

## 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)

Home > Domains > itheroes.cz Enable Dark mode

### itheroes.cz

Managed at Cloudflare - Default domain

Remove domain Refresh

Overview **DNS records** Users Teams & groups Apps

To manage DNS records for itheroes.cz, go to your DNS hosting provider: [Cloudflare](#).

Connect your services to your domain by adding these DNS records at your domain registrar or DNS hosting provider. Select a record to see all of its details and 'copy and paste' the expected values to your registrar. [Learn more about DNS and record types](#).

Check health **Manage DNS** Download CSV file Download zone file Print Search records

#### Microsoft Exchange

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

## DomainKeys Identified Mail (DKIM)

 It can take up to 48 hours to create DKIM records.

DKIM helps stop attackers from sending email with a forged sender address in every outbound message header. DKIM requires the following DNS records:

Type	Host name
CNAME	selector1._domainkey
CNAME	selector2._domainkey

Poté co máte tyto věci nastavené, tak si vygenerujte DMARC pomocí [easydmarc](#), nebo [Dmarcian](#) (nebo dalších služeb). DMARC vypadá přibližně takto:

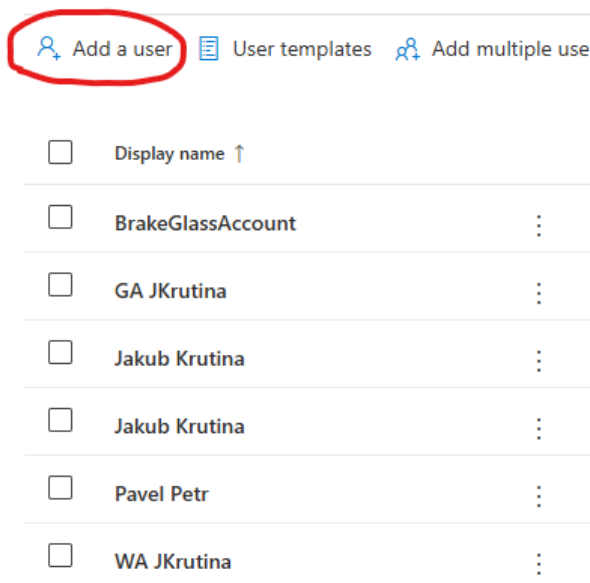
```
v=DMARC1;p=quarantine;sp=quarantine;pct=100;rua=mailto:example@example.eu;ruf=mailto:example@example.eu;ri=86400;aspf=s;adkim=s;fo=1;
```

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 ujistíte, 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)

### Active users



Add a user  User templates  Add multiple users

<input type="checkbox"/>	Display name ↑	
<input type="checkbox"/>	BrakeGlassAccount	⋮
<input type="checkbox"/>	GA JKrutina	⋮
<input type="checkbox"/>	Jakub Krutina	⋮
<input type="checkbox"/>	Jakub Krutina	⋮
<input type="checkbox"/>	Pavel Petr	⋮
<input type="checkbox"/>	WA JKrutina	⋮

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

## Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name	Last name
<input type="text" value="Jan"/>	<input type="text" value="Novák"/>
Display name *	
<input type="text" value="Jan Novák"/>	
Username *	Domains
<input type="text" value="novak"/>	@ <input type="text" value="itheroes.cz"/>

- Automatically create a password
- Require this user to change their password when they first sign in

## Přidejte licenci

### Add a user

- Basics
- Product licenses**
- Optional settings
- Finish

## Assign product licenses

Assign the licenses you'd like this user to have.

Select location \*

Licenses (1) \*


- Assign user a product license
  - Microsoft 365 Business Premium  
25 of 25 licenses available
  - Office 365 E5 EEA (no Teams)  
22 of 25 licenses available
- Create user without product license (not recommended)  
They may have limited or no access to Microsoft 365 until you assign a product license.


Apps (62)

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

## Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles (User: no administration access) 

Profile info 

Job title

Department

Office

Office phone  Fax number

Mobile phone

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.

## Jan Novák added to active users

Jan Novák will now appear in your list of active users.

### User details

 Print

Display name: Jan Novák

Username: novak@itheroes.cz

Password: \*\*\*\*\* 

### Licenses bought

None


### Licenses assigned

Office 365 E5 EEA (no Teams)

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

## Set up the basics

To get started, fill out some basic information about who you're adding as a user.

<b>First name</b>	<b>Last name</b>
<input type="text" value="Admin"/>	<input type="text" value="Admin"/>
<b>Display name *</b>	
<input type="text" value="Admin Admin"/>	
<b>Username *</b>	<b>Domains</b>
<input type="text" value="administrator"/>	@ <input type="text" value="M365ICTG001.onmicrosoft.com"/> 

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

- Basics
- Product licenses**
- Optional settings
- Finish

## Assign product licenses

Assign the licenses you'd like this user to have.

**Select location \***

**Licenses (0) \***

- Assign user a product license
  - Microsoft 365 Business Premium**  
25 of 25 licenses available
  - Office 365 E5 EEA (no Teams)**  
22 of 25 licenses available
  - Create user without product license (not recommended)**  
They may have limited or no access to Microsoft 365 until you assign a product license.

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!

- Basics
- Product licenses
- Optional settings**
- Finish

### Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

#### Roles

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

[Learn more about admin roles](#)

User (no admin center access)

**Admin center access**

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

Exchange Administrator ⓘ

Global Administrator ⓘ

Global Reader ⓘ

Helpdesk Administrator ⓘ

Service Support Administrator ⓘ

## 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 doporučené <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.

The screenshot shows the Microsoft 365 Groups Overview page. The 'New group' button is highlighted with a red box. The page displays the following information:

- Overview:** Overview, Tutorials
- Search:** Search your tenant
- Basic information:**

Total groups	15	Dynamic groups	4
M365 groups	4	Cloud groups	15
Security groups	11	On-premises groups	0
- Alerts:** Alerts
- Feature highlights:**
  - Access reviews:** Make sure only the right people have continued access.
  - Conditional Access:** Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

The screenshot shows the Microsoft 365 Groups 'New Group' creation page. The page displays the following information:

- Group type \*:** Security
- Group name \*:** ICTG\_G\_SEC\_ADMINS
- Group description:** Enter a description for the group
- Microsoft Entra roles can be assigned to the group:** Yes (selected), No
- Membership type \*:** Assigned
- Owners:** No owners selected
- Members:** No members selected

Got feedback?

Group type \*

Group name \*

Group description

Microsoft Entra roles can be assigned to the group

Membership type

Owners

Members

Try changing or adding filters if you don't see what you're looking for.

Search

120 results found

All Users Groups Devices Enterprise applications

	Name	Type	Details
<input type="checkbox"/>	AAD Terms Of Use	Enterprise ap...	d52792f4-ba38-424d-8140-ada5b883f293
<input type="checkbox"/>	All Users	Group	
<input checked="" type="checkbox"/>	BrakeGlassAccount	User	BGAccount@M365ICTG001.onmicrosoft.co...
<input type="checkbox"/>	ER88CN340KCX	Device	e971c858-203d-4594-9f99-bb9a2d1a5b5c
<input type="checkbox"/>	AADReporting	Enterprise ap...	1b912ec3-a9dd-4c4d-a53e-76aa7adb28d7
<input type="checkbox"/>	Group Creators	Group	
<input checked="" type="checkbox"/>	GA JKrutina	User	ga.jkrutina@M365ICTG001.onmicrosoft.co...
<input type="checkbox"/>	VM_W11	Device	d779eeca-ce99-4a5f-9b41-c3abf520507e
<input type="checkbox"/>	Azure AD Notification	Enterprise ap...	fc03f97a-9db0-4627-a216-ec98ce54e018

Selected (3)  
Reset

- BrakeGlassAccount  
BGAccount@M365ICTG001.onmicrosoft.c...
- GA JKrutina  
ga.jkrutina@M365ICTG001.onmicrosoft.com
- WA JKrutina  
wajkrutina@M365ICTG001.onmicrosoft.co...

## New Group ...

Got feedback?

Group type \*

Group name \*

Group description

Microsoft Entra roles can be assigned to the group

Membership type \*


Owners  
1 owner selected

Members  
3 members selected

Teď si vytvoříme dynamickou skupinu pro HP zařízení.



## 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**

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
<input type="checkbox"/>	deviceManufacturer	Equals	HP

+ Add expression

**Rule syntax**

```
(device.deviceManufacturer -eq "HP")
```

Edit

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 neadministrátoři 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 zavírovaný.

Home > M365-ICTG001 | Users > Users

## Users | User settings

M365-ICTG001

Refresh | Got feedback?

- All users
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Deleted users
- Password reset
- User settings**
- Bulk operation results
- New support request

### Default user role permissions

[Learn more](#)

- Users can register applications  No
- Restrict non-admin users from creating tenants  Yes
- Users can create security groups  No

### Guest user access

[Learn more](#)

- Guest user access restrictions  Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

### Administration center

[Learn more](#)

- Restrict access to Microsoft Entra admin center  Yes

### LinkedIn account connections

[Learn more](#)

- Allow users to connect their work or school account with LinkedIn  Yes
- Selected group
- No

### Show keep user signed in

- Show keep user signed in  No

## [ICT] GROUP

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

[Groups - Microsoft Azure](#)

### Groups | General

M365-ICTG001

Save Discard | Got feedback?

- Overview
- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
  - General**
  - Expiration
  - Naming policy
- Activity
- Troubleshooting + Support

#### Self Service Group Management

Owners can manage group membership requests in My Groups  Yes  No

Restrict user ability to access groups features in My Groups. Group and User Admin will have read-only access when the value of this setting is 'Yes'.  Yes  No

**i** Restrict user ability to access groups features in My Groups' setting - original planned for June 2024 - deferred. New date will be shared later this year. [Learn more](#)

#### Security Groups

Users can create security groups in Azure portals, API or PowerShell  Yes  No

#### Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell  Yes  No

## [ICT] GROUP

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](#)

[Home](#) > [M365-ICTG001 | Groups](#) > [Groups](#)



## Groups | Expiration

M365-ICTG001



Save



Discard



Got feedback?



Overview



All groups



Deleted groups



Diagnose and solve problems



Settings



General



Expiration



Naming policy



Activity



Troubleshooting + Support

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration for Outlook, SharePoint, Teams, and Power BI.

Group lifetime (in days) \* ⓘ

365



Email contact for groups with no owners

\* ⓘ

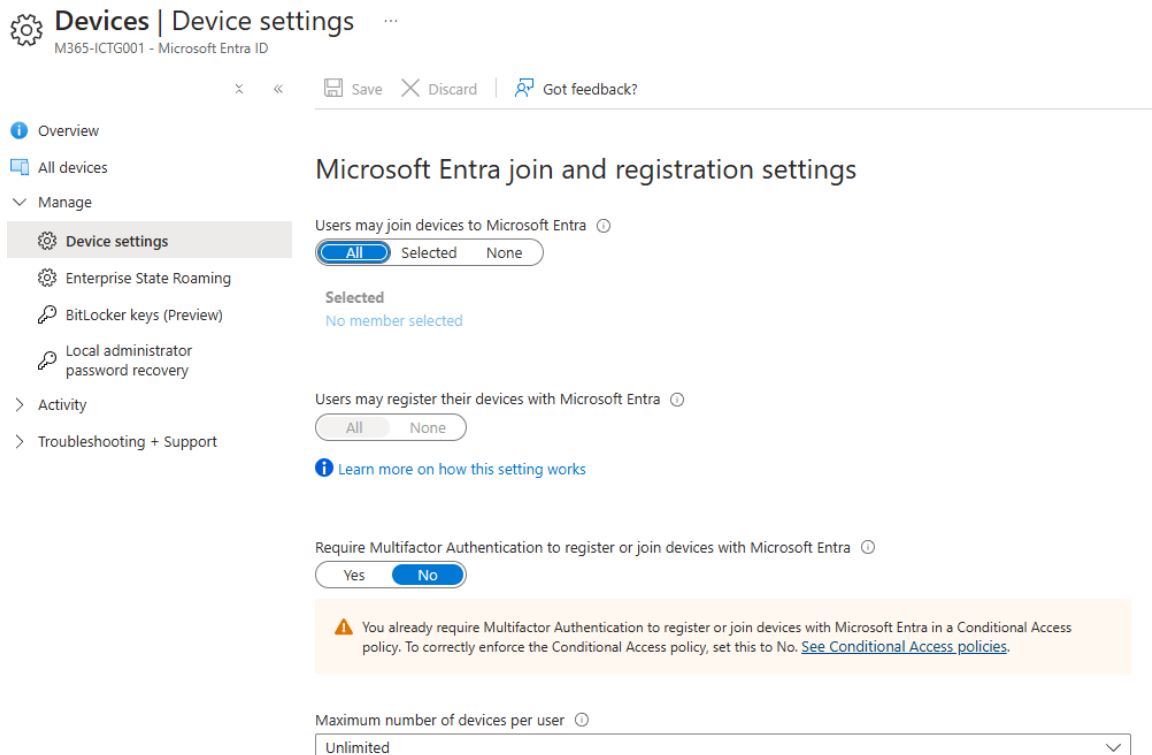
Enable expiration for these Microsoft 365 groups ⓘ

All

Selected

None

**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 vypnete. Do počítačů se jako administrátoři dostanete přes workstation admin účty.



The screenshot shows the Microsoft Entra ID console interface for 'Device settings'. The left-hand navigation pane includes 'Overview', 'All devices', and a 'Manage' section with 'Device settings' (selected), 'Enterprise State Roaming', 'BitLocker keys (Preview)', and 'Local administrator password recovery'. The main content area is titled 'Microsoft Entra join and registration settings'. It contains three settings: 1) 'Users may join devices to Microsoft Entra' with a radio button set to 'All' (Selected), and a note 'No member selected'. 2) 'Users may register their devices with Microsoft Entra' with a radio button set to 'None'. 3) 'Require Multifactor Authentication to register or join devices with Microsoft Entra' with a radio button set to 'No'. Below this is a warning message: 'You already require Multifactor Authentication to register or join devices with Microsoft Entra in a Conditional Access policy. To correctly enforce the Conditional Access policy, set this to No. See Conditional Access policies.' At the bottom, there is a dropdown menu for 'Maximum number of devices per user' set to 'Unlimited'.

## Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

Yes  No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

All Selected  None

Selected  
No member selected

[Manage Additional local administrators on all Microsoft Entra joined devices](#)

Enable Microsoft Entra Local Administrator Password Solution (LAPS) ⓘ

Yes  No

## Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices ⓘ

Yes  No

## 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/](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.

Passkeys are a phishing-resistant, standards-based passwordless authentication method :  
Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target **Configure**

### GENERAL

Allow self-service set up  Yes  No

Enforce attestation  Yes  No

### KEY RESTRICTION POLICY

Enforce key restrictions  Yes  No

Restrict specific keys  Allow  Block

Microsoft Authenticator ⓘ

Add AAGUID

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/](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_/PasswordProtection/fromNav/)

The screenshot shows the 'Authentication methods | Password protection' configuration page in Microsoft Entra ID. The page is titled 'M365-ICTG001 - Microsoft Entra ID Security'. On the left, there is a navigation pane with sections 'Manage' and 'Monitoring'. Under 'Manage', 'Password protection' is selected. The main content area shows the following settings:

- Custom smart lockout:**
  - Lockout threshold: 10
  - Lockout duration in seconds: 60
- Custom banned passwords:**
  - Enforce custom list: Yes
  - Custom banned password list: bonemia, Praha2024, Brno2024, CZ2024, CZ1234, Heslo1123, HesloCZ2024, SlovoCZ
- Password protection for Windows Server Active Directory:**
  - Enable password protection on Windows Server Active Directory: Yes
  - Mode: Enforced

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/](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_/AuthStrengths/fromNav/)



## Manage

Policies

Password protection

Registration campaign

Authentication strengths

Settings

## Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

Authentication strengths determine the combination of authentication methods that can be used.

[Learn more](#)

Type: All Authentication methods: All Reset filters

Authentication strength	Type	Authentication methods	Condi
<a href="#">TAP Device Registration</a>	Custom	Temporary Access Pass (One-time use)	007 R
<a href="#">Multifactor authentication</a>	Built-in	Windows Hello For Business / Platform Credential ...	Not c
<a href="#">Passwordless MFA</a>	Built-in	Windows Hello For Business / Platform Credential ...	Not c
<a href="#">Phishing-resistant MFA</a>	Built-in	Windows Hello For Business / Platform Credential ...	Not c

## New authentication strength

Custom

Configure Review

Name \*

Description

Search authentication combinations

- Phishing-resistant MFA (3)
  - Windows Hello For Business / Platform Credential
  - Passkeys (FIDO2) [Advanced options](#)
  - Certificate-based Authentication (Multifactor) [Advanced options](#)
- Passwordless MFA (1)
  - Microsoft Authenticator (Phone Sign-in)
- Multifactor authentication (13)
  - Temporary Access Pass (One-time use)**
  - Temporary Access Pass (Multi-use)
  - Password + Microsoft Authenticator (Push Notification)
  - Password + Software OATH token
  - Password + Hardware OATH token
  - Password + SMS
  - Password + Voice

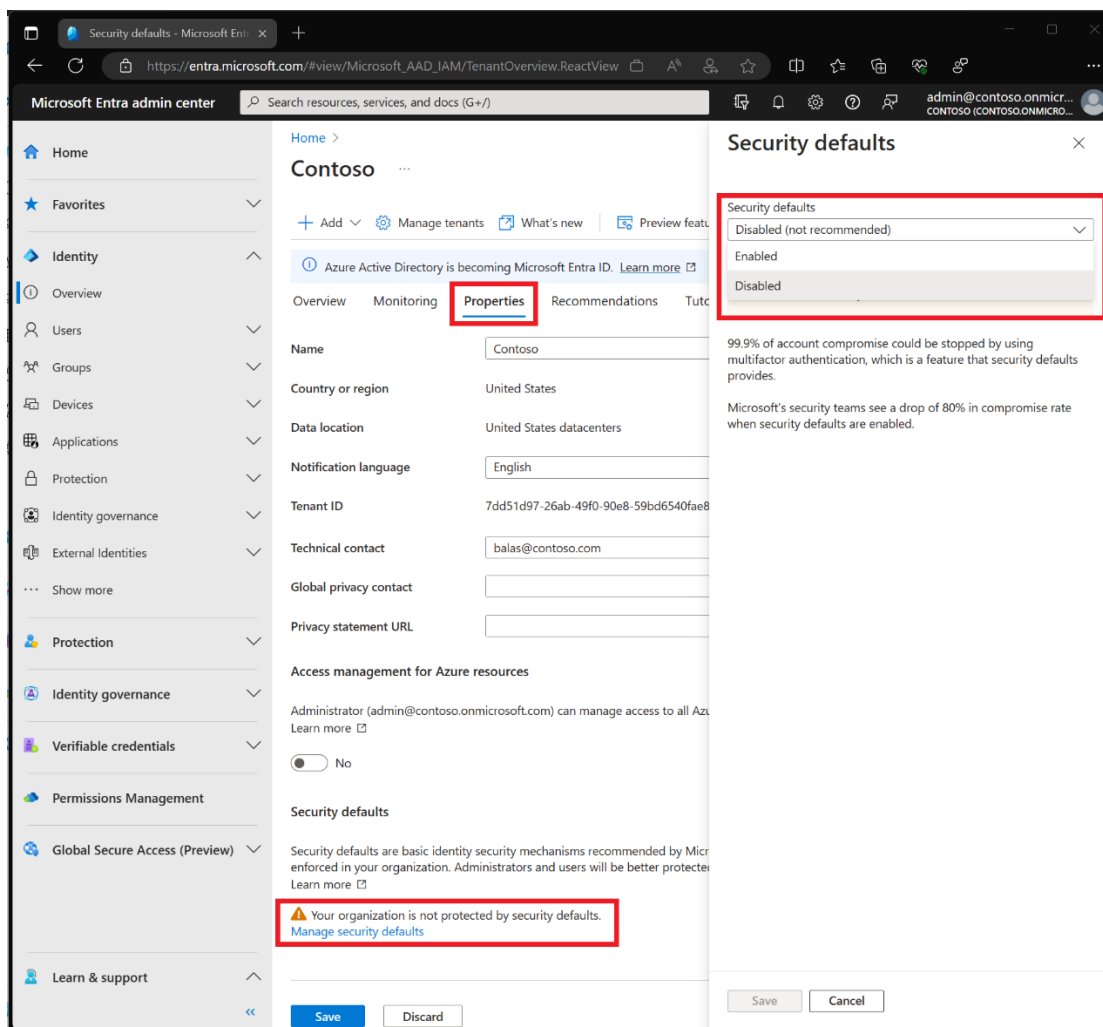
Samozřejmě můžete použít i multi-use TAP (Temporary Access Pass). Potom stačí jenom dát vytvořit a máte hotovo!

## Conditional Access Policies!

**Conditional Access 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.

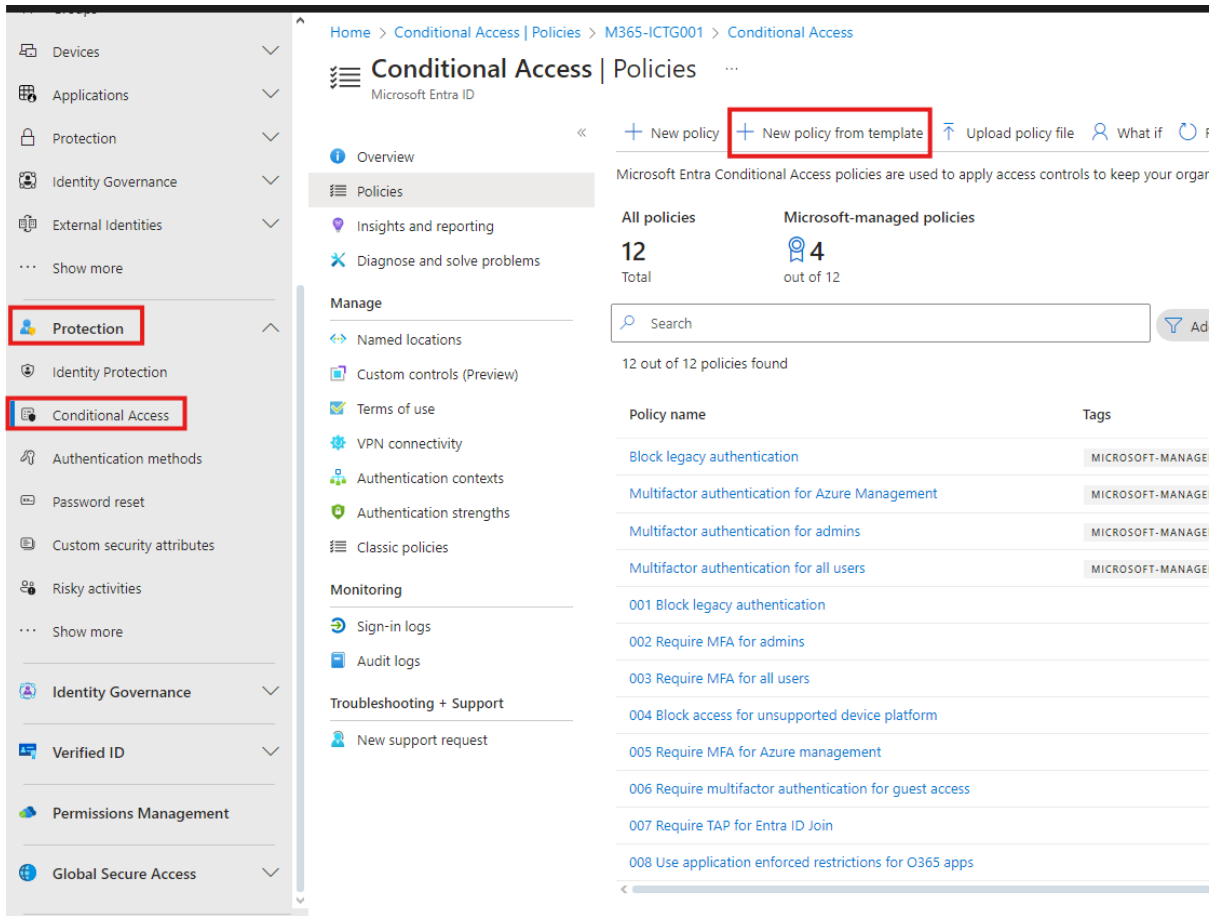
[https://entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/TenantOverview.ReactView/initialValue//tabId//recommendationResourceId//fromNav/Identity](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView/initialValue//tabId//recommendationResourceId//fromNav/Identity)



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

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



### Create new policy from templates

Select a template [Review + Create](#)

Search

[Secure foundation](#) [Zero Trust](#) [Remote work](#) [Protect administrator](#) [Emerging threats](#) [All](#)

<input checked="" type="radio"/> <b>Require multifactor authentication for admins</b> Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>	<input type="radio"/> <b>Securing security info registration</b> Secure when and how users register for Azure AD multifactor authentication and self-service password reset. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>	<input type="radio"/> <b>Block legacy authentication</b> Block legacy authentication endpoints that can be used to bypass multifactor authentication. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>
<input type="radio"/> <b>Require multifactor authentication for all users</b> Require multifactor authentication for all user accounts to reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>	<input type="radio"/> <b>Require multifactor authentication for Azure management</b> Require multifactor authentication to protect privileged access to Azure management. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>	<input type="radio"/> <b>Require compliant or hybrid Azure AD joined device or multifactor authentication for all users</b> Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>
<input type="radio"/> <b>Require MDM-enrolled and compliant device to access cloud apps for all users (Preview)</b> Require devices to be enrolled in mobile device management (MDM) and be compliant for all users and devices accessing company resources. This improves data security by reducing risk of breaches, malware, and unauthorized access. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks. <a href="#">Learn more</a> <a href="#">View</a> <a href="#">Download JSON file</a>		

[Review + create](#)

[< Previous](#)

[Next: Review + Create >](#)

Ze začátku 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.

Home > Conditional Access | Policies > M365-ICTG001 > Conditional Access | Policies >

### Create new policy from templates

Select a template **Review + Create**

**Basics**

Policy name \*

Policy state

Off

On

Report only

Template name

Require multifactor authentication for admins

**Assignments**

**Users and groups**

Excluded users

Included roles

**Create**

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!

Delete View policy information

### Assignments

Users

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network

Not configured

Conditions

0 conditions selected

### Access controls

Grant

1 control selected

Session

0 controls selected

Enable policy

Report-only On Off

### Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

Consider testing the new "Require authentication strength". [Learn more](#)

Require authentication strength

"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require device to be marked as compliant

Require Microsoft Entra hybrid joined device

Require approved client app

[See list of approved client apps](#)

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

Create new policy from templates

Select a template Review + Create

Search

Secure foundation Zero Trust Remote work Protect administrator Emerging threats All

Require multifactor authentication for admins

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults. [Learn more](#)

View Download JSON file

Securing security info registration

Secure when and how users register for Azure AD multifactor authentication and self-service password reset. [Learn more](#)

View Download JSON file

Block legacy authentication

Block legacy authentication endpoints that can be used to bypass multifactor authentication. [Learn more](#)

View Download JSON file

Require multifactor authentication for all users

Require multifactor authentication for all user accounts to reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks. [Learn more](#)

View Download JSON file

Require multifactor authentication for Azure management

Require multifactor authentication to protect privileged access to Azure management. [Learn more](#)

View Download JSON file

Require compliant or hybrid Azure AD joined device or multifactor authentication for all users

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks. [Learn more](#)

View Download JSON file

Require MDM-enrolled and compliant device to access cloud apps for all users (Preview)

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**.

## 001 Block legacy authentication

Conditional Access policy

[Delete](#) [View policy information](#)

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

Name \*  
001 Block legacy authentication

Assignments

Users

All users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network **NEW**

Not configured

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

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

Device platforms

Not configured

Locations

Not configured

Client apps

2 included

Filter for devices

Not configured

Authentication flows

Not configured

Enable policy

[Report-only](#) On Off[Save](#)

Control user access to target specific applications not using modern authentication. [Learn more](#)

Configure  Yes  No

Select the client apps this policy will apply to

Modern authentication clients

 Browser Mobile apps and desktop clients

Legacy authentication clients

 Exchange ActiveSync clients Other clients[Done](#)

## 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 kreativě 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](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AddGroupBlade)

Home > Conditional Access | Policies > Groups | All groups >

## New Group

Got feedback?

Group type \* ⓘ  
Security

Group name \* ⓘ  
ICTG\_G\_SEC\_USR\_MFA

Group description ⓘ  
Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ  
Yes No

Membership type \* ⓘ  
Assigned

Owners  
No owners selected

Members  
No members selected

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

## Create new policy from templates

Select a template Review + Create

Search

Secure foundation Zero Trust Remote work Protect administrator Emerging threats All

- Require multifactor authentication for admins  
Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.  
[Learn more](#)
- Securing security info registration  
Secure when and how users register for Azure AD multifactor authentication and self-service password reset.  
[Learn more](#)
- Require multifactor authentication for all users**  
Require multifactor authentication for all user accounts to reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.  
[Learn more](#)
- Require multifactor authentication for Azure management  
Require multifactor authentication to protect privileged access to Azure management.  
[Learn more](#)

View Download JSON file

## Create new policy from templates ...

Select a template Review + Create

### Basics

Policy name \*

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 >



Ted 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!

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

Name \*  
ICTG\_CA\_03\_Require\_MFA\_for\_users

Assignments

Users

Specific users included and specific users excluded

"Select users and groups" must be configured

Target resources

All resources (formerly 'All cloud apps')

Network **NEW**

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Enable policy

**Report-only** On Off

Control access based on v apply to, such as users and identities, directory roles, [Learn more](#)

Include Exclude

None

All users

Select users and groups

Guest or external users

Directory roles

Users and groups

Select

0 users and groups selected

Select at least one user or group

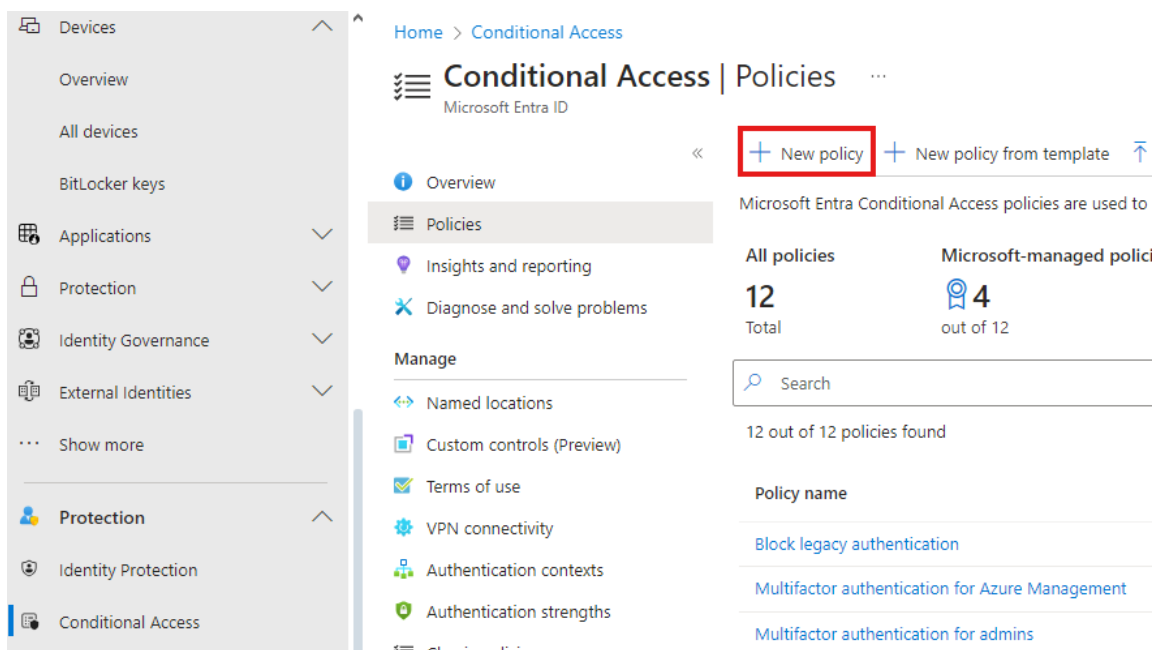
Search

25 results found

All Users Groups

	Name	Type
<input type="checkbox"/>	Pavel Petr	User
<input type="checkbox"/>	ICTG_G_SEC_DEV_Company	Group
<input type="checkbox"/>	WA JKrutina	User
<input type="checkbox"/>	ICTG_G_SEC_DEV_HPDEVICE	Group
<input type="checkbox"/>	ICTG_G_SEC_EXC_CAP	Group
<input type="checkbox"/>	ICTG_G_SEC_EXC_DEV_AUTOPILOT	Group
<input type="checkbox"/>	ICTG_G_SEC_USR_BrakeGlassAcc...	Group
<input checked="" type="checkbox"/>	ICTG_G_SEC_USR_MFA	Group
<input type="checkbox"/>	ICTG_G_SEC_USR_WORKSTATION...	Group
<input type="checkbox"/>	ICTG_SEC_USR_UPD_RING1	Group

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.



Home > Conditional Access

### Conditional Access | Policies

Microsoft Entra ID

**+ New policy** + New policy from template

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication contexts
- Authentication strengths
- Classic policies

All policies: 12 Total

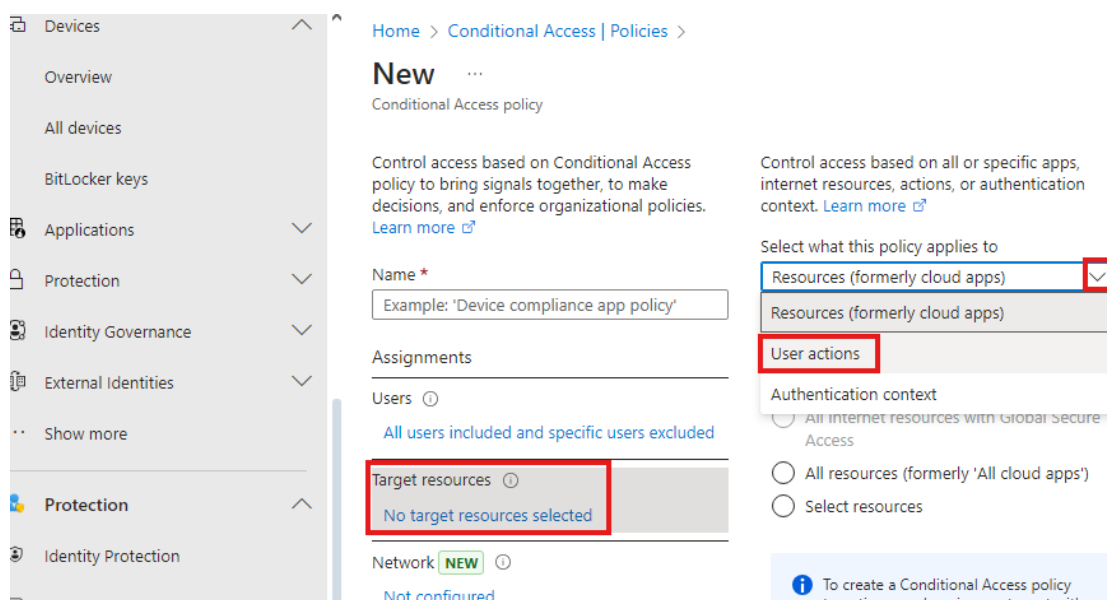
Microsoft-managed policies: 4 out of 12

Search: 12 out of 12 policies found

Policy name

- Block legacy authentication
- Multifactor authentication for Azure Management
- Multifactor authentication for admins

Začlíme 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**.



Home > Conditional Access | Policies >

### New

Conditional Access policy

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

Name \*

Example: 'Device compliance app policy'

Assignments

Users

All users included and specific users excluded

Target resources

No target resources selected

Network **NEW**

Not configured

Control access based on all or specific apps, internet resources, actions, or authentication context. [Learn more](#)

Select what this policy applies to

- Resources (formerly cloud apps)
- Resources (formerly cloud apps)
- User actions
- Authentication context

All internet resources with Global Secure Access

All resources (formerly 'All cloud apps')

Select resources

To create a Conditional Access policy, register a member in your tenant with...

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.