účet poslední záchrany a můžete mít hotovo. Pokud, ale nechcete být tak přísní a stačí vám, že na telefonech budou lidi používat Microsoft aplikace a na počítačích ať si dělají co chtějí, nebo naopak (nebo jakkoliv jinak), tak můžete upravit zacílení na specifický druh zařízení. Po rozkliknutí politiky přejděte do sekce **Conditions** a poté do sekce **Device platforms.**

[ICT] GROUP

Home > Conditional Access | Overview > Policies >

008 Use application enforced restrictions for O365 apps

Conditional Access policy

Delete | View policy information | View policy impact (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

008 Use application enforced restrictions fo...

Assignments

Users

All users included and specific users excluded

Target resources

1 resource included

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

Device platforms

Any device and 2 excluded

Locations

Not configured

Client apps

Not configured

Filter for devices

Not configured

Authentication flows

Not configured

Zde si vyberte **Any device** a poté přejděte do kolonky **exclude**.

Device platforms

Apply policy to selected device platforms.
Learn more

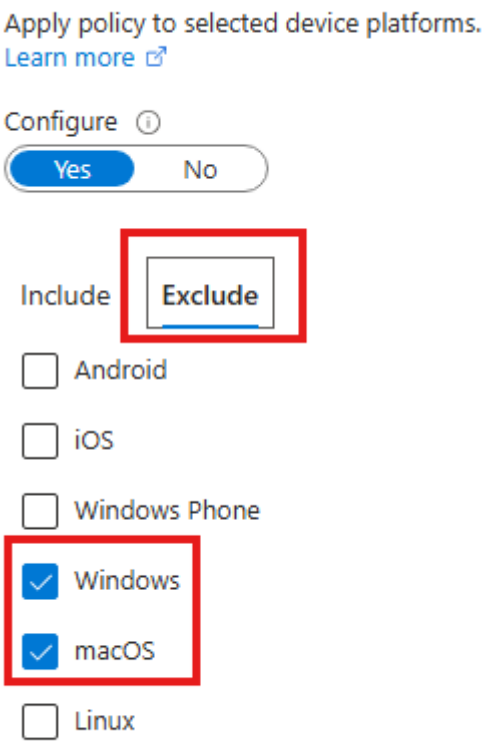
Configure

Yes | No

Include | Exclude

- Any device
- Select device platforms
  - Android
  - iOS
  - Windows Phone
  - Windows
  - macOS
  - Linux

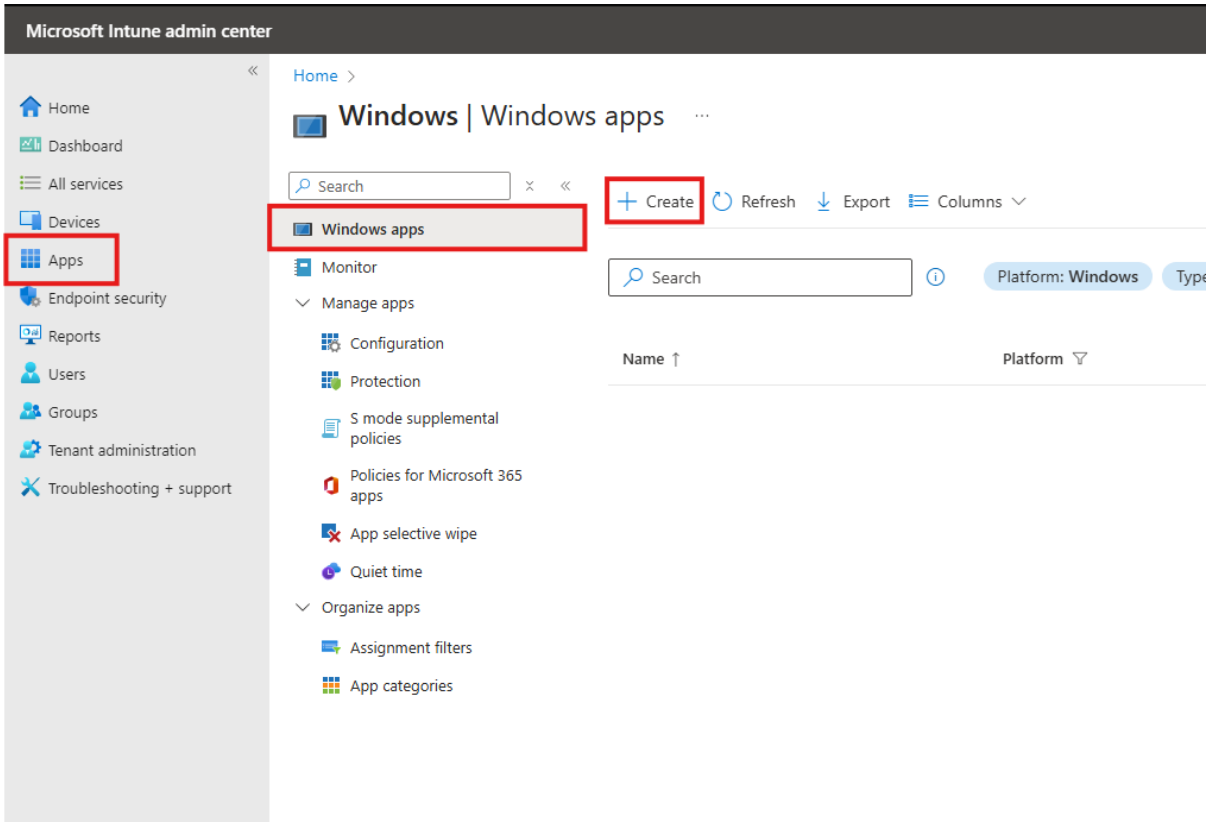
V této kolonce si vyberte, na jaká zařízení nechcete cílit a máte hotovo!



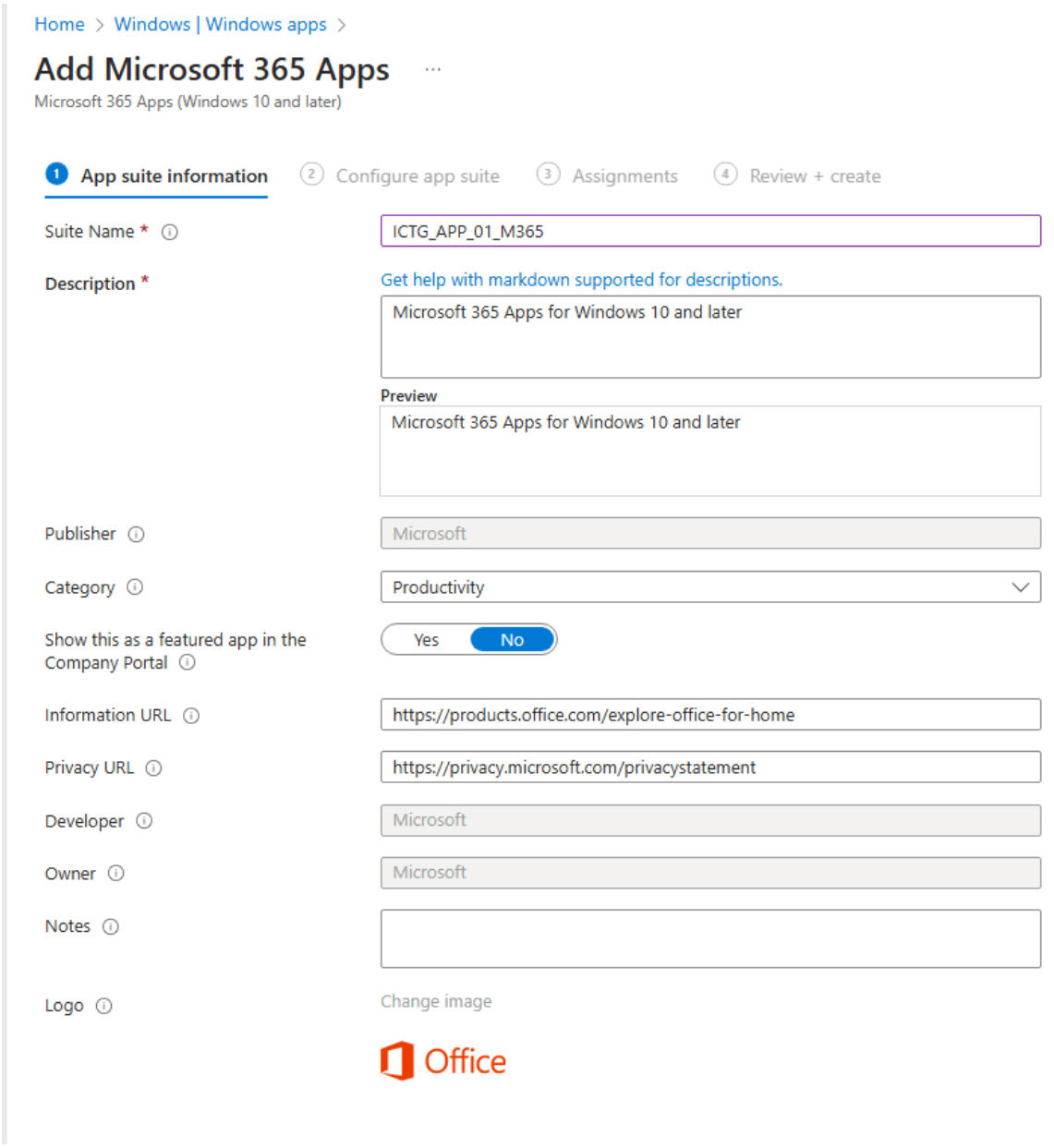
Na závěr k **CAP**. Rozhodně si vytvořte účet posední záchrany, bude se vám hodit! A buďte při nastavování pozorní, protože odříznout se je jednoduché. Také velmi důležitá věc, opravdu si nechte všechny politiky v módu **Report Only** (pokud už ve vašem tenantu fungujete) a až po odlazení je zapínejte. Ze zkušenosti je totiž dost velká šance, že něco rozbijete.

Intune

Po dlouhých útrapách s **Conditional Access Policies** se přesuneme do portálu **Intune**, který ne jenom, že je ještě komplexnější, ale také nás dostává do administrace zařízení. Doposud jsme administraci zařízení nakousli jen opravdu maličko, protože je to, z mého pohledu nejsložitější část hned po forensním zkoumání incidentů, které občas nastanou. Abych vás ale neodradil hned ze začátku, tak je to taky jeden z portálů, který řeší věci, které „opravdu pocítíte“ (a to tedy, jak v dobrém, tak i v ne tak dobrém).
Z portálu **Intune** jdou kontrolovat věci, které si týkají například: automatické synchronizace **OneDrive** a jeho automatické přihlášení, možnost přidávat aplikace do **Company Portal,** ze kterého můžou uživatelé stahovat bez nutnosti administrátorských oprávnění, zabezpečení dat v aplikacích a mnoho mnoho dalších. V dnešním článku projdeme úplný základ a přidáme si povinné aplikace **M365.**

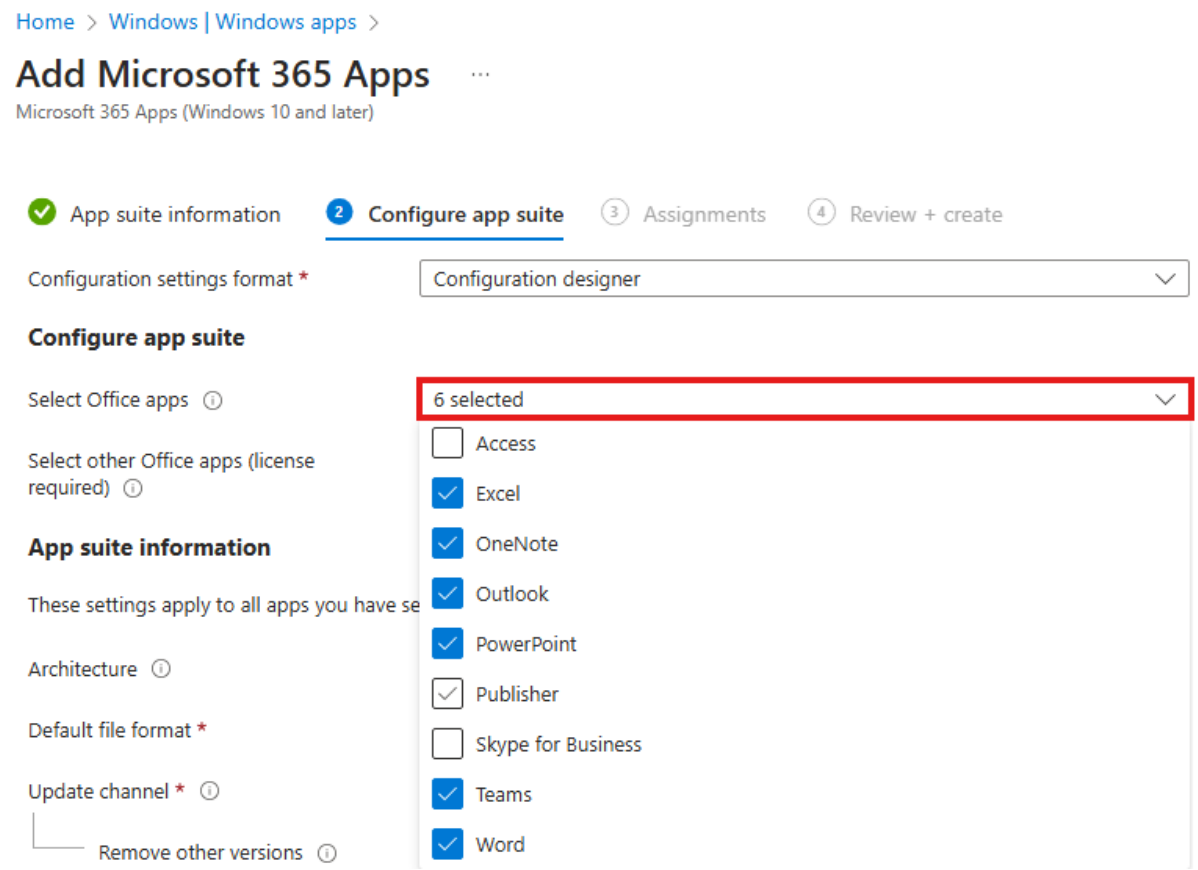


Pro vynucení instalace všech **M365** aplikací do počítače se přihlaste do **Intune** admin portálu (https://intune.microsoft.com) a otevřete si záložku **Apps > Windows** a poté **Create**

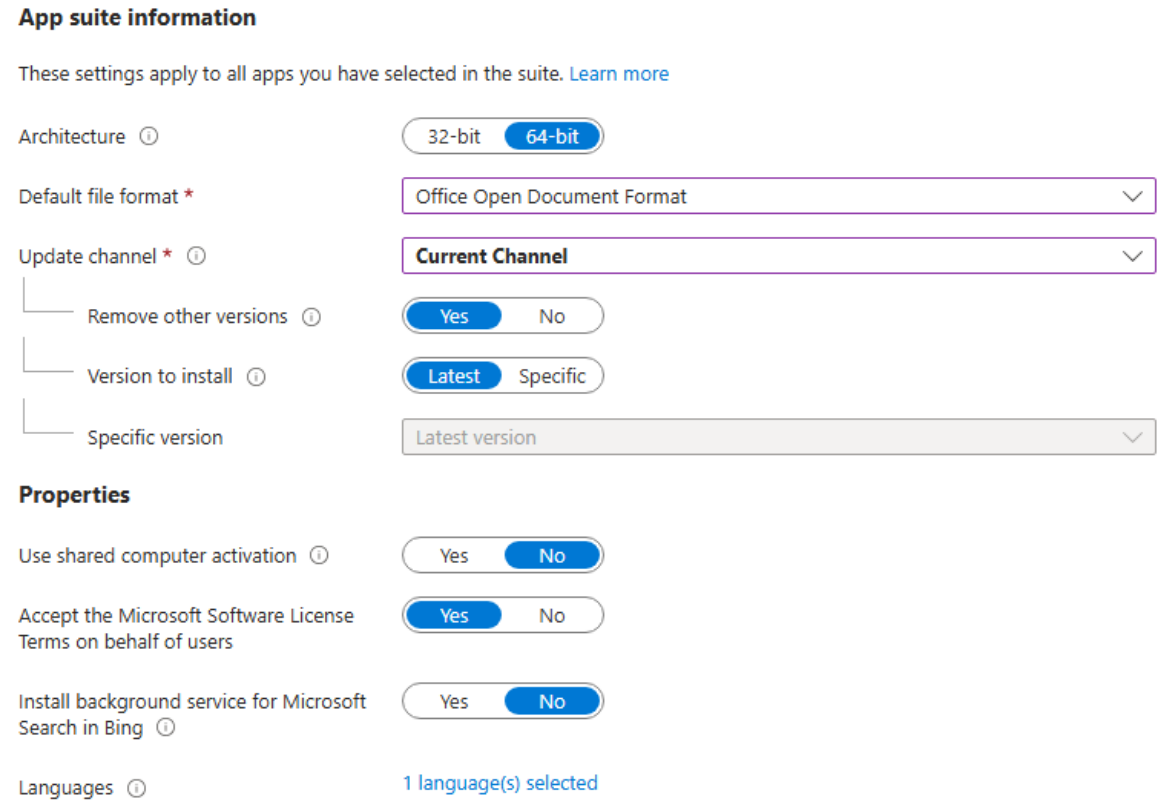


Poté vyberete **Microsoft 365 Apps Windows 10 and later.**

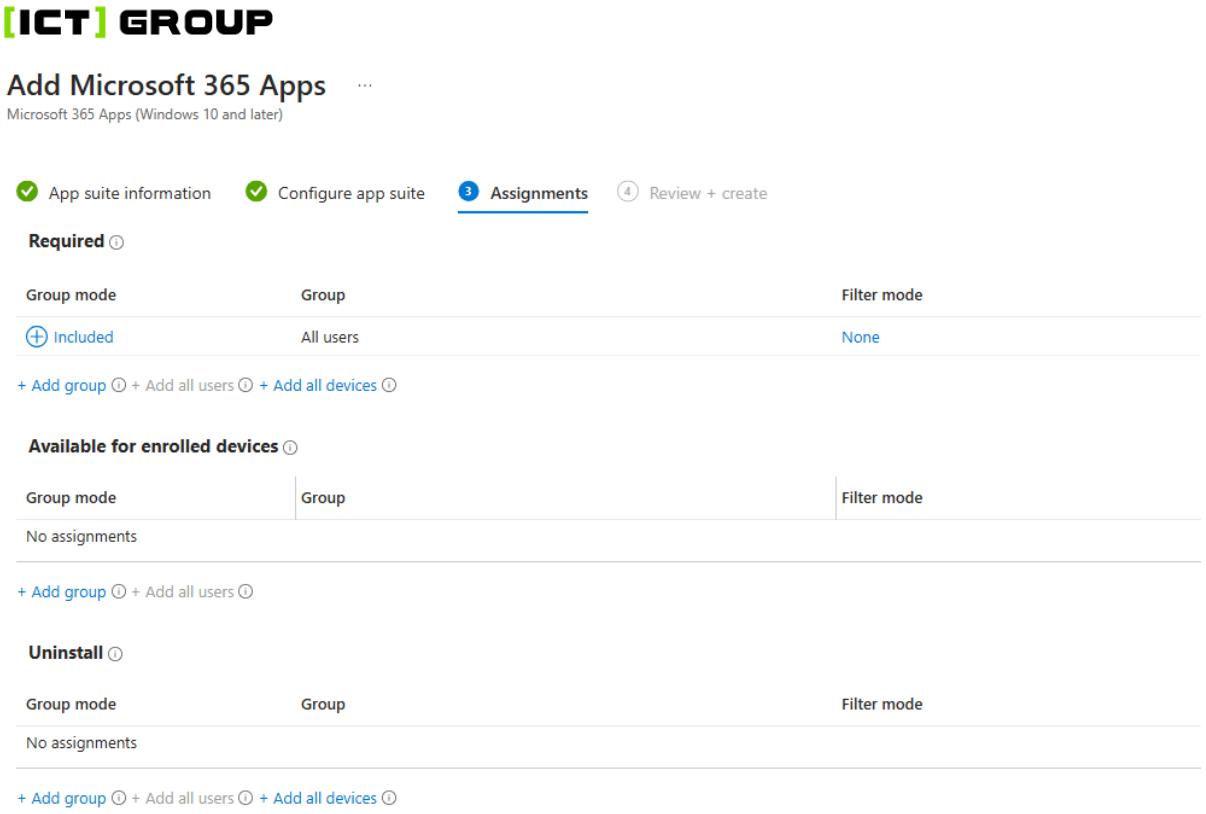
Politiku pojmenujte. **Show this as a featured app in the Company Portal** můžete nechat vypnutý, protože stejně budeme aplikace vynucovat.



Pokud máte konfigurační XML soubor, tak můžete vybrat místo **Configuration designer Enter XML data**. Pro nás méně odvážné je tu konfigurátor přímo v **Intune**. V sekci **Select Office apps** si můžete vybrat, které aplikace se nainstalují. Pokud chcete i nad rámcové aplikace (**Viso Online Plan 2** nebo **Project Online Desktop Client**), tak si je můžete vybrat o jedno pole níže.



Poté si vyberte formát, ve kterém budou ze základu data z **O365** aplikací. Jako **file type** vyberte **Office Open Dokument Format,** jinak vám politika nepůjde vytvořit (s těmito nastaveními). **Update channel** nastavuji vlastně vždy na **Current Channel**, protože chci mít všechno co nedříve aktualizované. Zbytek nastavení se v celku sám popisuje názvem. Jen dole nezapomeňte vybrat jazyk (pokud tedy chcete, aby všichni měli **O365** aplikace ve stejném jazyce).



Politiku zacílíme na všechny uživatele a máme hotovo.

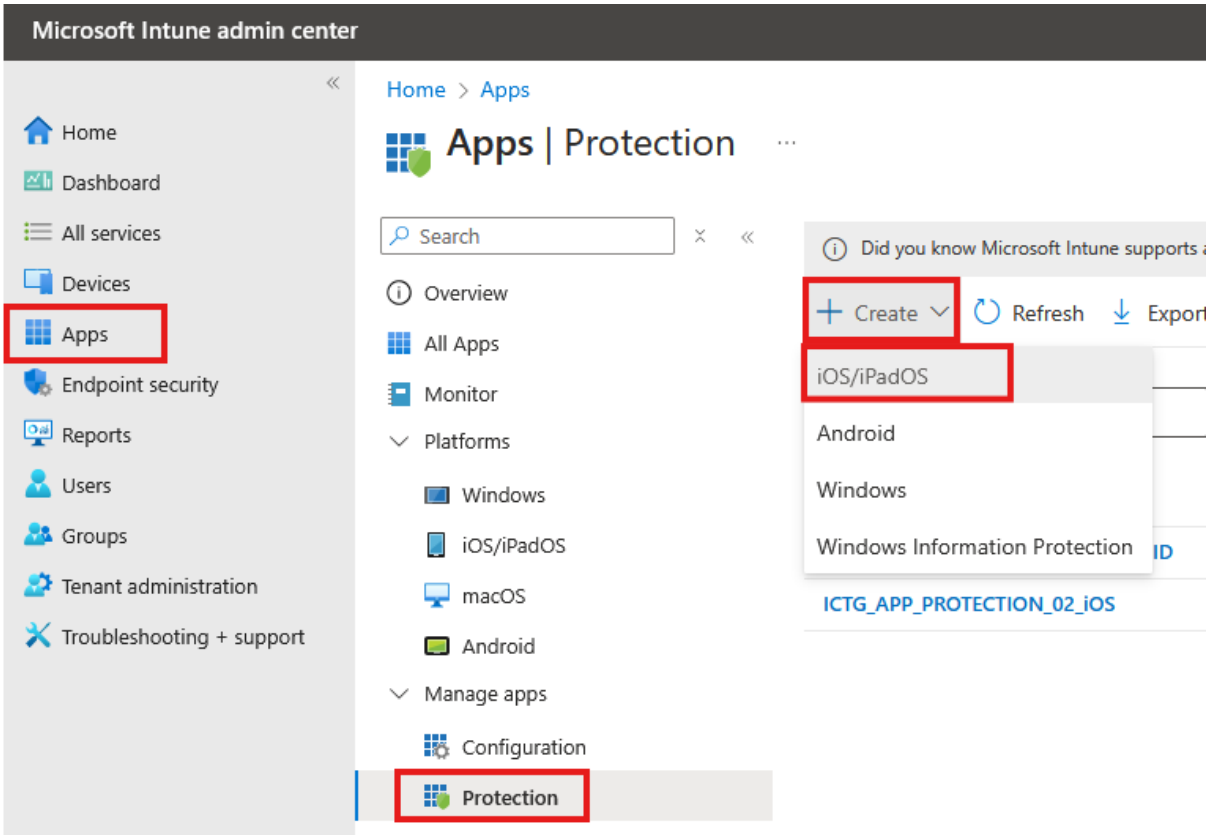
[ICT] GROUP

Ochrana aplikací (na mobilech)

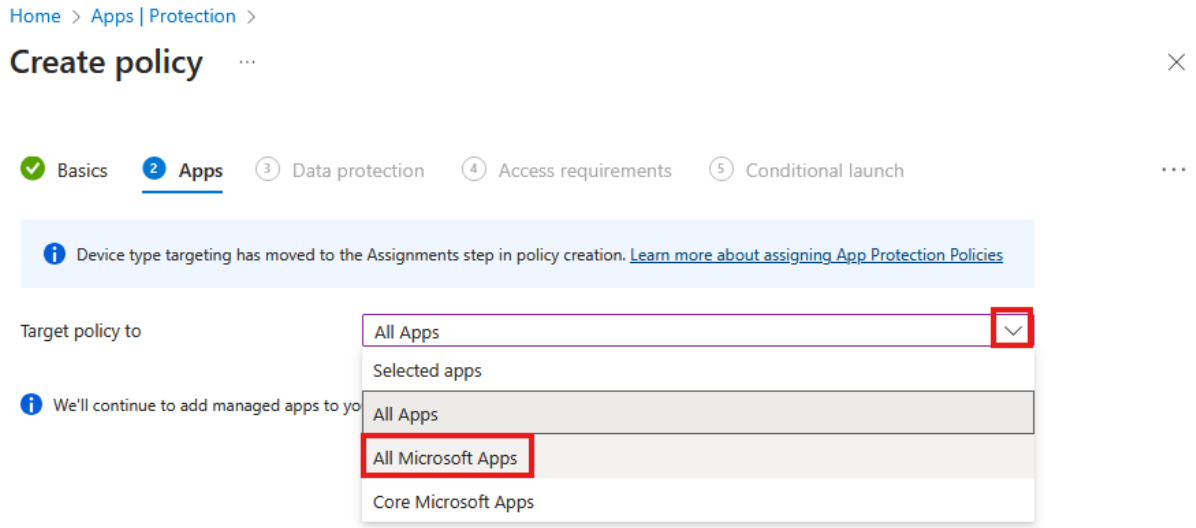
V minulé epizodě jsem vás provedl nastavením automatické instalace O365 aplikací na Windows. Dnes se podíváme na ochranu mobilních O365 aplikací a dat v nich. První věc, která vás asi napadne je, proč to řešit na telefonech? A další otázka asi bude, budeme to řešit na počítačích? Na první otázku je jednoduchá odpověď a to, že skoro každý má mobilní telefon, a ne každá firma dává firemní telefony. S tím přichází problém osobních zařízení, protože nemůžete zařízení ovládat kompletně, ale pořád potřebujete zabezpečit firemní data a účty. V tuto chvíli je více možností, jak vyřešit tento problém, mohli bychom: vytvořit **enrollment** profil, který vytvoří separátní „pracovní profil“ na zařízení a nenechá vás kopírovat data z pracovního do osobního. To je velmi dobré řešení, ale funguje pouze pro Android. Proto vytvoříme tzv. **App Protection Policy**, které nám dovolí granulárně ovládat co kdo může a nemůže v O365 aplikacích.

Pro vytvoření si otevřete **Intune** > **Apps** > **Protection.**

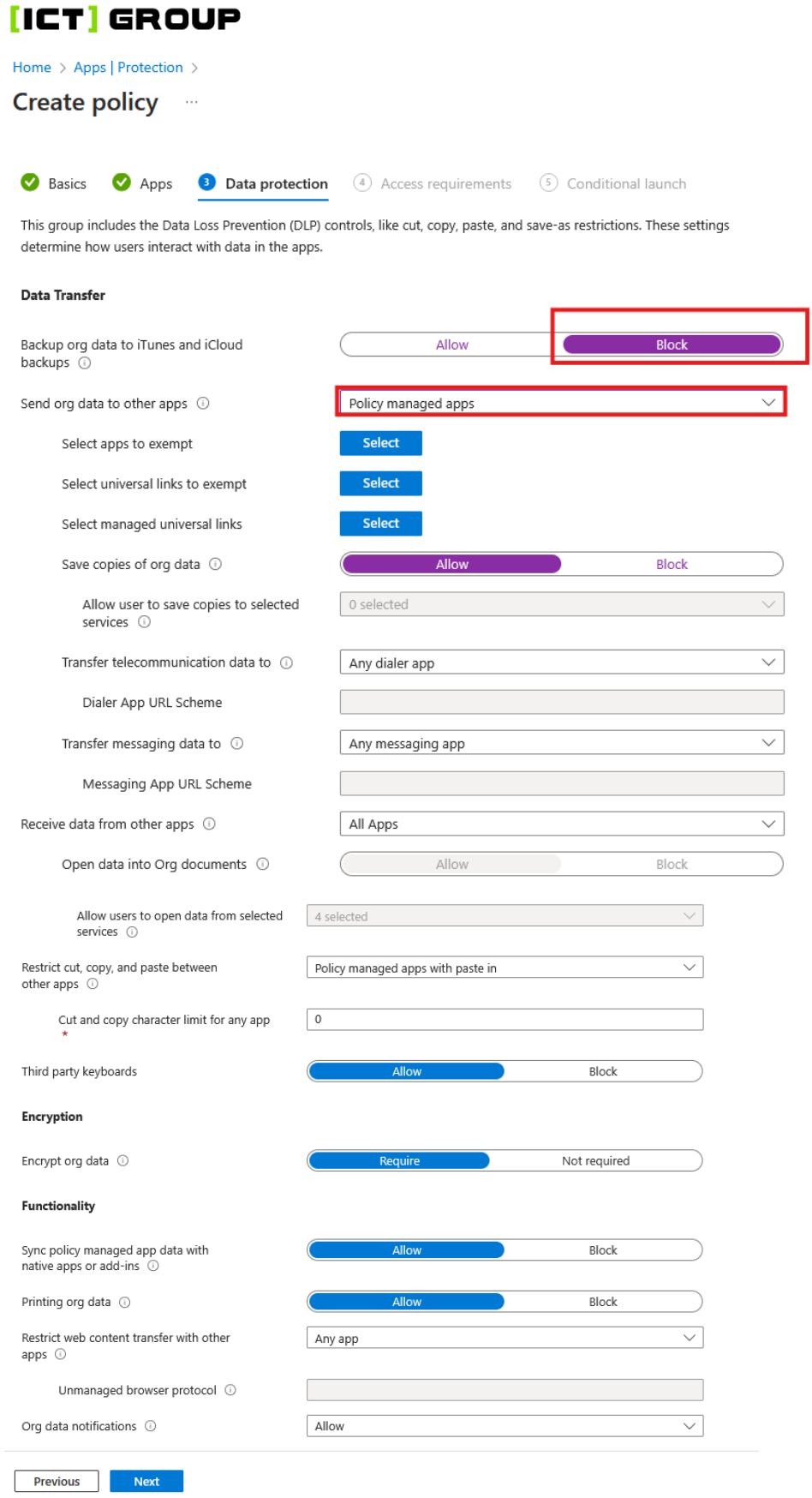
https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsMenu/~/protection



Poté klikněte na **Create** a **iOS/iPadOS.**



Pojmenujte svoji politiku, klikněte **Next** a vyberte **All Microsoft Apps.**



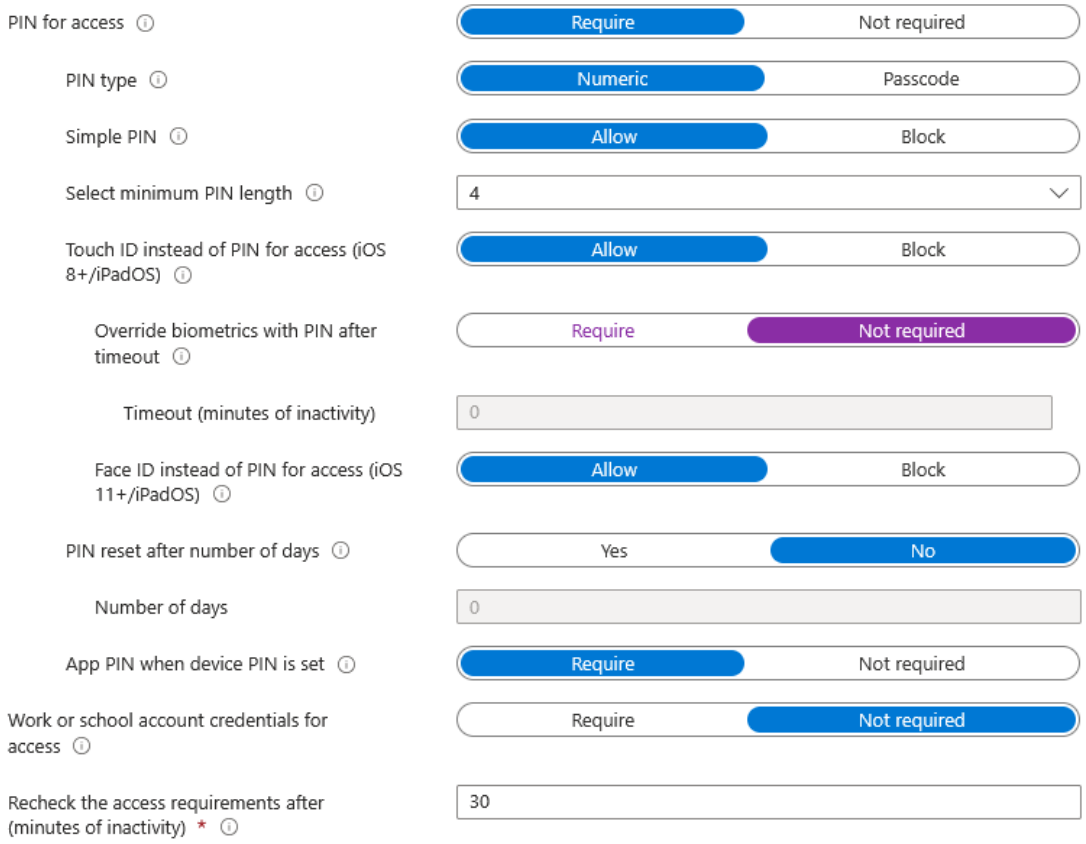
Tyto nastavení jsou volnější, ale pokud je plánujete nasazovat, tak doporučuji začít zvolna.

[ICT] GROUP

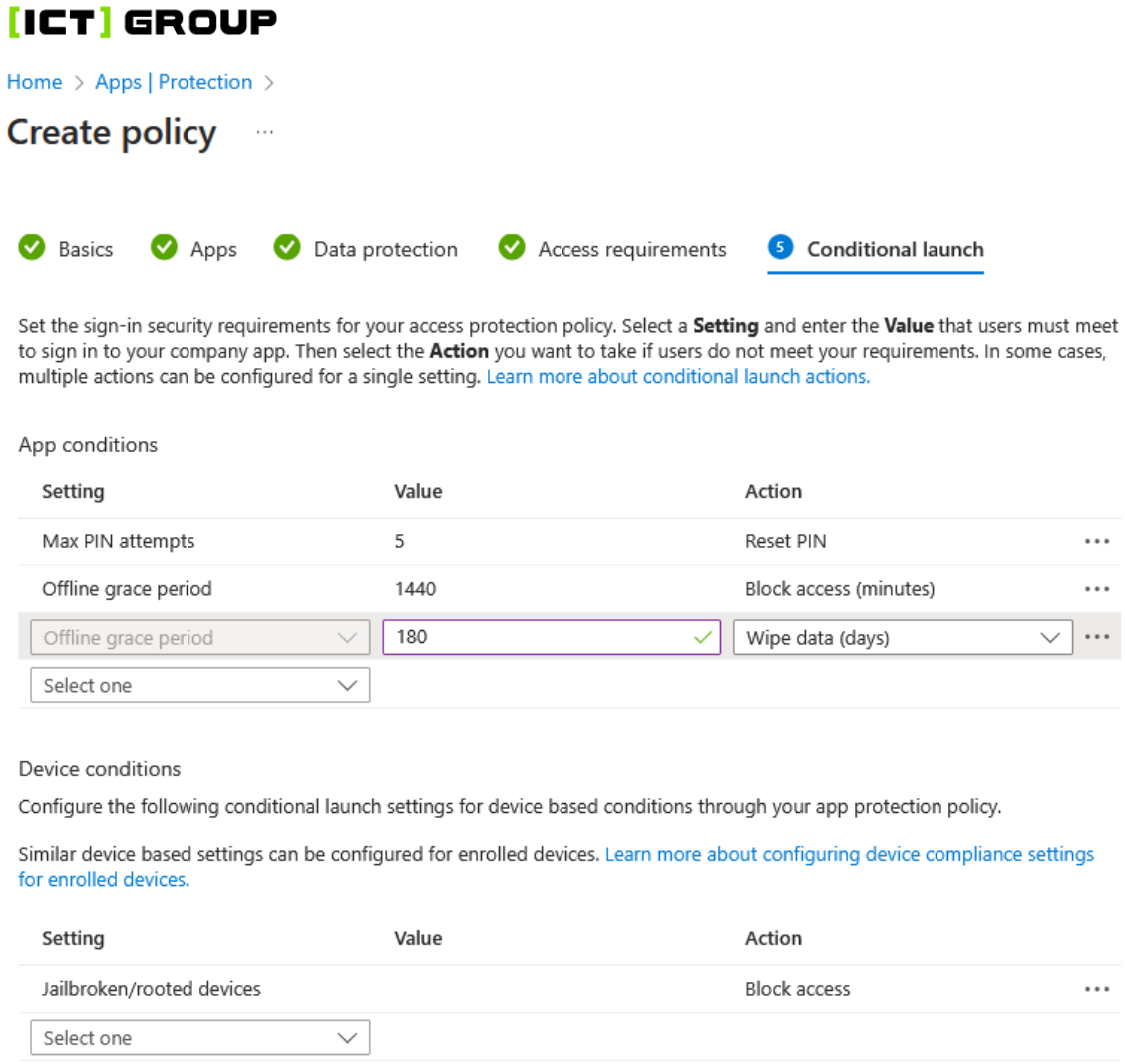
Create policy ...

Basics | Apps | Data protection | 4 Access requirements | 5 Conditional launch

Configure the PIN and credential requirements that users must meet to access apps in a work context.



Tímto nastavíte zabezpečení aplikací pinem. Samozřejmě povolujeme použití biometriky a nezapínáme expiraci pinu.



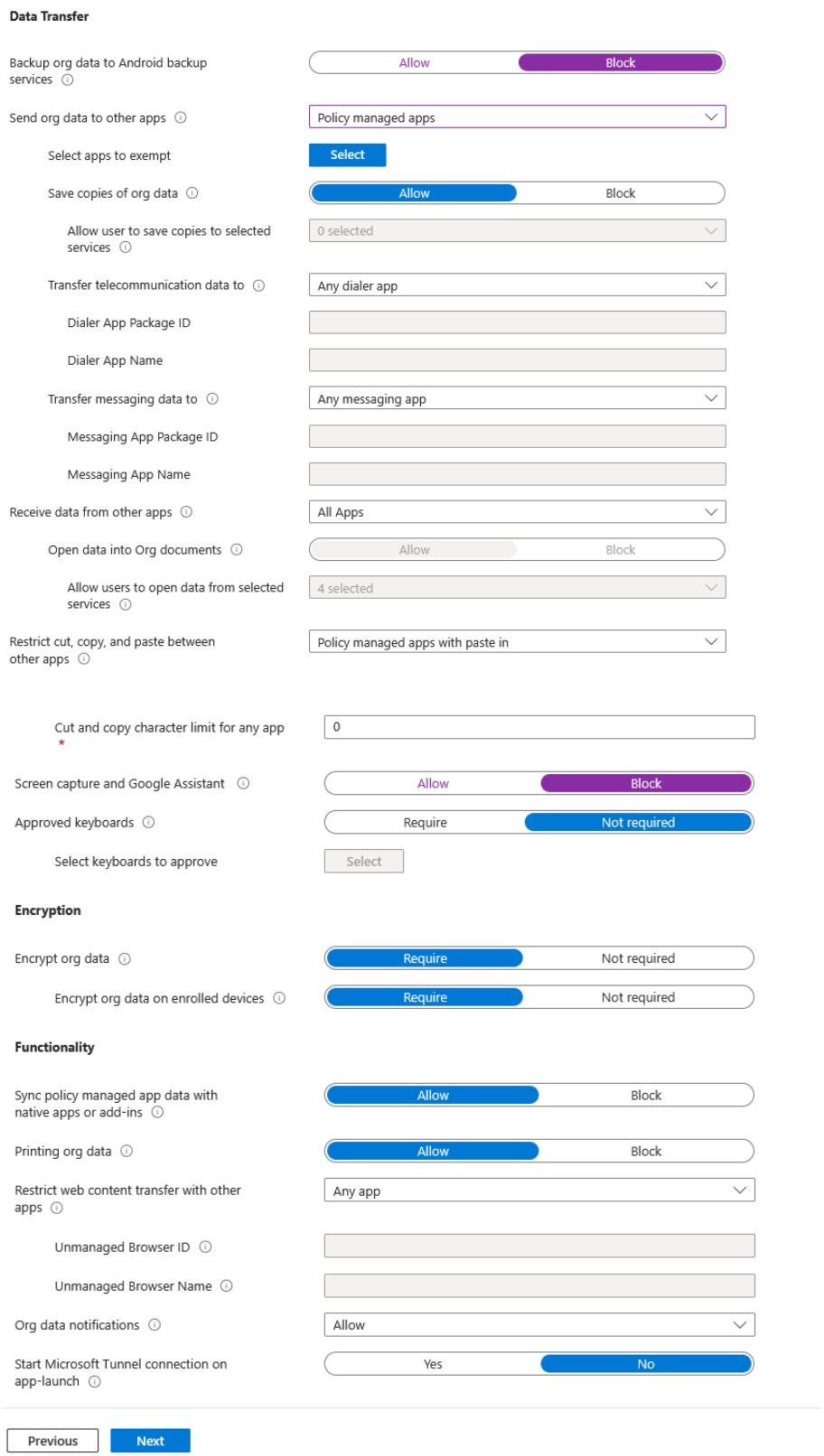
Jediné, na co si musíte dát pozor zde je **wipe data.** Já osobně nastavuji 180 dní pro jistotu.

Poté stačí zacílit na skupinu uživatelů, ano musí to být uživatelé, ale nemusí vás zajímat, jestli mají nebo nemají iOS, a máte hotovo.

Politika pro Android se nastavuje podobně, ale není to úplně stejné.

Znovu pojmenujeme politiku a vybereme **All Microsoft Apps**.

[ICT] GROUP

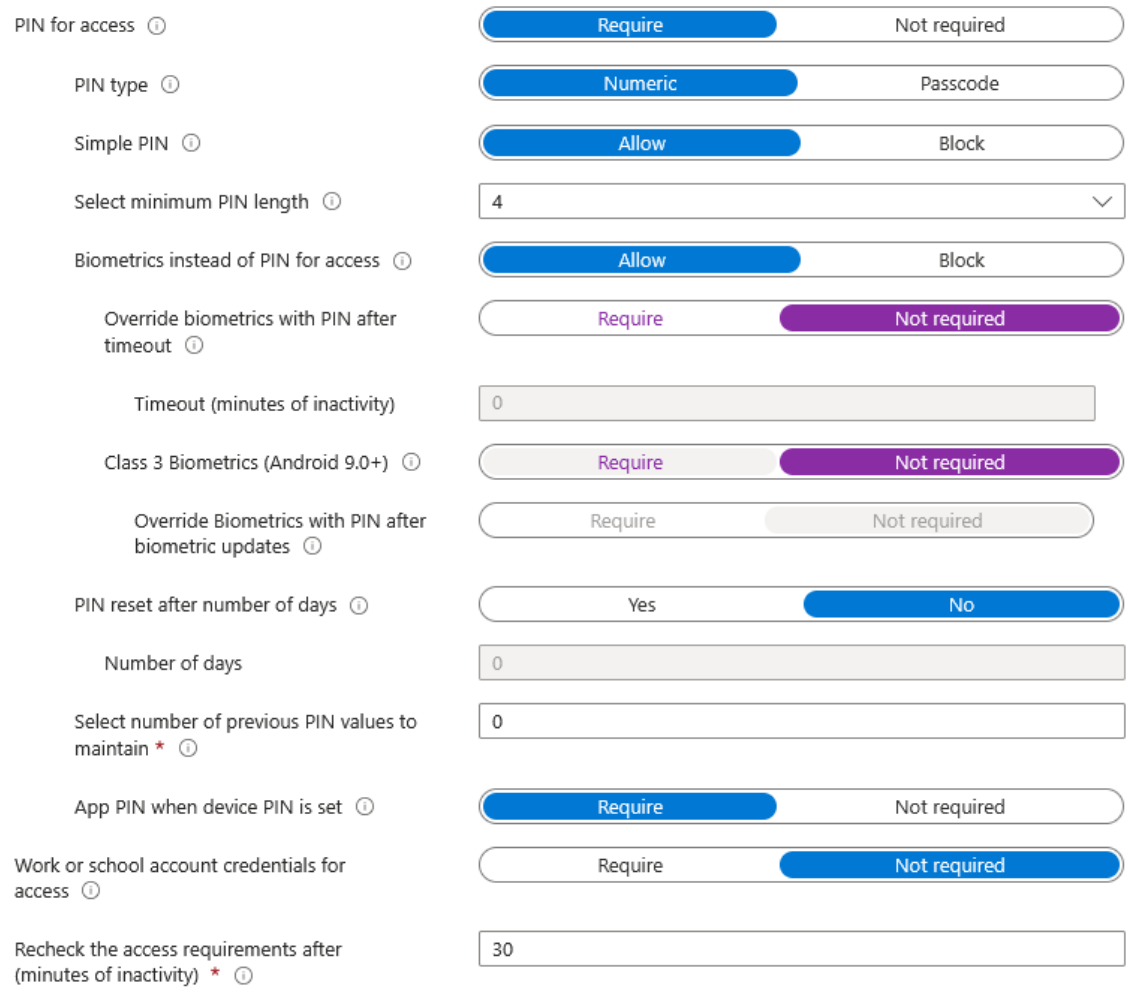


Toto nastavení povoluje ukládat firemní data na zařízení, ale nedovoluje pořizování snímků a nahrávek obrazovky. Také šifruje všechna firemní data a zakazuje automatickou zálohu na zařízení/cloud uživatele. Znovu jsou nastavení v celku volná a vždy se dá utáhnout, pokud bude v budoucnu potřeba.

[ICT] GROUP

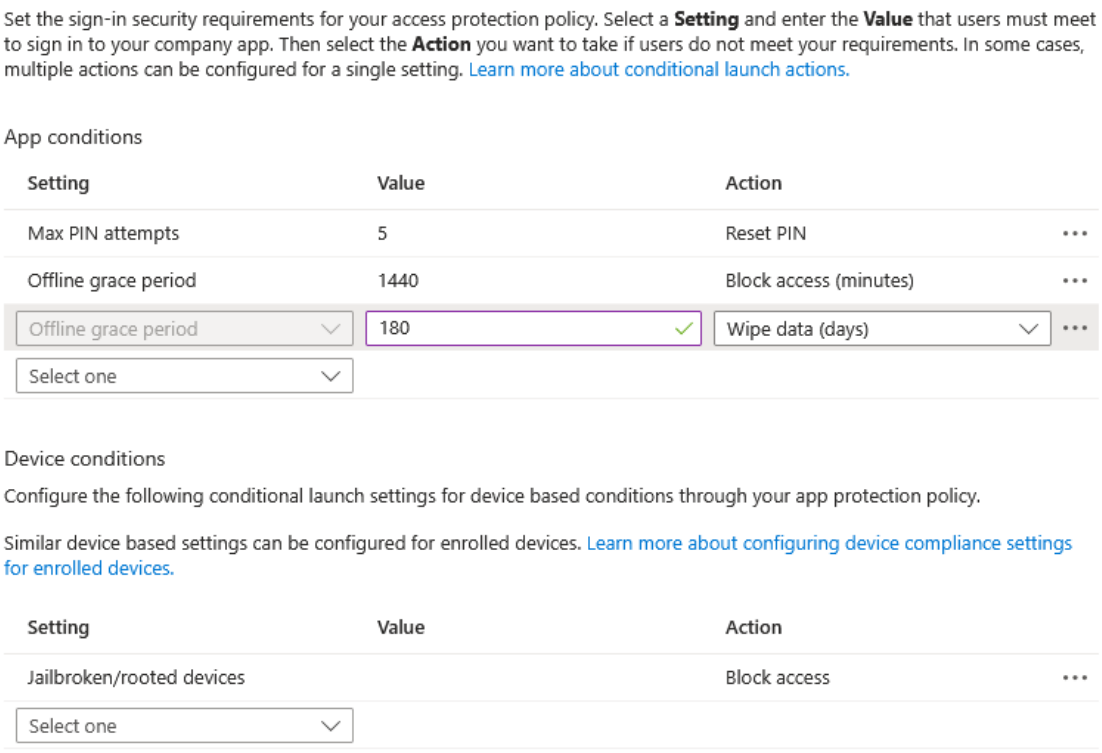
Create policy ···

Configure the PIN and credential requirements that users must meet to access apps in a work context.



Nastavení pinu nechávám velmi podobné jako u iOS.

[ICT] GROUP



Toto nastavení je úplně stejné jako iOS.

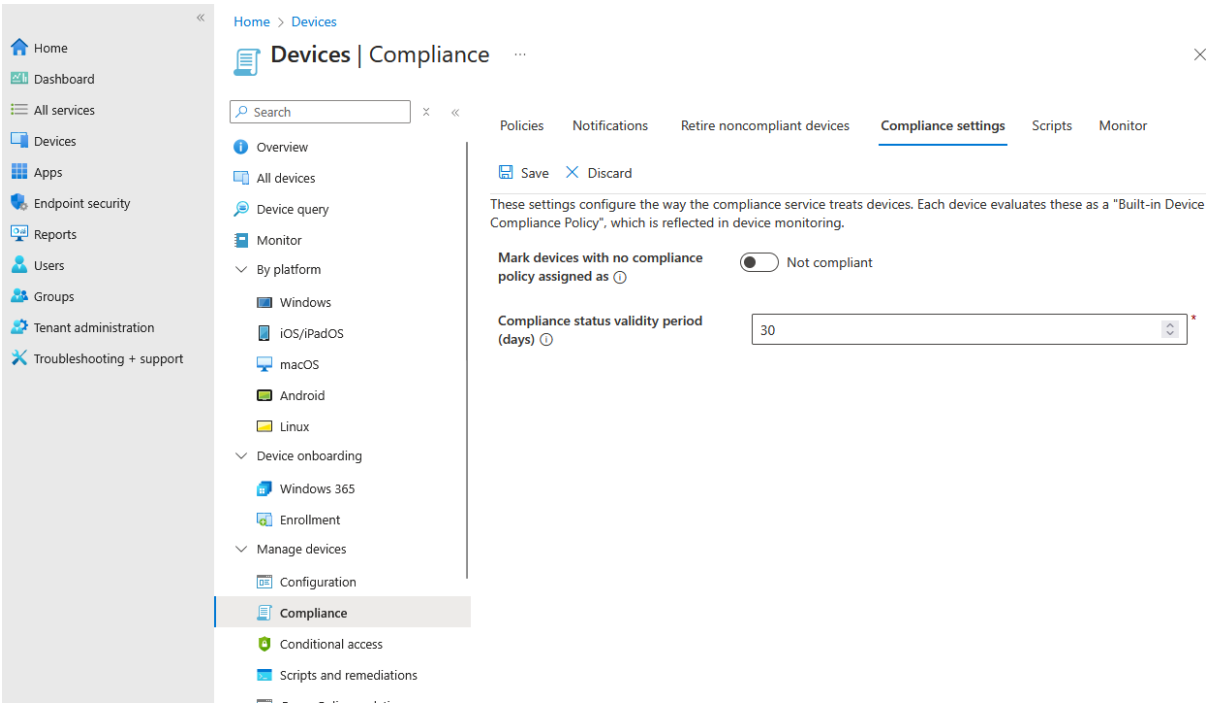
Poté stačí zacílit na uživatele a máte hotovo!

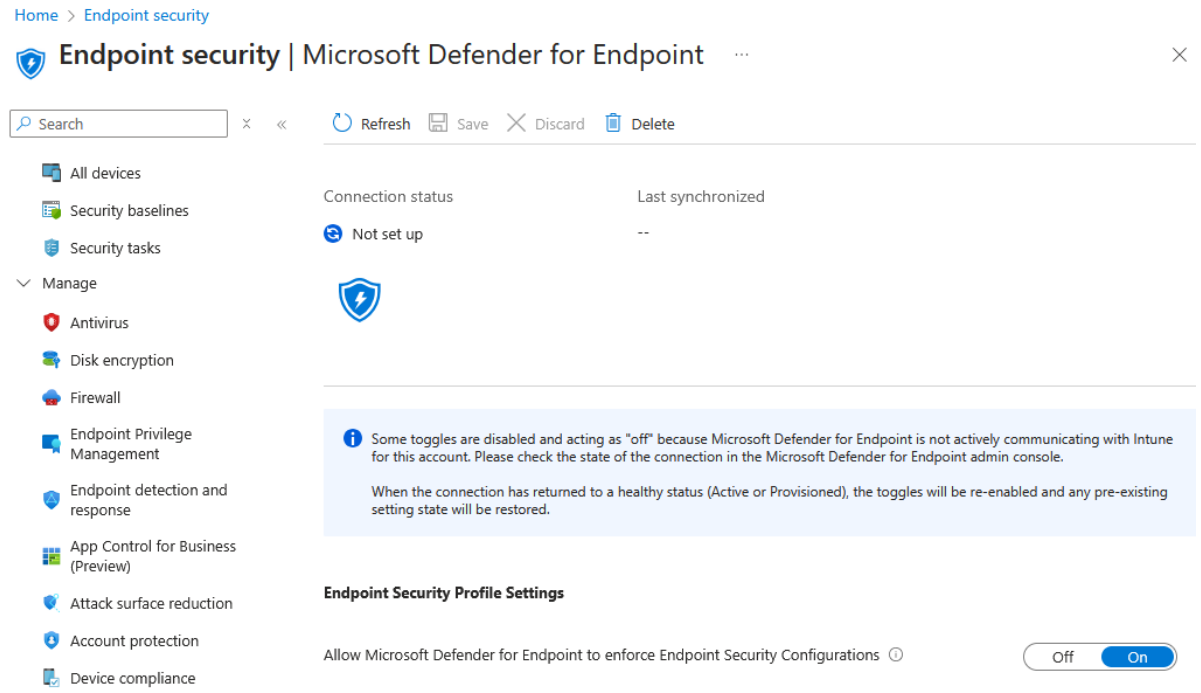
[ICT] GROUP

Příprava pro řízení zařízení

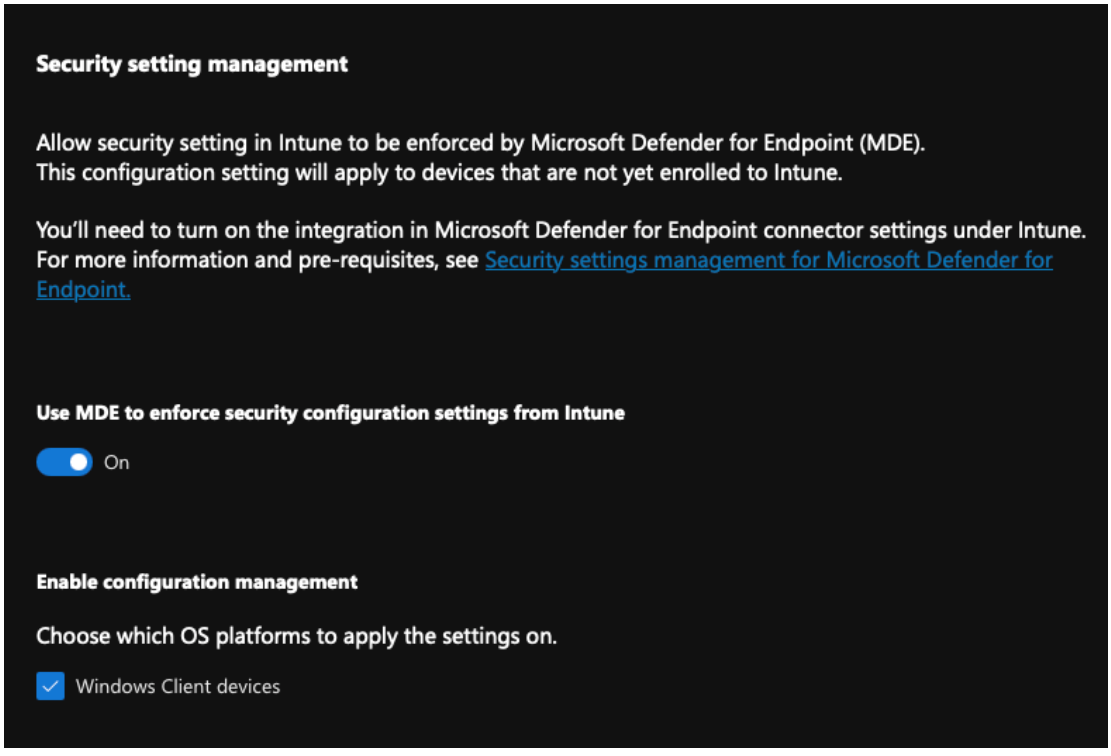
V dnešní kratší epizodě si připravíme nutné věci, na kterých budeme stavět v pozdějších článcích. Jsou to věci, které jsou nutné, většinou zaberou nějaký čas, než se projeví, ale nejsou dostatečně „zajímavé“ na samostatné epizody. První věc, kterou si nastavíme, je základní stav zařízení. Microsoft má nastavené, že ze základu (pokud na zařízení není udělená žádná tzv. **compliance** politika) je zařízení **compliant**. To ale nechceme, takže si to přepneme na přesný opak. Přihlaste se do administrátorského portálu **Intune**, klikněte na **Devices**, **Compliance**, **Compliance settings** a přepněte šoupátko z **compliant** na **not compliant.**

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/compliance





Jako další a poslední věc, kterou si dnes nastavíme, je konektor mezi **Defender for Endpoint (DfE)** a **Intune.** Pro to stačí jít do **Intune, Endpoint security** a poté do **Microsoft Defender for Endpoint** a přepnout šoupátko z Off na On.



Poté stačí přejít do **Security** centra (security.microsoft.com) a jít do **Settings, endpoints** a zde zapnout **Use MDE to enforce security configuration settings for Intune**. Tím máte konektor zapnutý. Jenom malá rada, pokud v **security** centru tuto možnost nevidíte, tak je čas si zajít na kafe, ona se objeví, jen to občas trvá 😉.

[ICT] GROUP

První pohled na správu zařízení

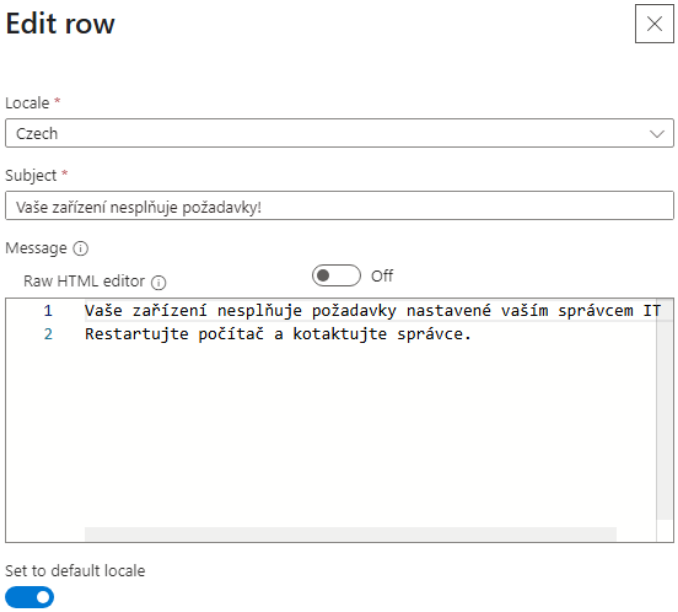
Téma správy zařízení je jedna z komplikovanějších částí M365. Většinu politik, které nastavíte, můžete cílit, jak na uživatele, tak na zařízení (ne zároveň) a to zajistí velmi nepatrně jiný průběh nasazení. A to zmiňuji jen malinkou část komplexního světa **Intune**. Politiky, které vám v průběhu tohoto a příštích několika článků budu představovat, budou relativně málo restriktivní (jinak by nás zákazníci zakopali), ale přesto by vám měly usnadnit život a posunout vaši kybernetickou bezpečnost zase o krok dál. Pokud máte jakékoliv nastavení, které se vám osvědčilo, nebo si s ním naopak nevíte rady, tak se o něj podělte (jestli teda není tajné), ať jsme společně o něco chytřejší 😉 .

Jako první se vrhneme na **compliance,** v minulé epizodě jsme si nastavili, že zařízení, která nemají nastavenou **compliance** politiku nastavíme jako **noncompliant.** To by teď ale znamenalo, že všechna naše zařízení budou svítit červeně.

Pro nastavení **compliance** politiky musíme nejdřív nastavit notifikaci, která přijde, když je zařízení vyhodnocené jako **noncompliant.** Pro to si otevřete **Intune > Devices > Compliance > Notifications** a klikněte na **Create notification.**

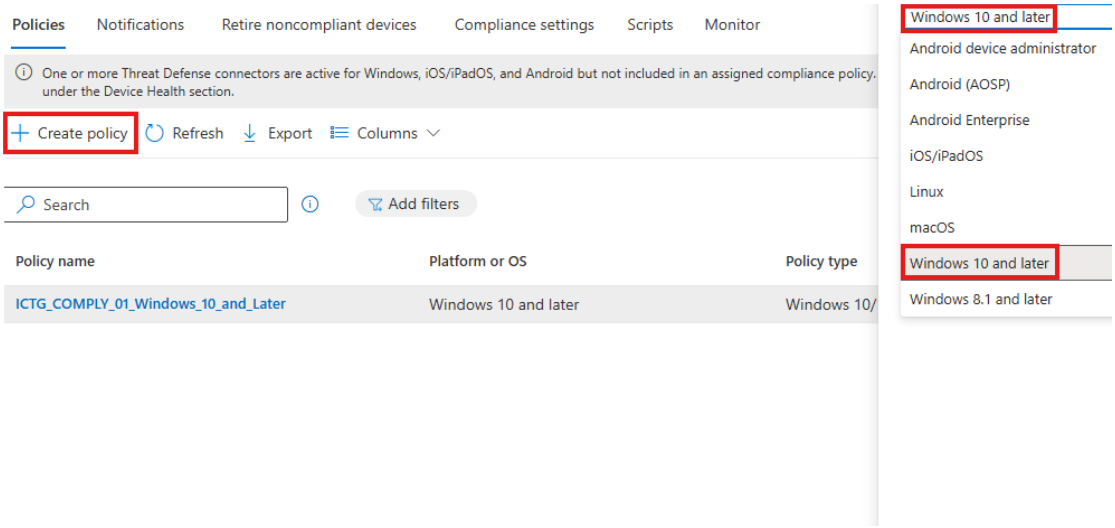
https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/compliance

Notifikaci pojmenujte. Pokud máte, tak přidejte logo firmy a kontakt. Poté vytvořte zprávu, která přijde příjemci a máte hotovo!

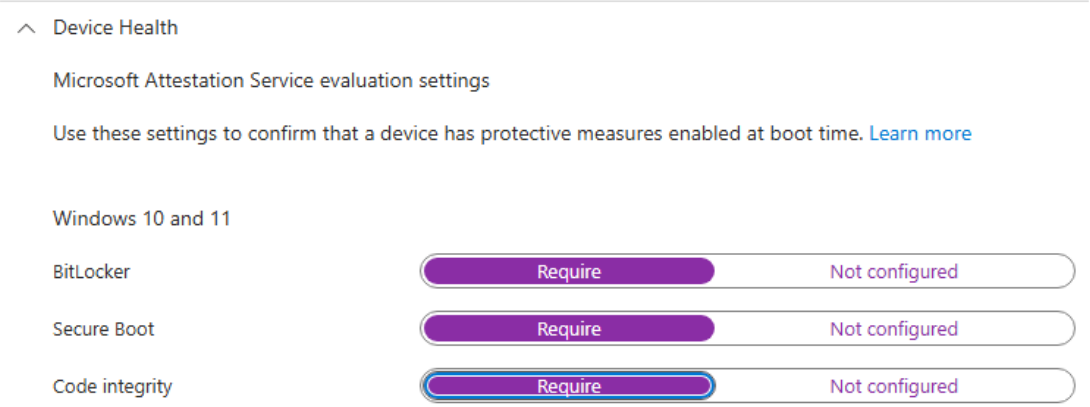


[ICT] GROUP

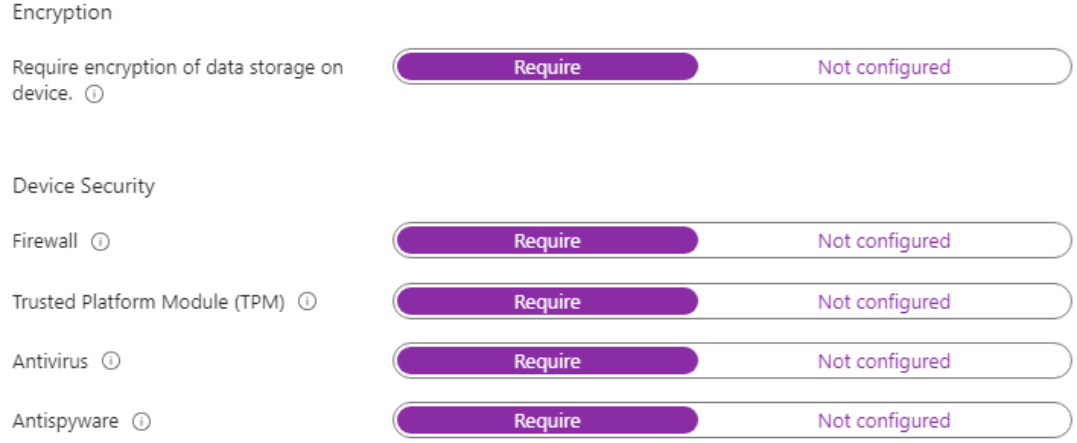
Teď už si můžeme bez problému vytvořit **compliance**, vytvoříme si ji pro **Windows 10 and later.**



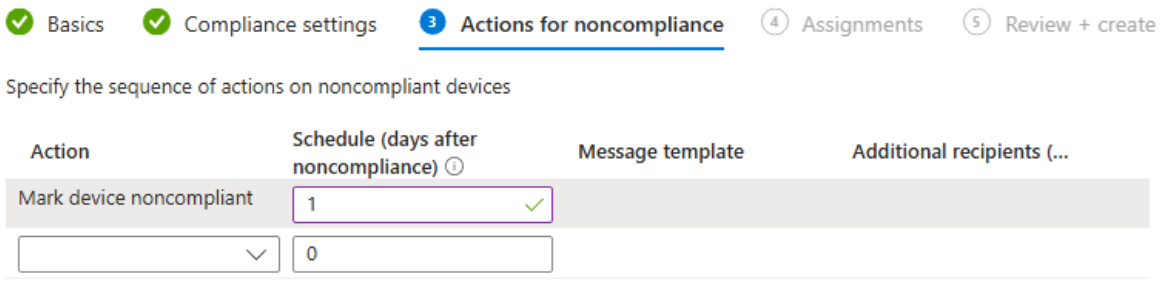
Pojmenujeme a pustíme se do nastavování. Pod záložkou **Device Health** zapneme všechno.



A pod záložkou **System Security** zaškrtáme **Encryption, Firewall, TPM, Antivirus** a **Antispyware.**



Pak nastavíme dobu, za kterou se zařízení stane **noncompliant,** když nebude v souladu s těmito nastaveními, já osobně dávám jeden den.



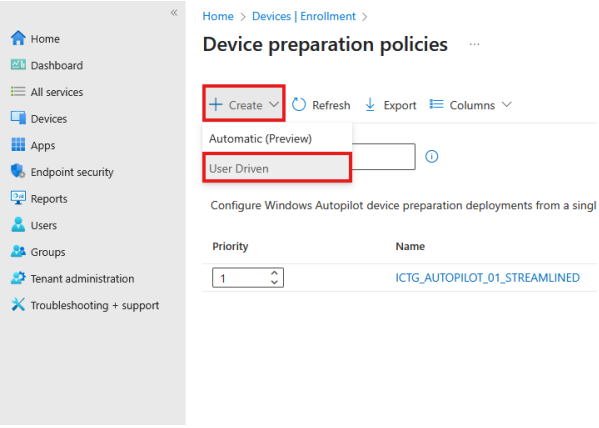
Jako poslední nastavení musíme zacílit na zřízení nebo uživatele, pokud máte **security** skupinu, která v sobě má jen **Windows** zařízení, tak ji použijte, pokud ne, tak **All users,** většinou funguje bez problémů. A to je vše. Máte nastavenou první politiku, která říká, že zařízení (pro to, aby bylo **compliant**) musí mít zapnutý **BitLocker, Firewall, Antimalware, Antispyware** a musí fyzicky mít **TPM** čip.

Autopilot!!!

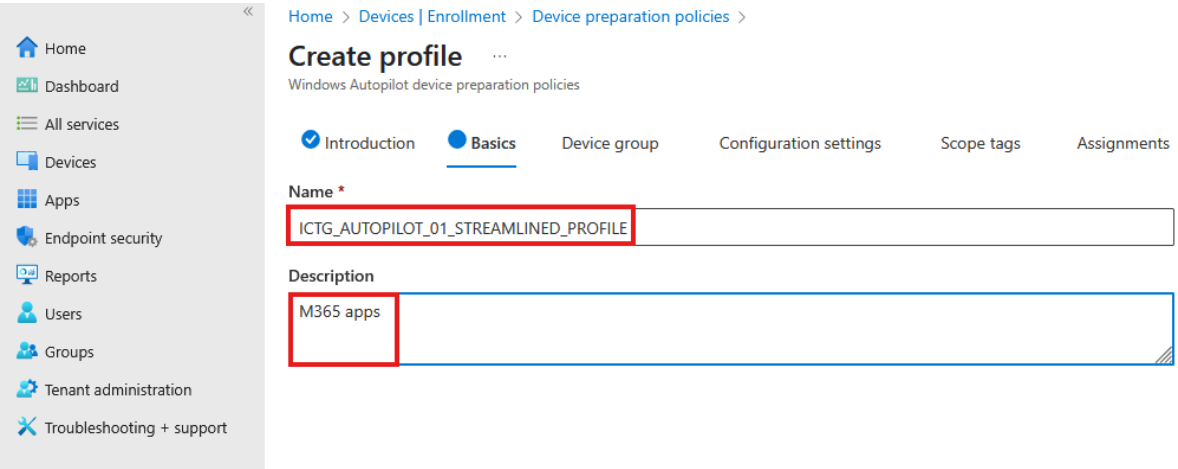
Pomalu, ale jistě se v tomto zpravodaji posouváme bažinou **Microsoft** vymožeností, na které velmi rád nadávám a občas i oprávněně, ale tahle věc se musí **Microsoftu** nechat: **Autopilot** je velmi dobře vymyšlená (o trochu hůř zpracovaná) úžasná vymoženost, která nám ajťákům ušetří spousty hodin ročně. Nastavení ale není úplně jednoduché a dá se nastavit dvěma způsoby. V této kuchařce se podíváme na ten modernější způsob nastavení **autopilota**, který i když lehce ořezává všechny možnosti, tak je na jednom místě a je násobně jednodušší.

Pro nastavení této politiky si otevřeme **Intune** > **Devices > Enrollment > Device preparation policies** dáme **Create** a **User Driven.**

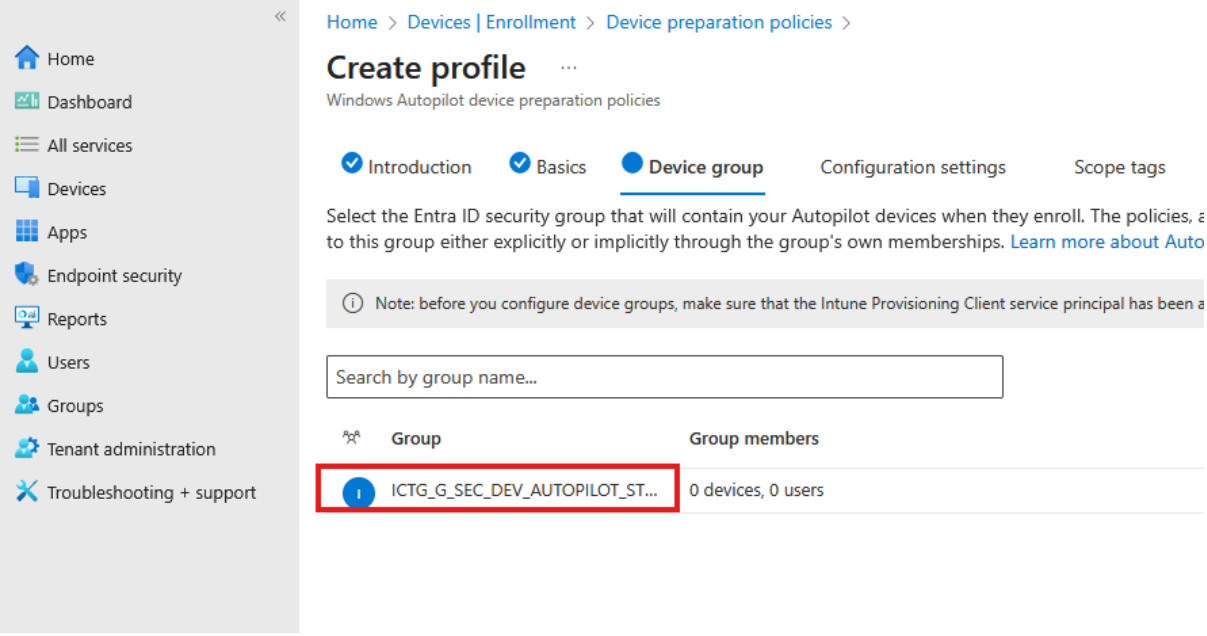
https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/enrollment



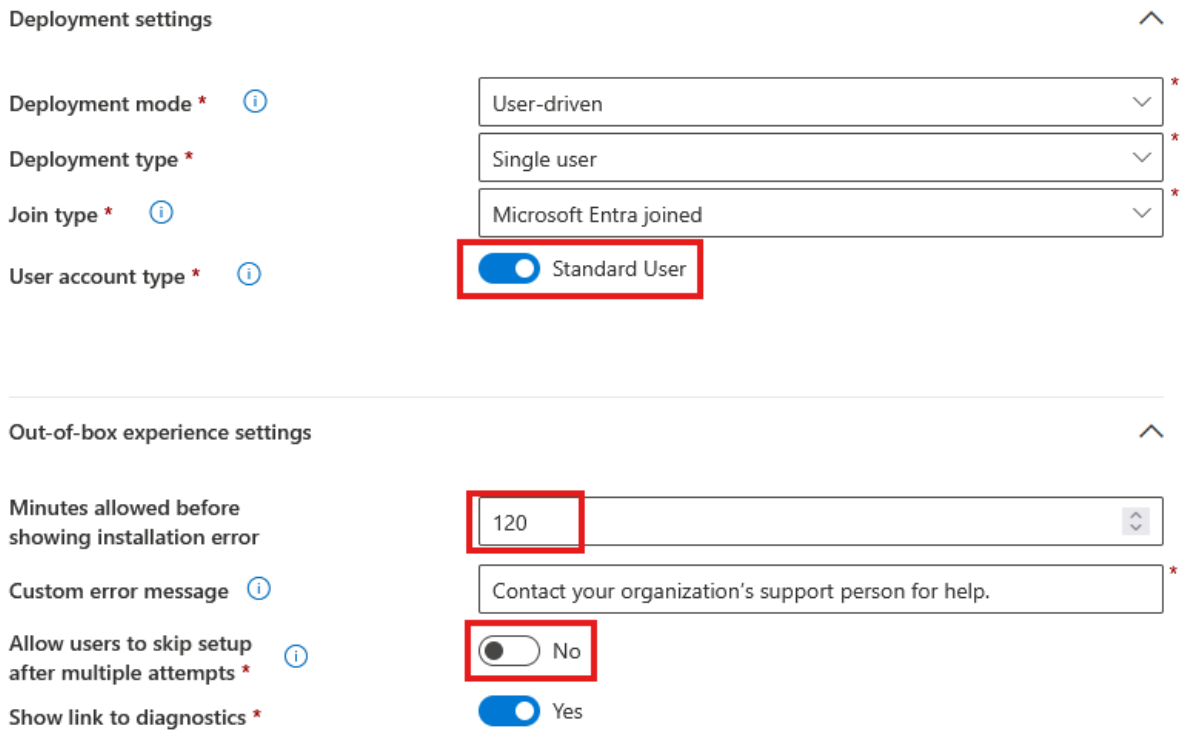
V záložce **Introduction** je popsané, co tato politika dělá a odkaz na ne moc přehledný **Microsoft Learn**, který popisuje, jak politiku nastavit. Pod záložkou **Basics** si politiku pojmenujeme a přidáme jí popisek, který říká, jaké aplikace a scripty budeme do počítače posílat.



Pod záložkou **Device Group** musíme přidat security skupinu, která je **assigned** a její **Owner** je účet s tímto ID **f1346770-5b25-470b-88bd-d5744ab7952c.** Tento účet je tzv. **Intune Provisioning Client** nebo **Intune Autopilot ConfidentialClient**, který bude automaticky zařazovat zařízení do vámi vytvořené skupiny a potom s nimi pracovat. Pokud tento účet nemáte v **tenantu**, tak vás odkážu na dříve zmiňovaný **Microsoft Learn** článek (https://learn.microsoft.com/en-us/autopilot/device-preparation/tutorial/user-driven/entra-join-device-group). Poté co vytvoříme skupinu, tak ji přidáme do nastavení **Autopilota**.

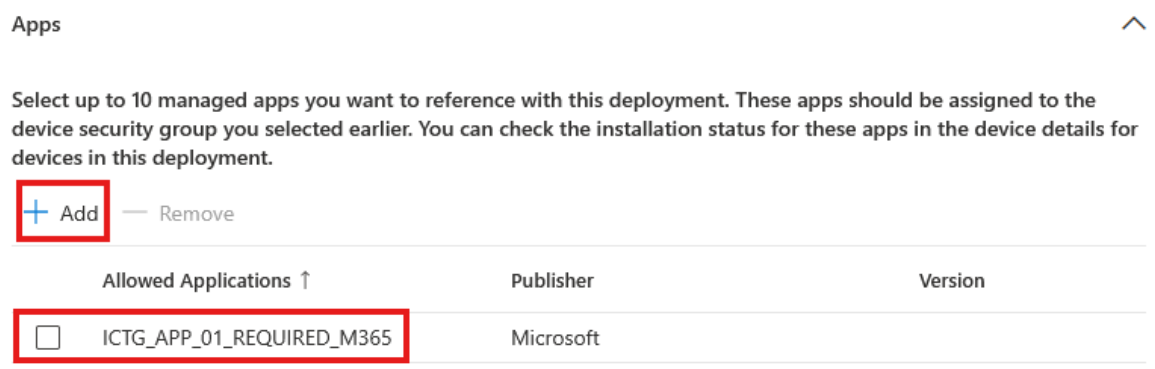


Jako další si nastavíme, jak se samotný **Autopilot** bude chovat, co bude dělat, jaké aplikace nainstaluje, a jaké **scripty** pustí.



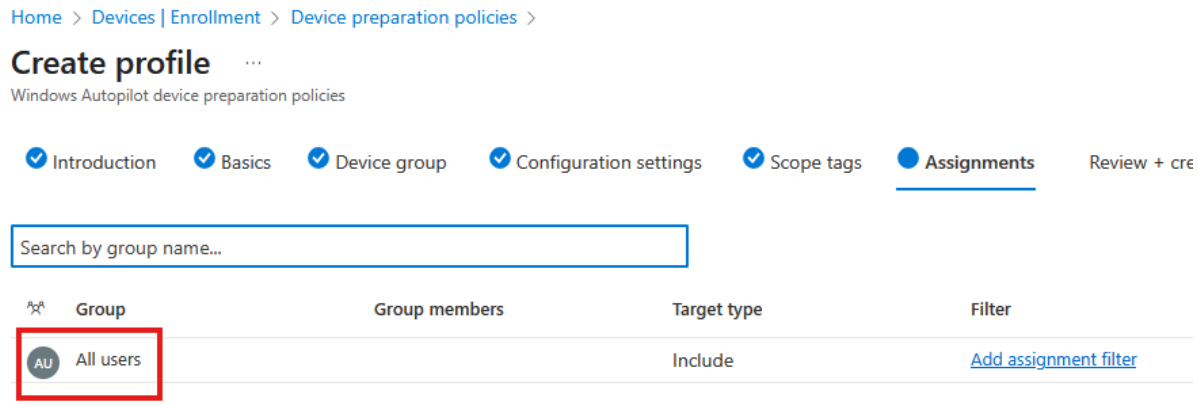
Toto nastavení zařadí počítač do systému **EntraID**, nastaví limit před ukázáním **errorové** hlášky na 2 hodiny a zakáže uživateli přeskočit toto nastavení.

Teď si přidáme vynucené aplikace, v našem případě máme na výběr jen **M365**, protože jsme jiné nepřidávali. Můžete, ale vynutit až 10 aplikací při samotné instalaci počítače, což by mělo pokrýt i náročnější uživatele.



Scripty zatím žádné nemáme, takže jdeme dál.

Scope tag necháme už klasicky na **Default** a v záložce **Assignments** si přidáme skupinu uživatelů.



A máme hotovo. Nezapomeňte, že takováto nastavení občas trvají 24 nebo až 48 hodin na propsání, takže není dobrý nápad hned testovat, ale s přicházející **deadline** na **upgrade** z **Windows** 10 na 11, si můžete potencionálně ušetřit nějakou tu hodinu, nebo 20.

[ICT] GROUP

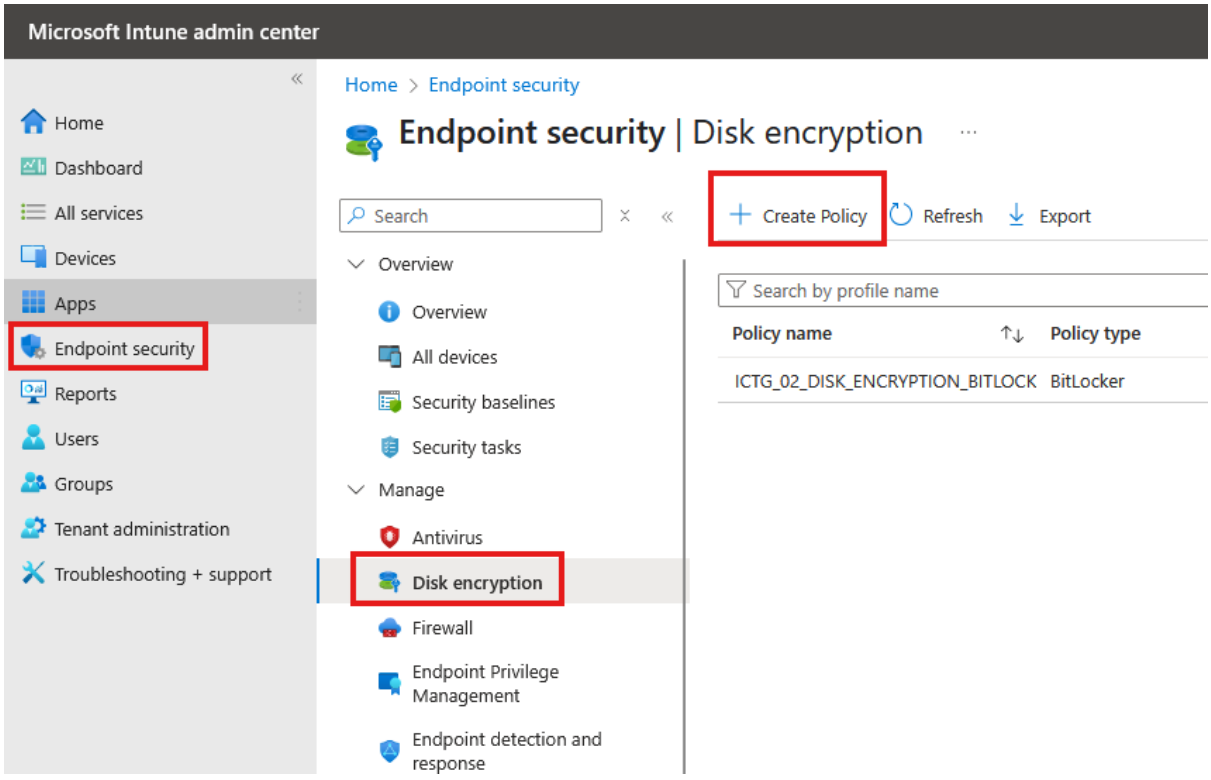
Automatický BitLocker

Postupně se dostáváme k nastavení zařízení a jejich zabezpečení. Zde se dá nastavit opravdu snad cokoliv, a i to bych řekl, že je málo. Pokud potřebujete nastavit co se stane po zavření počítače, tak hledejte zde. Stejně tak, ale pokud chcete zablokovat hru s dinosaurem v **chromu**, je tu opravdu všechno. Malý **disclamer** na začátek, nastavení, které si s vámi projdu v následujících pár článcích se nebudou ani blížit všemu co se nastavit dá, spíše zachycují pro nás ty nejdůležitější politiky, které opravdu potřebujeme na každém počítači.

Dnes se konkrétně podíváme na nastavení šifrovacího nástroje od **Microsoftu** a tím je **BitLocker**. **BitLocker** je pojistka proti ukradení disku, nebo klonování počítače a osvědčil se, jako jedna z povedenějších částí **Windows**. Samozřejmě se dá zapnout manuálně a většina počítačů ho zapnutý má z výroby, přesto definitivně není dobrý nápad na to spoléhat.

BitLocker se dá, jako spousta věcí, nastavit z více míst. Já v tomto článku použiji tu modernější cestu. Pro nastavení si otevřete **Intune > Endpoint Security > Disk Encryption** a poté **Create Policy,** u **Select platform** vyberte **Windows** a u **Profile** vyberte **BitLocker**.

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SecurityManagementMenu/~/diskencryption



Politiku pojmenujte a přejděte dál. Teď přichází jádro pudla, na kterém vyhoří většina lidí (na nějaký čas jsem nebyl výjimkou) a to je samotné nastavení. Většina lidí chce **BitLocker** bez nutnosti pinu navíc a já k nim patřím, takže to je to, co si ukážeme.

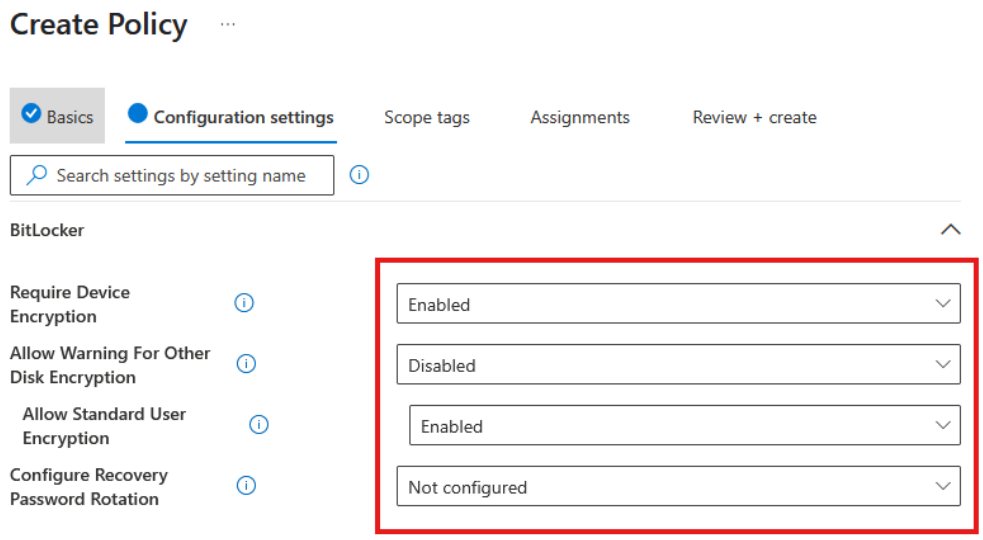
Pod záložkou **BitLocker** vyberte:

Require Device Encryption – Enabled

Allow Warning For Other Disk Encryption – Disabled

Allow Standard User Encryption – Enabled

Configure Recovery Password Rotation – Not configured

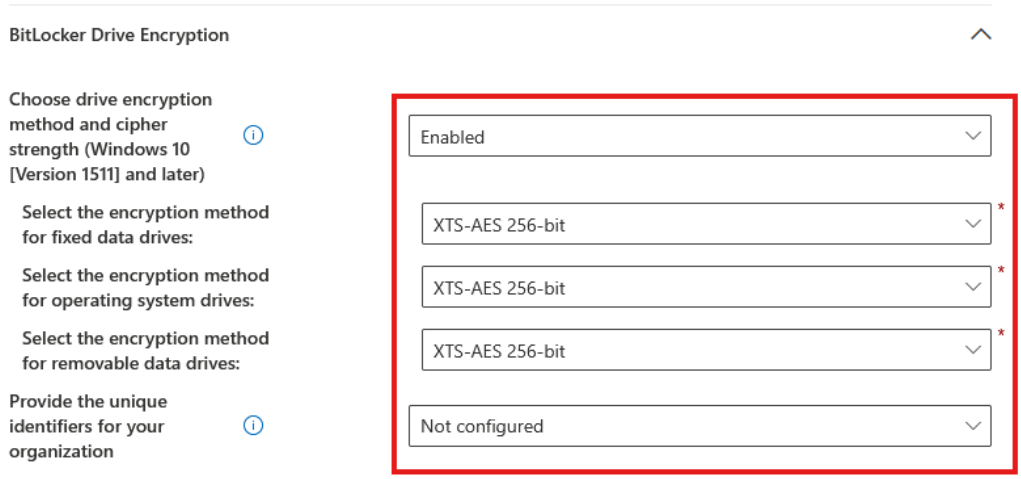


Dále pod záložkou **BitLocker Drive Encryption** vyberte:

Pro první možnost – **Enabled**

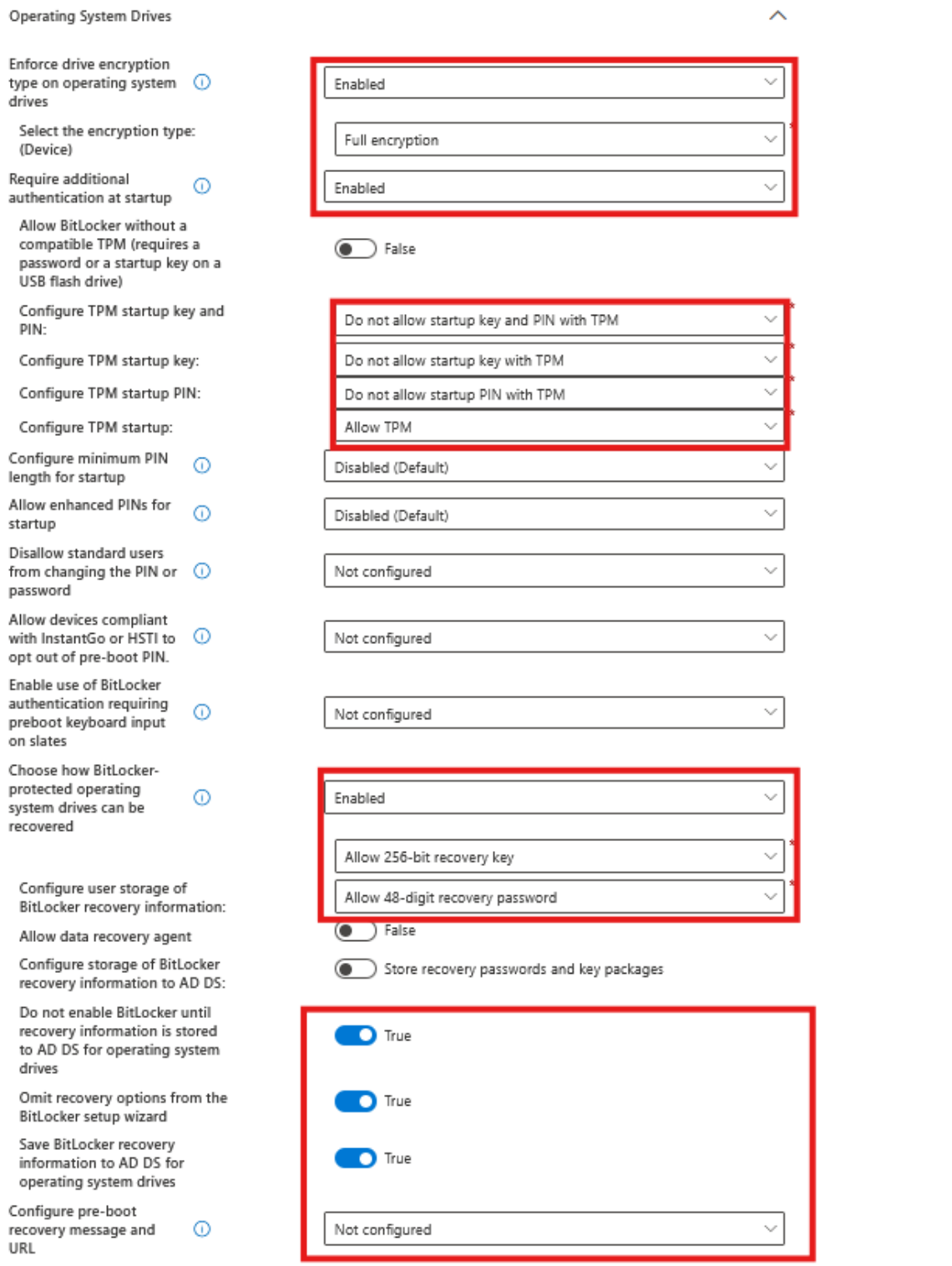
Pro prostřední tři – **XTS-AES 256-bit**

A pro poslední – **Not configured**

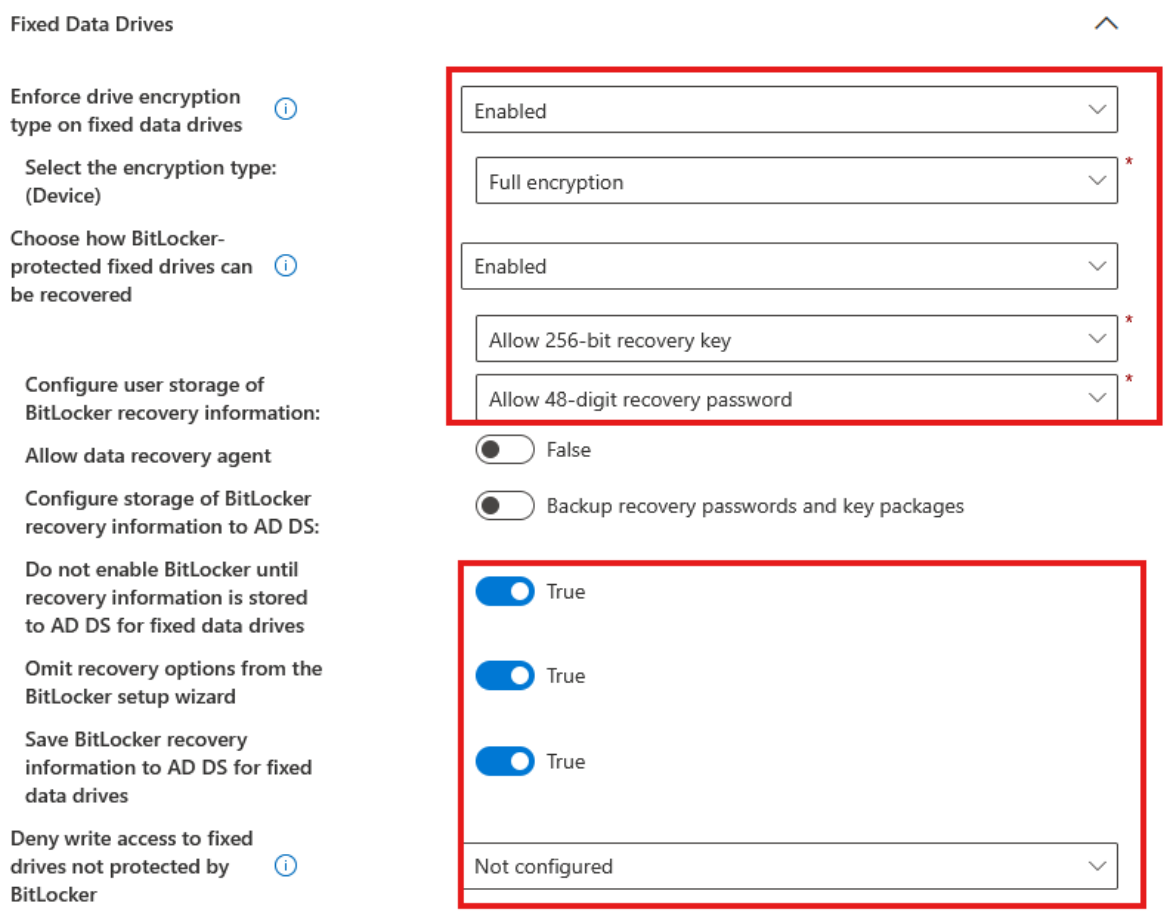


První nastavení z předchozího bodu zajišťuje možnost vybrat si jakou metodou disky šifrovat a další tři specifikují typ šifrovací metody, pro fixní disky, disky s operačním systémem a **flash** disky.

Pod záložkou **Operating System Drives** nastavíme, co je vidět na screenshotu (většina polí se vysvětlí sama)



U **Fixed Data Drives** je nastavení v základu stejné, až na to že neřešíme, co se má dít po nastartování počítače a jestli chceme další pin.



Ve zkratce toto nastavení vynutí šifrování i sekundárních disků. Nastaví jim 256bitový **recovery** klíč a 48místné **recovery** heslo. Poté uloží **recovery** klíče do **AD DS** nebo **EntraID.**

Pro odnímatelné disky nemám šifrování nastavené, protože je to pro nás zatím nedůležité. Nastavení je ale stejné.

Poté stačí zacílit na skupinu zařízení a máte hotovo!!!

[ICT] GROUP

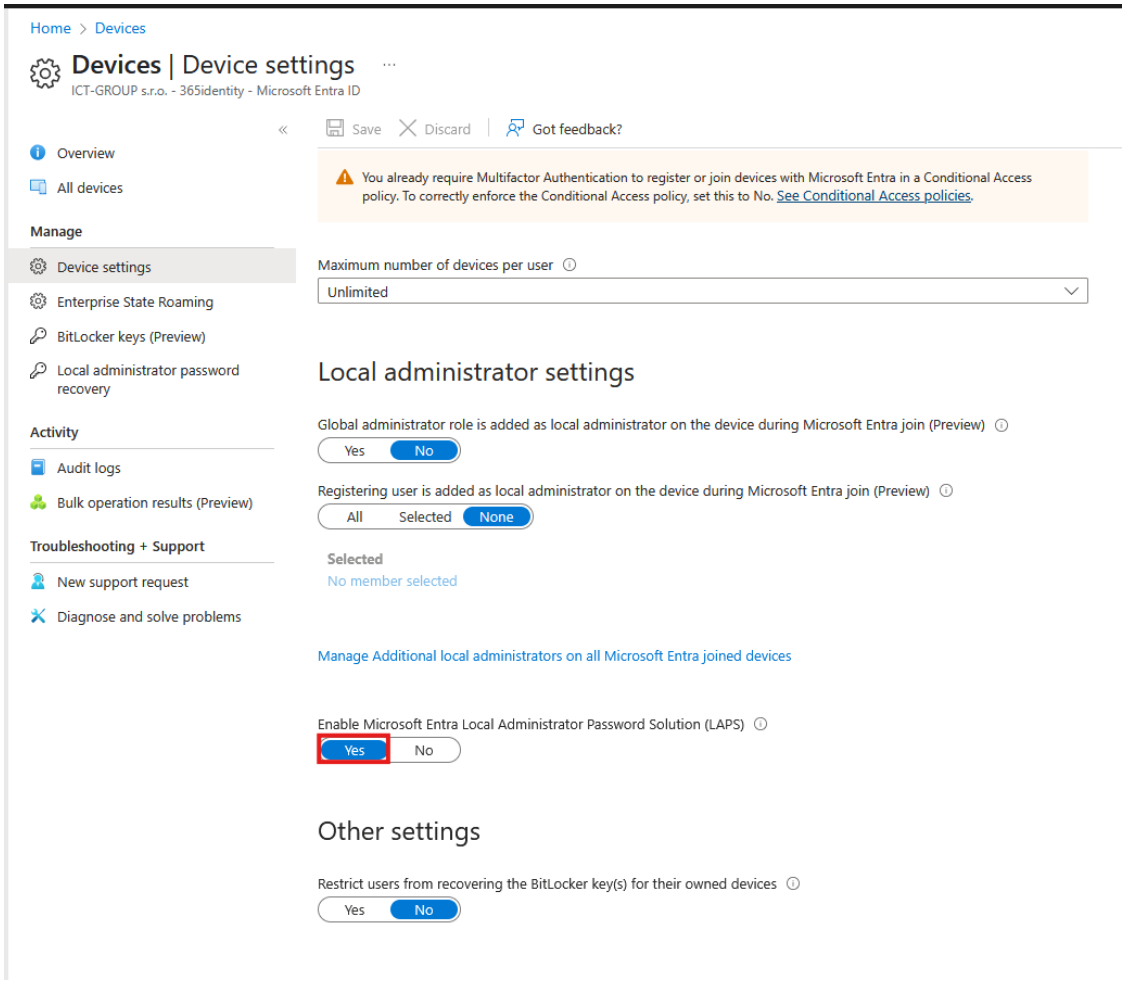
LAPS (local administrator password solutions)

LAPS je jedna z věcí, se kterou jsme celkem bojovali. Před nedávnem jsme ale přišli, jak na to. V základu to není úplně složitá funkce, ale je potřeba spousta pro to, aby fungovala správně a používala **best practice** nastavení neboli nepoužívala zabudovaný účet **„Administrator“**. Tato funkce na každém **Windows** zařízení, které je spravované pomocí **Intune,** vytvoří účet lokálního administrátora, kterému se periodicky mění heslo. Toto je ideální, když chcete někomu udělit přístup lokálního administrátora bez vytváření dedikovaného účtu pro něj, prostě pošlete heslo, a to po nějaké době vyprší nebo se automaticky vyresetuje po použití a restartu počítače. Samozřejmě pokud si člověk v dobu, co má přístup k heslu od účtu lokálního administrátora vytvoří svůj účet, který bude lokální administrátor, tak jste v průšvihu. I to se dá kontrolovat, ale na to se zaměřovat v tomto článku nebudu.

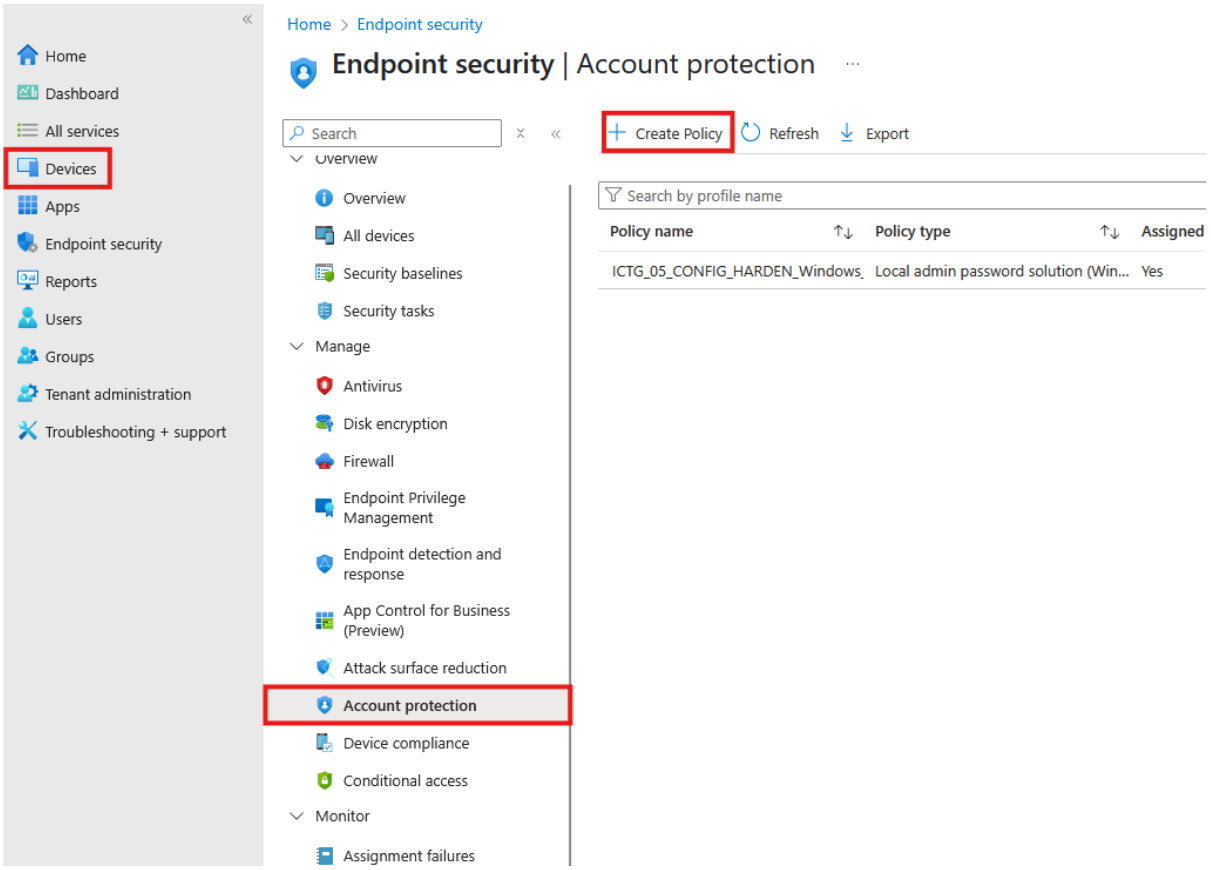
Jak takovouhle srandu nastavit?

Nejprve ji musíte povolit v portálu **Entra**. Otevřete si portál **Entra > Devices > All devices > Device settings** a zapněte možnost **Enable Microsoft Entra Local Administrator Password Solution (LAPS)**

https://entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/DeviceSettings/menuId/Overview



Poté si vytvoříme politiku, která bude říkat, jak má vypadat heslo pro účet, a jak často se má obnovovat. Pro to si otevřeme portál **Intune > Endpoint security > Account protection** a klikneme na **Create Policy.**



Vybereme platformu **Windows** a profil **Windows LAPS.**

Politiku si pojmenujeme a dáme jí popis.

Poté klikneme na další a pustíme se do nastavování **LAPS.**

Jako **Backup Directory** si vybereme **Azure AD only.**

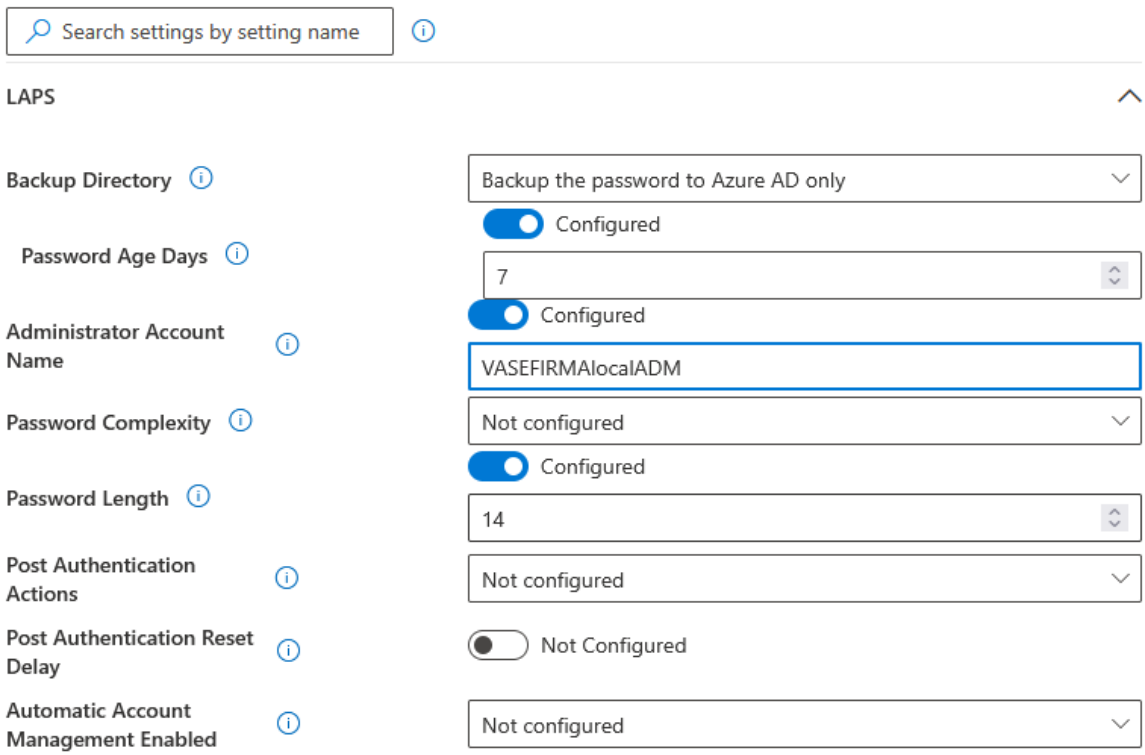
Administrator Account Name určuje, pro jaký účet se bude heslo měnit. Pozor nevytváří účet!!!

Password Age Days je z velké části na vás s tím, že budeme používat reset po použití a restartu zařízení, tak není tento údaj tak důležitý. I tak bych nastavil 30 dní max.

Password Complexity rozhodně co jde a **Improved readability** je dobrý nápad.

Password Length minimálně 14, já používám 16.

Post Authentication Action je právě reset hesla po **rebootu**.

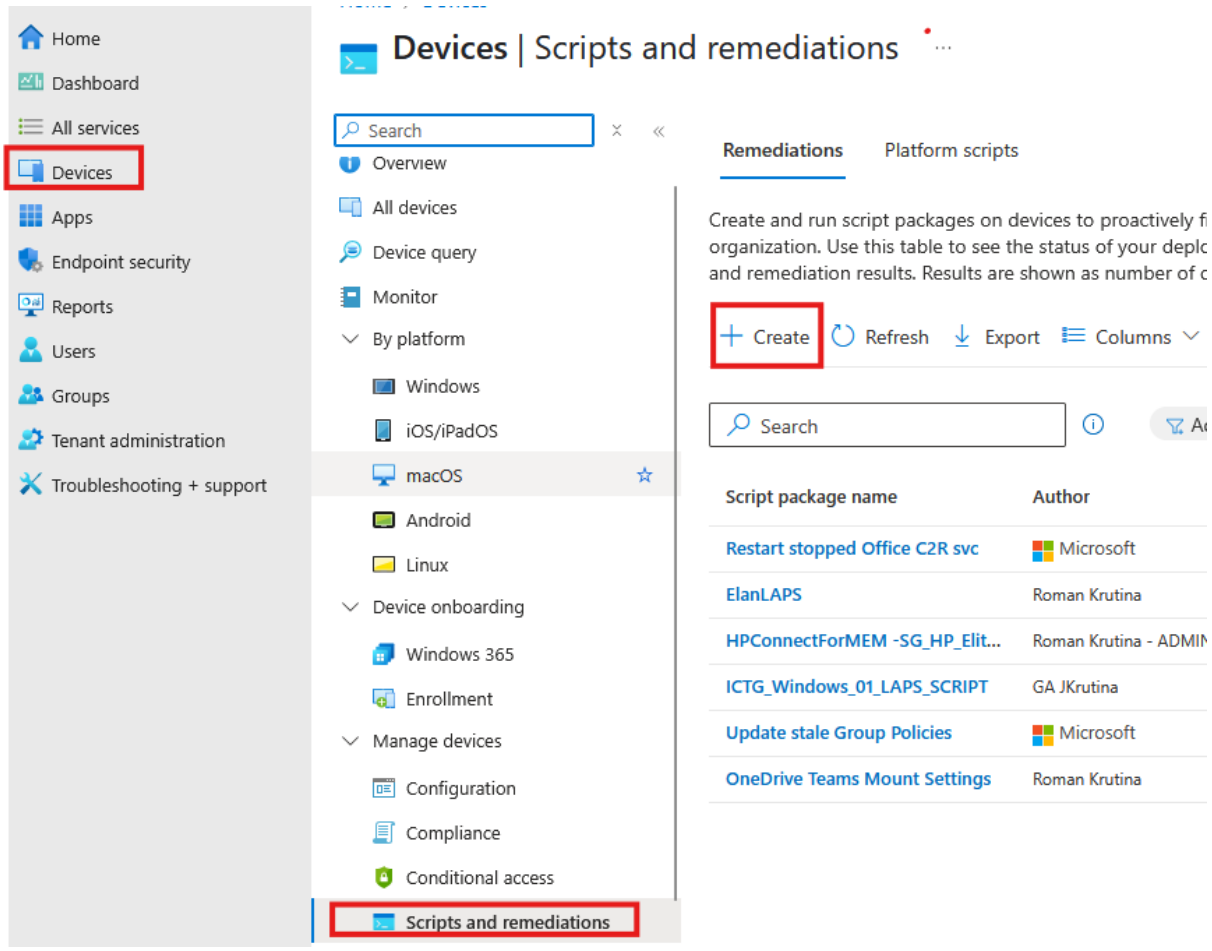


Scope tag je **default.**

Politiku zacílíme na skupinu zařízení spravovaných pomocí **Intune.**

[ICT] GROUP

Teď na tu zajímavou část, a tou je vytvoření **remediation scriptu.** Otevřete si **Intune > Devices > Scripts and remediations** a klikněte na **Create.**



Script pojmenujte a dejte a popište, co dělá a jaký účet vytváří

Do první časti nahrajte **powershell script**, který kontroluje, jestli na počítači je takový účet

```
$username = "VASEFIRMAlocalADM“
try {
  $user = Get-LocalUser -Name $username -ErrorAction Stop
  if ($user.Enabled) {
    Write-Output ("User {0} present and enabled" -f $username)
    exit 0
  }
  else {
    Write-Output ("User {0} present but NOT enabled" -f $username)
    Exit 1
  }
}
catch {
  Write-Output ("User {0} not found" -f $username)
  Exit 1
}
```

Vyměňte VASEFIRMAlocalADM za jméno, které jste nastavili v **LAPS** konfiguraci.

Do druhého pole nahrajte tento **script**, který vytváří lokální účet VASEFIRMAlocalADM a přidává ho do skupiny administrators

```
Add-Type -AssemblyName 'System.Web'

$userParams = @{
   Name = 'VASEFIRMAlocalADM '
   Description = 'LAPS Client Admin'
   Password = [System.Web.Security.Membership]::GeneratePassword(16, 0) | ConvertTo-SecureString -
AsPlainText -Force
}

# create user with random password
$user = New-LocalUser @userParams

# Add user to built-in administrators group
Add-LocalGroupMember -SID 'S-1-5-32-544' -Member $user
```

Poté nastavte, že se účet nespustí pod právy uživatele, a že spustí v **64-bit PowerShellu.**

Poté stačí zacílit stejně, jako **LAPS** konfigurace a máte hotovo!!!

[ICT] GROUP

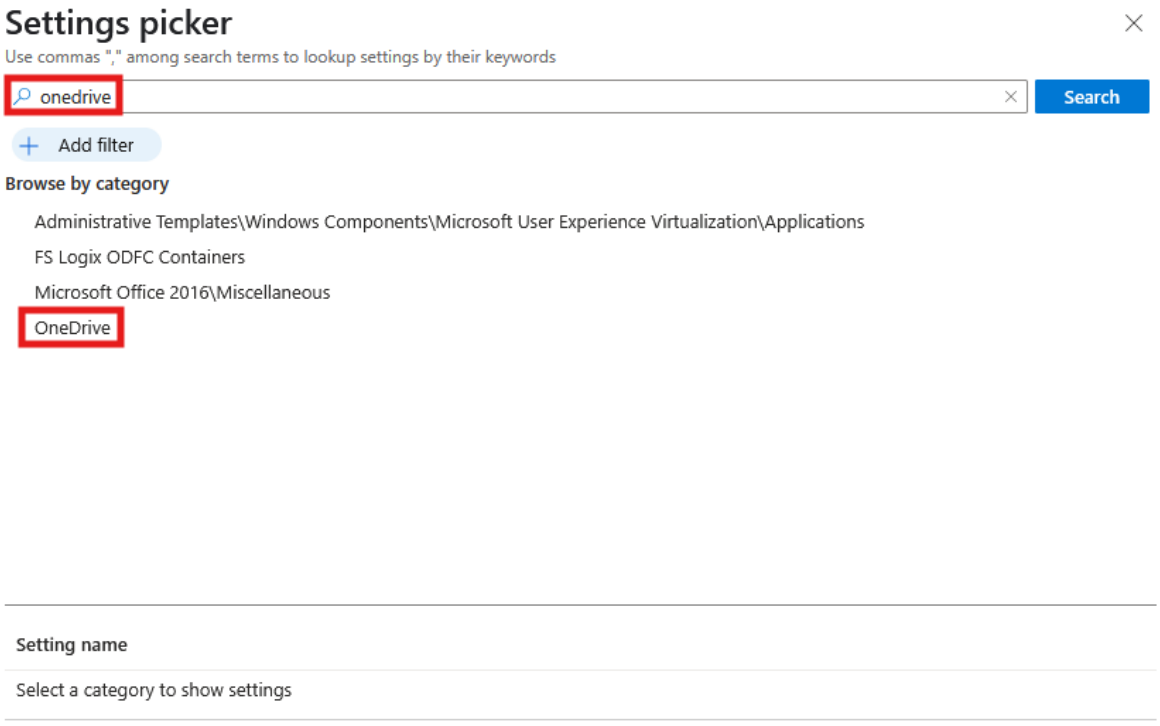
Automatický OneDrive sync

Dneska tu máme zase menší nastavení, které je ale absolutní záchrana, pokud používáte **OneDrive**. A teda vlastně i pokud ho moc nepoužíváte. Tahle konfigurace řeší automatické přihlášení do **OneDrive** a mapování standardních složek do **OneDrive**. Proč by vás to mělo zajímat? Protože až si jednou některý z vašich zaměstnanců uloží jednou kopii toho důležitého souboru na plochu a potom mu selže disk, tak to budete mít na **OneDrive,** a ne v koši. Jediné, co je důležité zmínit je, že toto nastavení funguje jen na **EntraID joined** zařízeních.

Jak to nastavit? Otevřete si **Intune > Devices > Configuration** a **Create > New Policy** poté **Windows 10 and later** a **Settings catalog**

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/configuration

Politiku si pojmenujeme a dáme jí popis. Klikněte na **Add settings** a napište **OneDrive** a klikněte na možnost **OneDrive.**



Poté vyberte možnosti:

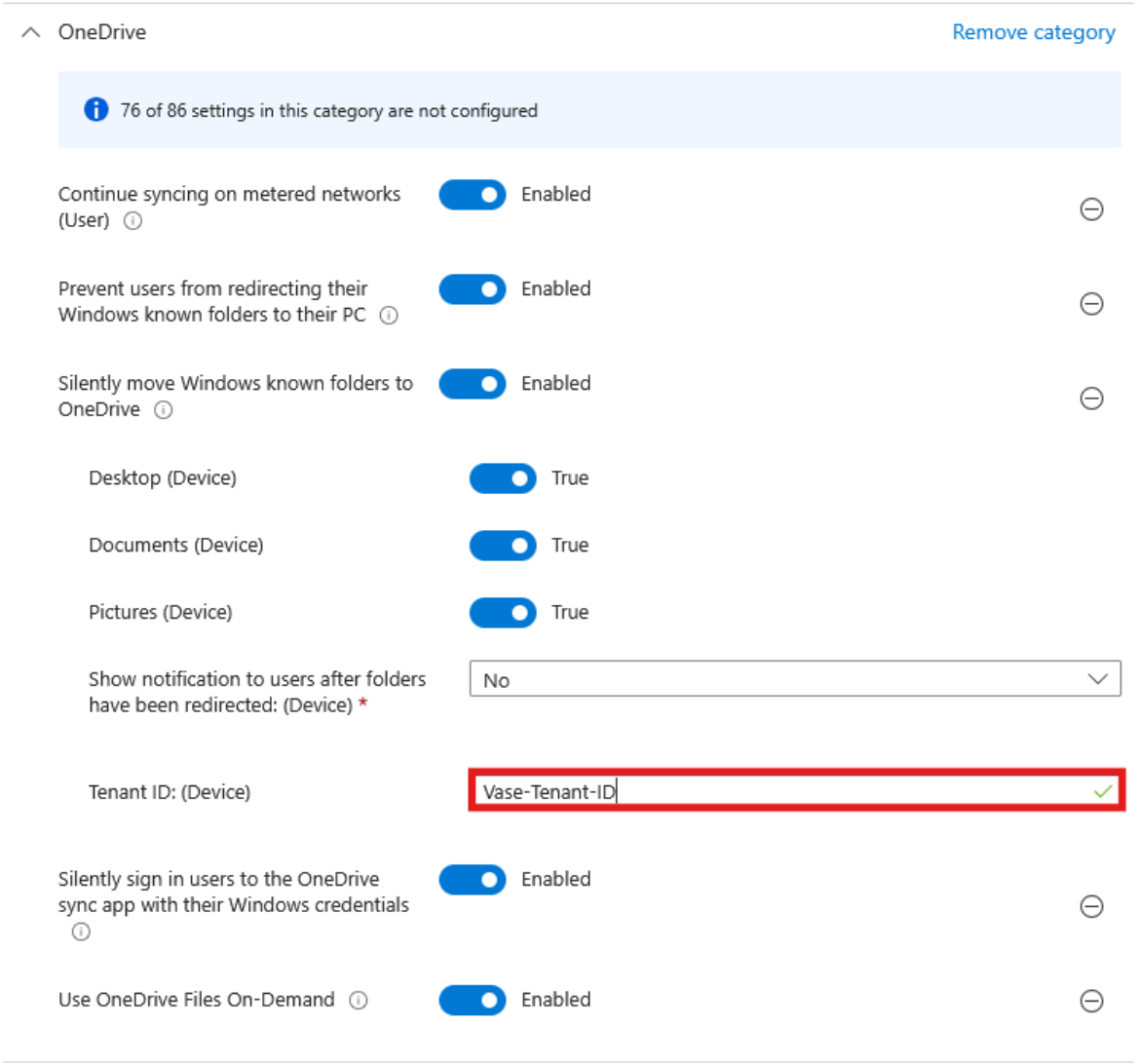
Use OneDrive Files On-Demand

Silently sign in users to the OneDrive sync app with their Windows credentials

Silently move Windows known folders to OneDrive

Prevent users from moving their Windows known folders to OneDrive

Continue syncing on metered networks (User)



Do červeného obdélníku vyplňte vaše **tenant ID**, to najdete na úvodní stránce v portálu **Entra**.

Důležitá věc je zacílit tohle na skupinu uživatelů. Doporučuji vytvořit **dynamic device** skupinu se syntaxí *(device.deviceTrustType -eq "AzureAD")*. To vytvoří skupinu, ve které budou jenom Entra Joined zařízení. Na tu stačí politiku zacílit a máte hotovo!

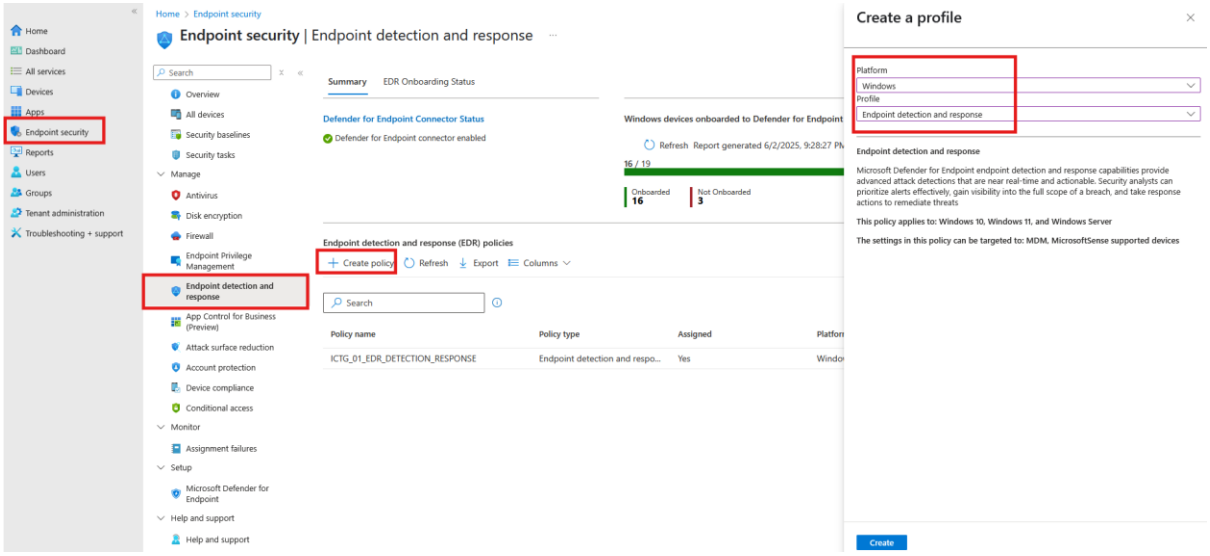
[ICT] GROUP

Defender for Endpoint enrollment

Název této kapitoly může znít složitě, ale složité to rozhodně není. Pokud máte nastavený konektor mezi **Intune** a **Defender for Endpoint**, tak je toto nastavení na maximálně 5 minut. Pokud nemáte nastavený konektor, tak se podívejte na stranu 47 (nebo přes **Ctrl+LClick** na číslo 47 😉). Pokud konektor máte, tak se pojďme podívat na nastavení.

Otevřete si **Intune admin centrum > Endpoint security > Endpoint detection and response > Create policy**

Vyberte platformu **Windows** a profil **Endpoint detection and response** poté klikněte na **Create**



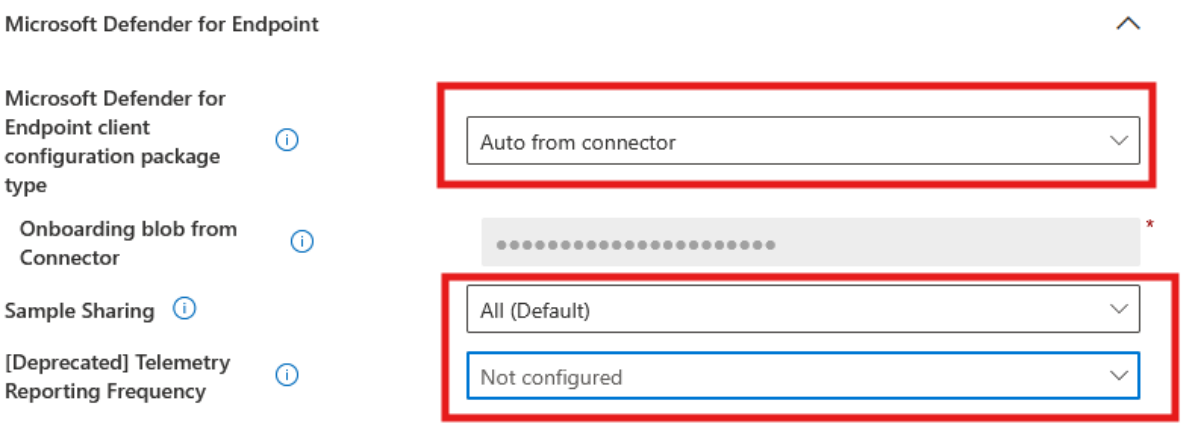
Politiku pojmenujte a dejte jí popis. Třeba *automatický **enrollment** pro **DfE***

V nastavování toho moc nevymyslíte, pro:

Microsoft Defender for Endpoint client configuration package type nastavte **Auto from connector.**

Sample Sharing na **All.**

Poslední kolonka nehraje v nastavení žádnou roli, protože je **Deprecated.**



Scope tag nechávám zase na **Default** a cílím politiku na skupinu s **Entra Joined zařízeními.** A máte první část antiviru nastavenou. V příštím článku se podíváme na tu druhou část!

Defender for Endpoint AV nastavení

V poslední epizodě jsme se podívali na to, jak zařadit zařízení do **Defender for Endpoint,** dnes se podíváme na to, jak využít tohoto antiviru naplno bez toho, aby vás co možná nejméně otravoval. Nastavit se totiž dá velká spousta věcí, ale žít se nedá s většinou. Nastavení je tu opravdu spousta, takže se do toho bez dalšího otálení pustíme.

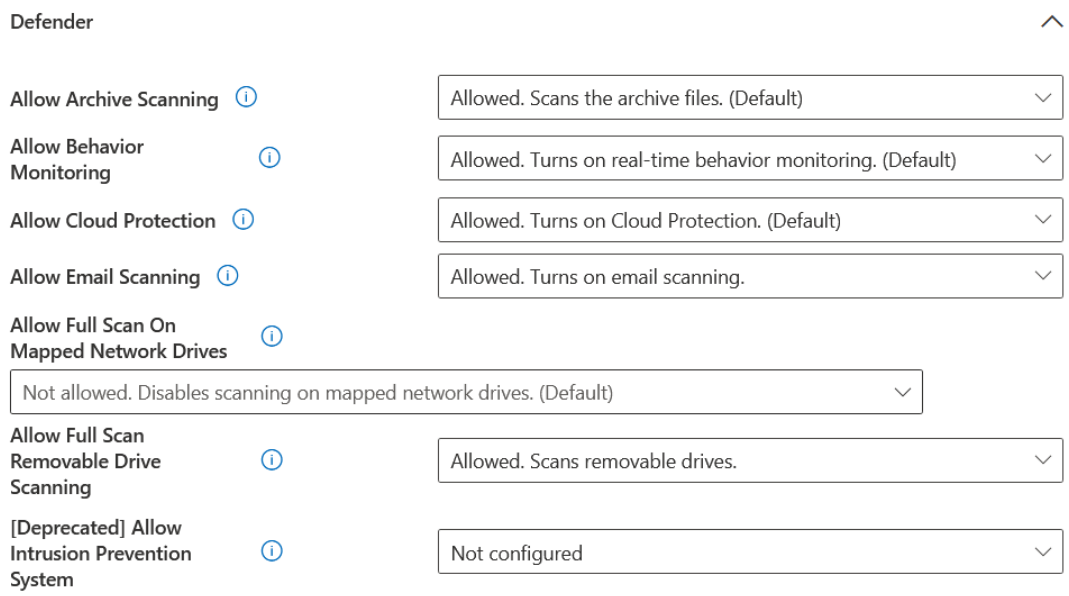
Otevřete si administrátorský portál **Intune,** v něm záložku **Endpoint security** a zde záložku **Antivirus.**

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SecurityManagementMenu/~/antivirus

Zde pod menu **Summary** klikněte na **Create Policy,** jako platformu vyberte **Windows** a jako profil vyberte **Microsoft Defender Antivirus.**

Politiku pojmenujte a pokud chcete, tak jí dejte popis. (Něco typu **Less restrictive AV**)

[ICT] GROUP



Allow Archive Scanning – povoluje/zakazuje **AV** skenování archivů, jako je **.ZIP** nebo **.CAB**.

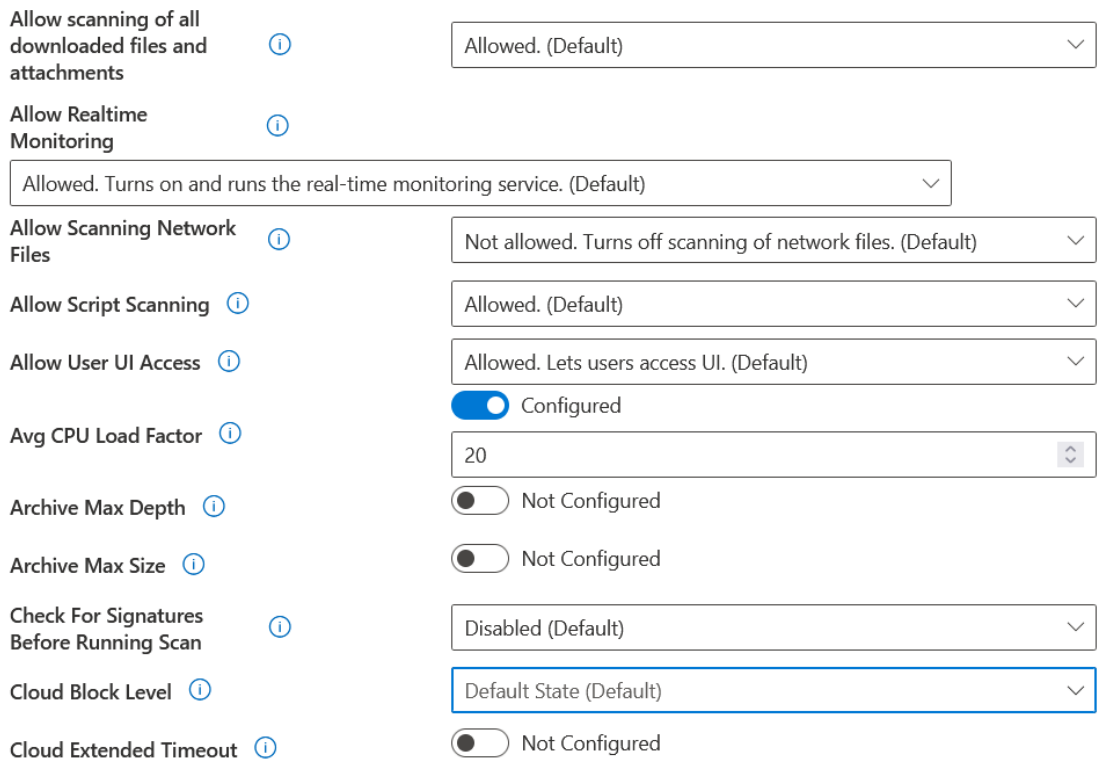
Allow Behavior Monitoring – povoluje/zakazuje **AV** sledovat a kontrolovat zvláštní aktivitu a blokovat ji v reálném čase

Allow Cloud Protection – posílá/neposílá informace o problémech nalezených na vašem počítači **Microsoftu**

Allow Email Scanning – povoluje/zakazuje skenování emailu

Allow Full Scan On Mapped Network Drives – P/Z (povoluje/zakazuje) skenování síťovích úložišť např. **NAS**

[Deprecated] Allow Intrusion Prevention System – již nedělá nic



Allow scanning of all downloaded files and attachments – P/Z skenování všech stažených souborů a doplňků

Allow Realtime Monitoring – P/Z monitorování hrozeb v reálném čase

Allow Scanning Network Files – P/Z skenování souborů dostupných na síti. Doporučuji toto nastavení mít zapnuté, ale u nás dělalo neplechu

Allow Script Scanning – P/Z skenování skriptů

Allow User UI Access – P/Z přístup uživatelů do nastavení **Defenderu** ve **Windows**

Avg CPU Load Factor – Nastavuje přibližnou průměrnou hodnotu využití procesoru při skenování. Pokud máte starší HW, tak doporučuji rozhodně nepřekračovat 20 %, na novějších strojích klidně jděte na 30-40 %

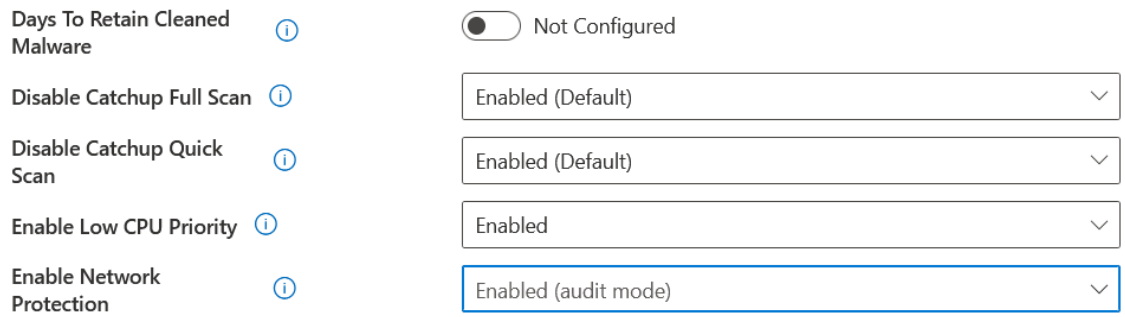
Archive Max Depth – Nenastavuji, protože chci skenování všech složek. Jinak řeší, jak hluboko do složek se bude **Defender** koukat

Archive Max Size – Nenastavuji, protože chci skenování všech souborů. Jinak řeší, jakou maximální velikost může mít soubor, aby byl oskenován a větší soubory se skenovat nebudou

Check For Signatures Before Running Scan – P/Z kontrolování **hashe** programů a porovnává je s databází **hashů**, ještě před samotným skenem. Pro nás bylo toto nastavení zbytečně náročné na síťové připojení se vším možným ostatním, ale je to určitě dobrá fičura

Cloud Block Level – Určuje, jak moc bude **Defender** agresivní při blokaci/karanténě

Cloud Extended Timeout – P/Z **Defenderu** pozastavit fungování a procesy souboru a prozkoumat jeho fungování



Days To Retain Cleaned Malware – Nastavuje, jak dlouho se **malware** zachová na zařízení, než se smaže. Ve stavu **Not Configured** se **malware** smaže hned

Disable Catchup Full Scan a **Disable Catchup Quick Scan** Z/P oskenovat počítač poté, co se nestihl ten předchozí sken

Enable Low CPU Priority P/Z využití nízké priority výkonu procesoru při kompletaci naplánovaných skenů

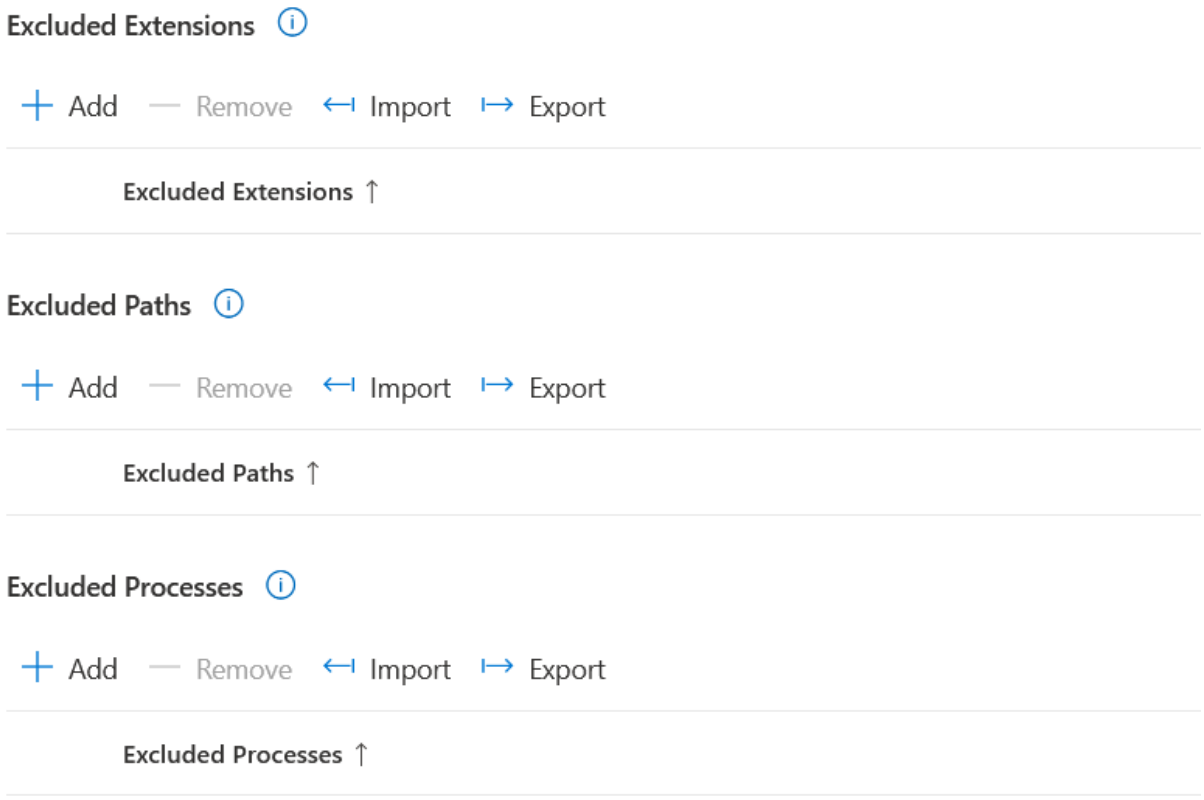
Enable Network Protection – chrání proti **Phishingu** a **malware** stránkám. Cíl je dostat se z **Audit modu** do **Block modu**, ale cesta tam je ještě dlouhá

Protože je nastavení v tomto bloku opravdu mraky a většina z nich má celkem slušný dopad, tak jsem se rozhodl rozdělit tuto epizodu na 2 části. Takže příští týden nás čeká **PUA** a **Threat Severity Default Action.** Bezpečnosti ZDAR!

[ICT] GROUP

Defender for Endpoint AV nastavení část druhá

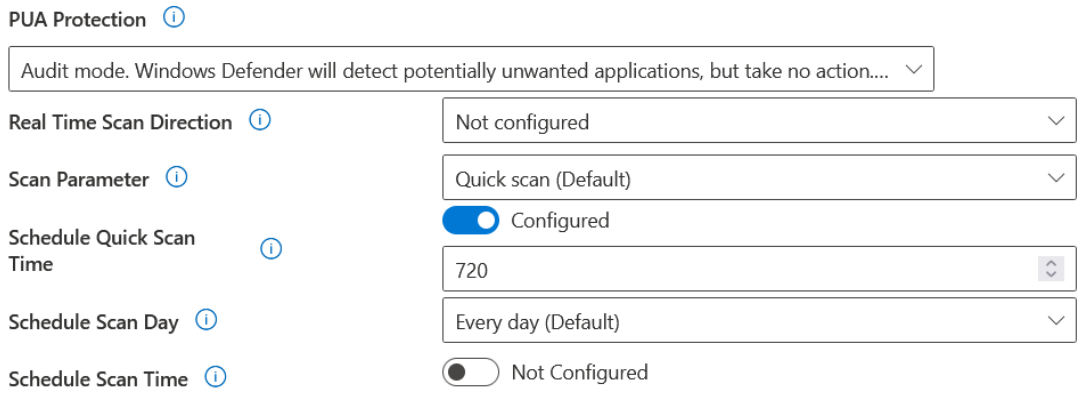
Sice s týdenní pauzou, ale přece. Vracíme se k nastavení **Defender for Endpoint AV**. Nebudeme to zdržovat a podíváme se rovnou na zbývající nastavení.



Excluded Extensions – Vylučují typy souborů, které se nemají skenovat

Excluded Paths – Vylučují specifikované složky nebo soubory, ty jsou specifikované cestou k souboru/složce

Excluded Processes – Vylučují úlohy, které nemají být skenované



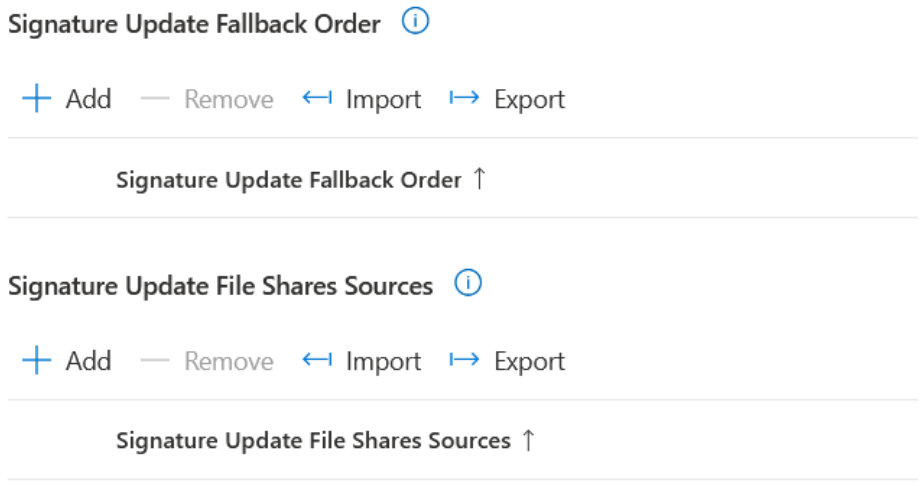
PUA Protection – Řeší, co má **Defender** dělat s potencionálně nechtěnými aplikacemi. **Audit** mód vyhodí uživateli upozornění, že aplikace je potencionálně nechtěná, ale nechá ho aplikaci nainstalovat. **ON** nedovolí aplikaci nainstalovat, rovnou ji zablokuje a zařadí jako incident. Cíl je mít tohle ve stavu **ON**, ale bohužel je vyhodnocení občas problematické

Real Time Scan Direction – Řeší, které soubory mají být skenované v reálném čase. **Not configured** je lehce neideální a doporučuji používat **bi-directional**, ale může to být lehce náročné na internet.

Scan Parameter – Nastavuje, jestli budete pouštět plný sken nebo **Quick scan**

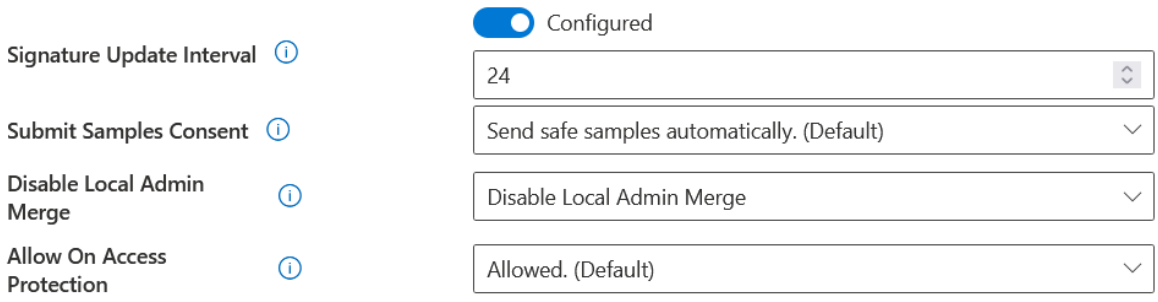
Schedule Scan Day – Určuje kadenci skenování

Schedule Scan Time – Určuje, v jaký přesný čas se sken pustí



Signature Update Fallback Order – Nastavuje, v jakém pořadí bude **Defender** kontaktovat zdroje, ze kterých si bude brát bezpečností aktualizace. Pokud toto (jako já) nenastavíte, tak se použije základní nastavení

Signature Update File Shares Sources – Řeší velmi podobnou věc, jako předchozí nastavení, a není potřeba se jím zabývat

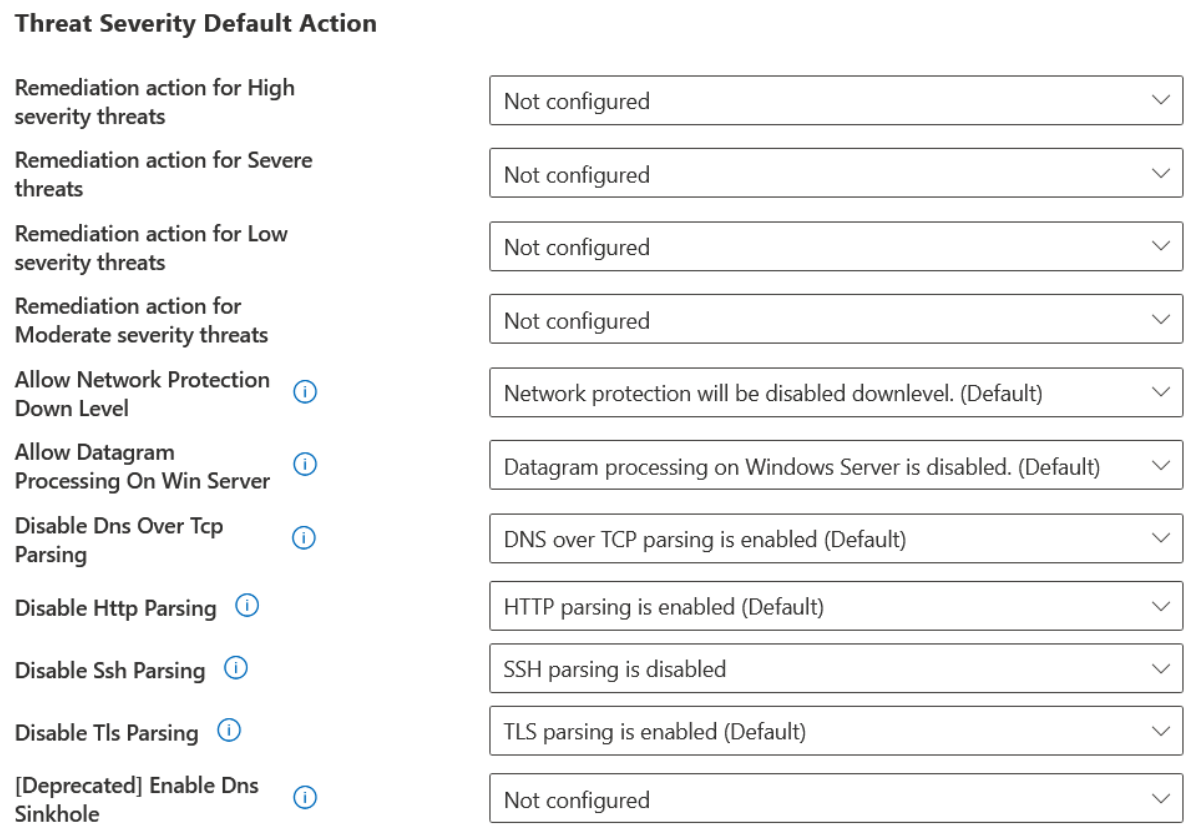


Signature Update Interval – Nastavuje, za jakou dobu se bude aktualizovat databáze **Signatures** virů. 24 určuje počet hodin, po kterých se tato aktualizace provede

Submit Samples Consent – Povoluje posílat některé informace **Microsoftu.** Ač nejsem pro posílání informací, tak toto mi moc nevadí

Disable Local Admin Merge – Zakazuje přepisování nastavených hodnot z **Intune**, i když je uživatel lokální administrátor

Allow On Access Protection – Povoluje kontrolu chování souborů a programů v reálném čase



První 4 nastavení řeší, co se stane po kategorizaci nebezpečí do jedné ze čtyř kategorií

Allow Network Protection Down Level – Řeší síťové zabezpečení starších **Windows 10** zařízení (1703)

Allow Datagram Processing On Win Server – Nastavuje síťové zabezpečení **Windows** Serverů

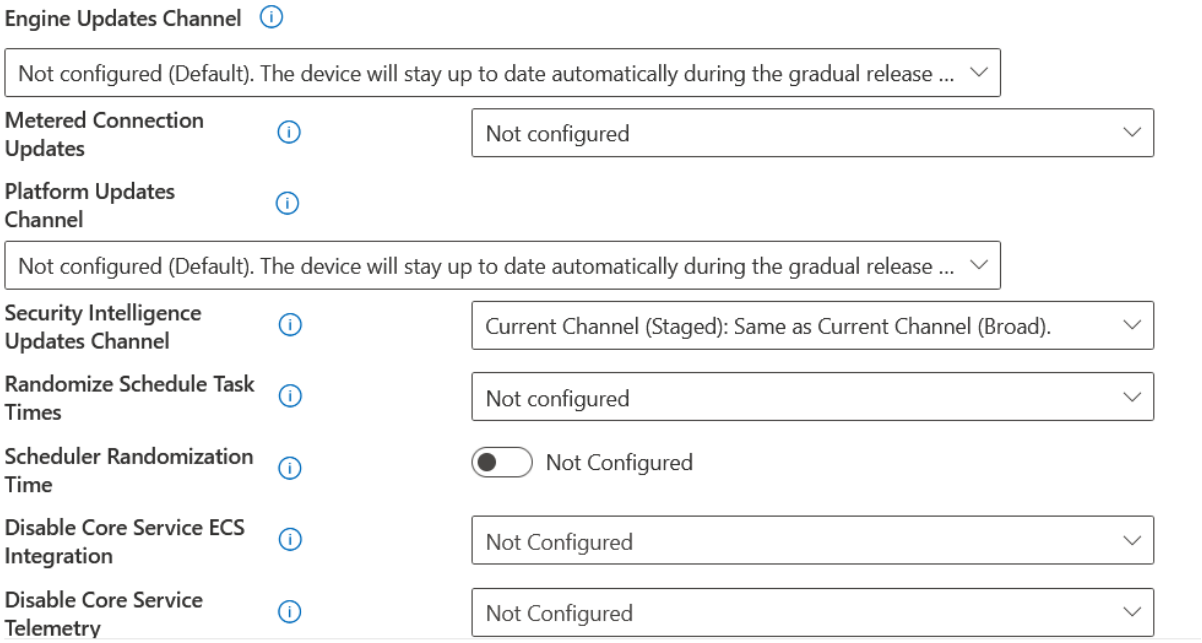
Disable Dns Over Tcp Parsing – Nastavuje kontrolu DNS dotazů

Disable Http Parsing – Povoluje/zakazuje kontrolu HTTP komunikace

Disable Ssh Parsing – P/Z kontrolu SSH komunikace (máme vypnuté, protože neprovozujeme moc **Linuxů**)

Disable Tls Parsing – P/Z kontrolu TLS komunikace

[Deprecated] Enable Dns Sinkhole – Již nedělá nic



Engine Updates Channel – Nastavuje kadenci aktualizací **Defender Engine**

Metered Connection Updates – P/Z aktualizaci **Defenderu** na měřených síťových připojeních

Platform Updates Channel – Nastavuje kadenci aktualizací **Defender Platform**

Security Intelligence Updates Channel – Nastavuje kadenci aktualizací „Inteligence“ (databáze virů)

Toto by mělo být vše pro nastavení **security** v tom jednoduchém slova smyslu, jestli se tohle dá považovat za jednoduché. V příštích pár článcích se pustíme do velké neznámé pro skoro všechny, a tím je integrace **Apple** zařízení s **Intune**, a propojení celé téhle parády s **ABM** (**Apple Business Manager**).