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)

≡			Home > Domains > itheroes.cz <) Enable Dark mode				
æ	Resources	\sim	itheroes.cz					
Ô	Marketplace		Managed at Cloudflare - Default domain					
	Billing	^	💼 Remove domain 🔿 Refresh					
	Your products Licenses		Overview DNS records Users Teams & groups Apps					
	Bills & payments Billing accounts		To manage DNS records for itheroes.cz, go to your DNS hosting provider: Cloudflare. 🧷					
	Payment methods Billing notifications		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.					
្ច	Support	\sim						
1	Settings	^	💝 Check health 🚳 Manage DNS 🛓 Download CSV file 🞍 Download zone file 🔒 Print 🔎 Search records	=				
	Domains							
	Search & intelligence							
	Org settings		Microsoft Exchange					
	Microsoft 365 Backup							

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!

Туре	Host name	Point to address or value	TTL
MX	@	0 itheroes-cz.mail.protection.outlook.com	1 Hour
ТХТ	@	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)
 i It can take up to 48 hours to create DKIM res
 DKIM helps stop attackers from sending em every outbound message header. DKIM nee
 Type Host name
 CNAME selector1._domainkey
 CNAME selector2. domainkey

Poté co máte tyto věci nastavené, tak si vygenerujte DMARC pomocí <u>easydmarc</u>, nebo <u>Dmarcian</u> (nebo dalších služeb). DMARC vypadá přibližně takto:

v=DMARC1;p=quarantine;sp=quarantine;pct=100;rua=mailto:example@example.e u;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 <u>Active users - Microsoft 365</u> <u>admin center</u> a klikněte na **Add a user** (Přidat uživatele)

Active users



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
Jan	Novák
Display name *	
Jan Novák	
Username *	Domains
novak	(a) itheroes.cz
Automatically create a password Require this user to change their password	ord when they first sign in

Přidejte licenci

Add a user

Basics	Assign product licenses
Product licenses	Assign the licenses you'd like this user to have.
Optional settings	
O Finish	Select location * Czech Republic
	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 sekcí **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)	\checkmark			
Profile info	\frown			
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.



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.

First name	Last name					
Admin	Admin					
Display name *						
Admin Admin						
Username *	Domains					
administrator	M365ICTG001.onmicrosoft.com					

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

0	Basics	Assign product licenses
	Product licenses	Assign the licenses you'd like this user to have.
0	Optional settings	
0	Finish	Select location * Czech Republic ✓
		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!

0	Basics	Optional settings
	Product licenses	You can choose what role you'd like to assign for this user, and fill in additional profile information.
	Optional settings	
0	Finish	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 (i)
		Global Reader ()
		Helpdesk Administrator ()
		Service Support Administrator (i)

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 <u>https://entra.microsoft.com/</u>.

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.



𝔅 ² Got feedback?	① Try changing or adding filters if you don't see what you're looking for.					Selected (3)		
roup type * ① Search ①								
Security						BrakeGlassAccount	Û	
Group name * 🕕	120 results four	nd				BGAccount@M365ICTG001.onmicrosoft.c		
ICTG_G_SEC_ADMINS	All Users	Groups Devices Enterprise	applications		2	GA JKrutina ga.jkrutina@M365ICTG001.onmicrosoft.com	Û	
Sroup description ①		Name	Type	Details				
Enter a description for the group						WA JKrutina	Û	
Microsoft Entra roles can be assigned to the group ③		AAD Terms Of Use	Enterprise ap	d52792f4-ba38-424d-8140-ada5b883f293		wajkrutina@M505iC10001.onmicrosoft.co		
Yes No								
Membership type ①	🗆 🎦	All Users	Group					
Assigned								
Dumorr	i 🗹 📈	BrakeGlassAccount	User	BGAccount@M365ICTG001.onmicrosoft.cor				
No owners salected								
No owners selected		ERB8CN3340KCX	Device	e971c858-203d-4594-9199-bb9a2d1a5b5c				
Members		4400	Fatancias an					
No members selected		AADReporting	Enterprise ap	10912ec3-a9dd-404d-a53e-76aa7adb28d7				
		Group Creators	Group					
		GA JKrutina	User	ga.jkrutina@M365ICTG001.onmicrosoft.com				
		VM_W11	Device	d7f9eeca-ce99-4a5f-9b41-c3abf520507e				
		Azure AD Notification	Enterprise ap	fc03f97a-9db0-4627-a216-ec98ce54e018				

New Group



Teď si vytvoříme dynamickou skupinu pro HP zařízení.

New Group Sot feedback? Group type * 🕕 Security \sim Group name * (i) ICTG_G_SEC_DEV_HPDEVICE \checkmark Group description ① Enter a description for the group Microsoft Entra roles can be assigned to the group ① 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 ①	
Enter a description for the group	
Yes No Membership type * ①	
Dynamic Device	\sim
Owners	
No owners selected	
Dynamic device members * ①	
Add dynamic query	



🖫 Save 🗙 Dis	a Save X Discard R Got feedback?							
Configure Rules	Configure Rules Validate Rules							
You can use the rul	ule build	er or rule syntax text box to create or edit a dynamic membership rule.	Learn more					
And/Or	<u>ا</u>	Property		Operator		Value		
]	deviceManufacturer	~	Equals	~	HP		Î
+ Add expression	n							
Rule syntax								🖉 Edit
(device.deviceManufacturer -eq "HP")								

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. <u>Users - Microsoft Azure</u>

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 přistup 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.



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

ŝ	Groups General		
	0	«	🖫 Save 🗙 Discard 🛛 🖗 Got feedback?
0	Overview		Self Service Group Management
24	All groups		Owners can manage group membership Yes No
24	Deleted groups		
×	Diagnose and solve problems		Restrict user ability to access groups features in My Groups. Group and User
\sim	Settings		Admin will have read-only access when the value of this setting is 'Yes'. ①
	 General 		
	🖏 Expiration		Restrict user shilling to access groups features in My Groups' setting - origina
	🔅 Naming policy		planned for June 2024 - deferred. New date will be shared later this year. Lea
>	Activity		
>	Troubleshooting + Support		Security Groups
			Users can create security groups in Azure Yes No portals, API or PowerShell
			Microsoft 365 Groups
			Users can create Microsoft 365 groups in Yes No Azure portals, API or PowerShell

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 > Gro	ups	
Groups Expiration		
≎ «	🖫 Save 🗙 Discard 🛛 🛜 Got feed	lback?
() Overview	Renewal notifications are emailed to group	owners 30 days, 15 days, and one day prior to gro
🚨 All groups	Outlook, SharePoint, Teams, and Power Bl.	
🏝 Deleted groups	Group lifetime (in days) * 🕕	365 🗸
🗙 Diagnose and solve problems	Email contact for groups with no owners	jakub.krutina@itheroes.cz
✓ Settings	* (i)	
l General	Enable expiration for these Microsoft 365	All Selected None
🐼 Expiration	groups ()	
🐯 Naming policy		
> Activity		

> Troubleshooting + Support

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.



Local administrator settings



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/AuthenticationMethodsMenuBl ade/~/AdminAuthMethods/fromNav/

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

Method	Target	Enabled
\checkmark 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 a 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 POI	LICY		
Enforce key restriction	IS	Yes	No
Restrict specific keys		Allow	Block
✓ Microsoft Auther	ticator 🛈		
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/AuthenticationMethodsMenuBl ade/~/PasswordProtection/fromNav/

Manage			
	Custom smart lockout		
Policies	Lockout threshold 🕕	10	
Password protection	Lockout duration in seconds	60	
Registration campaign	Lockour duration in Seconds ()		
	Custom banned passwords		
Authentication strengths	Enforce custom list 🛈	Yes	No
🔅 Settings			
	Custom banned password list 🕕	Praha2024	^
Monitoring		Brno2024	
Activity		CZ2024	
Activity		CZ1234	
User registration details		HesloC72024	
Registration and reset events		SlovoCZ	~
Bulk operation results	Password protection for Windows Serve	er Active Directory	
	Enable password protection on Windows Server Active Directory ①	Yes	No
	Mode 🕡	Enforced	Audit

Authentication methods | Password protection * ···

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 <u>https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBl</u> <u>ade/~/AuthStrengths/fromNav/</u>

Home > Authentication methods					New authentication strength
Authentication met M365-ICTG001 - Microsoft Entra ID Sec	hods Authentication	strengths			Custom
	+ New authentication strength	🕐 Refresh			Configure Review
Manage	Authentication strengths determine	the combination of a	uthentication methods that can be used.		Name *
Policies	Learn more 🛛				Name your authentication strength
Password protection	Type: All Authentication met	hods: All 🛛 🛣 Rese	t filters		Description
📙 Registration campaign					Add a description for your authentication strength
Q Authentication strengths	Authentication strength	Туре	Authentication methods	Condi	
🚸 Settings	TAP Device Registration	Custom	Temporary Access Pass (One-time use)	007 R/	Search authentication combinations
Monitoring	Multifactor authentication	Built-in	Windows Hello For Business / Platform Credential	Not co	
ni Activity	Passwordless MFA	Built-in	Windows Hello For Business / Platform Credential	Not co	Phishing-resistant MFA (3)
User registration details					Windows Hello For Business / Platform Credential
Registration and reset events	Phishing-resistant MFA	Built-in	Windows Hello For Business / Platform Credential	Not co	Passkeys (FIDO2) Advanced options
👶 Bulk operation results					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
					Daceword + Voice

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

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/init ialValue//tabld//recommendationResourceId//fromNav/Identity

	Security defaults - Microsoft Er	atr × +	- o x
÷	C 🗅 https://entra.mic	rrosoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView 📋 A [®]	
м	icrosoft Entra admin center	$\mathcal P$ Search resources, services, and docs (G+/)	日 口 恋 ⑦ 戸 admin@contoso.onmicr 🌑
^	Home	Home >	Security defaults \times
_		Contoso	
*	Favorites	→ → Add → ② Manage tenants ② What's new 🕞 Preview fe	Security defaults atu Disabled (not recommended)
4	Identity	Azure Active Directory is becoming Microsoft Entra ID. Learn more	Enabled
()	Overview	Overview Monitoring Properties Recommendations Tu	Disabled .
8	Users	Name Contoso	99.9% of account compromise could be stopped by using
^**	Groups		 multifactor authentication, which is a feature that security defaults provides.
圮	Devices	Country or region United States	Microsoft's security teams see a drop of 80% in compromise rate
₿,	Applications	Data location United States datacenters	when security defaults are enabled.
A	Protection	V Notification language English	
۲	Identity governance	Tenant ID 7dd51d97-26ab-49f0-90e8-59bd6540fa	168
ල්ල	External Identities	V Technical contact balas@contoso.com	
	Show more	Global privacy contact	_
4	Protection	Privacy statement URL	
-		Access management for Azure resources	
۵	Identity governance	Administrator (admin@contoso.onmicrosoft.com) can manage access to all A	Azı
	Verifiable credentials	Learn more 🛛	
-		No No	
	Permissions Management	Security defaults	
3	Global Secure Access (Preview)	 Security defaults are basic identity security mechanisms recommended by M enforced in your organization. Administrators and users will be better protect Learn more ID 	licr tte
		A Your organization is not protected by security defaults. Manage security defaults	
2	Learn & support	<u>^</u>	
		< Save Discard	Save

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.



Create new policy from templates

Search	t 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 [3]	Securing security info registration Secure when and how users register for Azure AD multifactor authentication and self-service password reset. Learn more ID	O Block legacy authentication Block legacy authentication endpoints that can be used to bypass multifactor authentication. Learn more ☑
O View	⑦ View ↓ Download JSON file	⑦ 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 ② View	 ○ Require multifactor authentication for Azure management Require multifactor authentication to protect privileged access to Azure management. Learn more C ○ 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 C view Download JSON file
Require MDM-enrolled and compliant device to access cloud apps for all users (Preview) 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 risks of breaches, mahures, and upputtherized access. Directory		

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.

品	Devices	\sim	Home > Conditiona	I Access Pol	icies > M365-ICTG001 > Conditional Access Policies >
_			Create new	policy f	rom templates
щ	Applications	\sim			
≙	Protection	\sim	Select a template	Review + C	reate
٢	Identity Governance	\sim			
Q	External Identities	\sim	Basics		
	Show more		Policy name *		ICTG_CA_01_Require_MFA_for_Admins
4	Protection	^	Policy state		O off
٢	Identity Protection				O on
R	Conditional Access				Report only
47	Authentication methods		Template name		
	Password reset		Require multifacto	r authenticatic	n for admins
Ð	Custom security attributes				
ĉ	Risky activities		Assignments		
	Show more		Users and group	s	
٨	Identity Governance	\sim	Excluded users		Current user
5	Verified ID	\sim	Included roles		Global Administrator
<	Permissions Management				Security Administrator
(Global Secure Access	~			SharePoint Administrator
_					Exchange Administrator
2	Learn & support	^			
		~	Create		< Previous Next >

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.**

Create new policy from templates



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 authentic	ation …	
Delete O View policy information		Control user access to target specific cl applications not using modern authentication. Learn more
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.	Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more 🖻	Configure ① Yes No
Learn more of	Device platforms ①	Select the client apps this policy will
Name *	Not configured	apply to
001 Block legacy authentication	Locations 🕕	Modern authentication clients
Assignments	Not configured	Browser
Users ①	Client apps ①	Mobile apps and desktop clients
All users included and specific users excluded	2 included	Legacy authentication clients
Target resources (i)	Filter for devices ①	Exchange ActiveSync clients
All resources (formerly 'All cloud apps')	Not configured	✓ Other clients ①
Network NEW ①	Authentication flows (i)	_
Not configured	Not configured	
Conditions ①		
1 condition selected		
Access controls		
Grant ()		
Session 🕢		
0 controls selected		
Enable policy		
Report-only On Off		
Save		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 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

	Home	î	Home > Conditional Access Policies > Groups All groups >
	nome		New Group
-	What's new		•
×	Diagnose & solve problems		R Got feedback?
*	Favorites	\sim	Group type * ① Security
٩	Identity	^	Group name * ()
()	Overview		Group description ①
8	Users	~	Enter a description for the group
	All users		Microsoft Entra roles can be assigned to the group ① Yes No
	Deleted users		Membership type * ①
	User settings		Assigned V
የድ	Groups	^	Owners No owners selected
	Overview		
	All groups		No members selected
	Deleted groups		

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.Re actView

	All devices		Create new policy from templates	
	BitLocker keys			
₿.	Applications	\sim	Select a template Review + Create	
A	Protection	\sim	✓ Search	
:	Identity Governance	\sim	Secure foundation Zero Trust Remote work Protect	administrator Emerging threats All
ą	External Identities	\sim		
	Show more		O Require multifactor authentication for admins	O Securing security info registration
4	Protection	^	Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This	Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
۲	Identity Protection		policy will target the same roles as security defaults. Learn more 🖸	Learn more 🖸
F	Conditional Access			
43	Authentication methods		'o' View 👱 Download JSON file	'o' View
	Password reset		Require multifactor authentication for all users	Require multifactor authentication for Azure
Ð	Custom security attributes		Dequire multifactor authentication for all user accounts to	management
ĉ	Risky activities		reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory	to Azure management.
	Show more		synchronization tasks. Learn more 🖸	
۲	Identity Governance	\checkmark	Over ↓ Download JSON file	ত View 🞍 Download JSON file

Create new policy from templates

elect a template	Review + Create
Basics	
Policy name *	ICTG_CA_03_Require_MFA_for_users
Policy state	O off
	O on
	Report only
Template name	
Require multifactor a	authentication for all users
Assignments	
Users and groups	
Included users	All users
Excluded users	Current user
Excluded roles	Directory Synchronization Accounts



< 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!

Control access based on Conditional Access	Control access based on v	Searc	h			
decisions, and enforce organizational policies.	identities, directory roles,	les, 25 results found				
Learn more 🖾	Learn more 🖾	All	Users	Gro	ups	
Name *	Include Exclude	—				
ICTG_CA_03_Require_MFA_for_users				N	ame	Type
Assignments	All users			Pa	avel Petr	User
Users 🕕	Select users and grc		_			
Specific users included and specific users excluded	Guest or externa]		TG_G_SEC_DEV_Company	Group
Select users and groups" must be configured	Directory roles]	w	'A JKrutina	User
Target resources 🕡	osers and grou.		1		TG G SEC DEV HPDEVICE	Group
All resources (formerly 'All cloud apps')	Select		· 🔺			
Network NEW ①	0 users and groups se]		TG_G_SEC_EXC_CAP	Group
Not configured	Select at least one us			- A		
Conditions ①]		TG_G_SEC_EXC_DEV_AUTOPILOT	Group
0 conditions selected]	, IC	TG_G_SEC_USR_BrakeGlassAcc	Group
Access controls					TG_G_SEC_USR_MFA	Group
Grant 🛈				<u> </u>		
1 control selected]	, IC	TG_G_SEC_USR_WORKSTATION	Group
Session ①			-			
0 controls selected]		TG_SEC_USR_UPD_RING1	Group
Enable policy		_		-		
Report-only On Off		<				

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**.

9	Devices	^	^	Home > Conditional Access Policies >	
	Overview			New	
	All devices				
	BitLocker keys			Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.	Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more 2
Ð	Applications	\sim		Learn more 🖻	Select what this policy applies to
9	Protection	\sim		Name *	Resources (formerly cloud apps)
3	Identity Governance	\sim		Example: Device compliance app policy	Resources (formerly cloud apps)
~				Assignments	User actions
10	External Identities	\sim		Users (i)	Authentication context
	Show more			All users included and specific users excluded	All internet resources with Global Secure Access
_				Target resources ①	All resources (formerly 'All cloud apps')
•	Protection	^		No target resources selected	○ Select resources
٢	Identity Protection			Network NEW ①	
-	6 DC 14			Not configured	To create a Conditional Access policy



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.

Home > Conditional Access | Overview > Policies >

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.

Create new policy from templates Select a template Review + Create Search Secure foundation Zero Trust Remote work Protect administrator Emerging threats All ○ Securing security info registration O Block legacy authentication O Require multifactor authentication for admins Require multifactor authentication for privileged Secure when and how users register for Azure AD multifactor Block legacy authentication endpoints that can be used to administrative accounts to reduce risk of compromise. This authentication and self-service password reset. bypass multifactor authentication. policy will target the same roles as security defaults. Learn more 🗹 Learn more 🗹 Learn more Require multifactor authentication for Azure O Require compliant or hybrid Azure AD joined device or \bigcirc Require multifactor authentication for all users management multifactor authentication for all user Require multifactor authentication for all user accounts to Require multifactor authentication to protect privileged access Protect access to company resources by requiring users to use reduce risk of compromise. Directory Synchronization to Azure management. a managed device or perform multifactor authentication. Accounts are excluded for on-premise directory Directory Synchronization Accounts are excluded for on-Learn more 🛽 synchronization tasks. premise directory synchronization tasks. Learn more 🖸 Learn more 🗹 ⊘ View ↓ Download JSON file ⊘ View ↓ Download JSON file ○ View ↓ Download JSON file

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

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!



Show more

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**.

Create new policy from templates

Secure foundation Zero Trust Remote work Protect	t administrator Emerging threats All	
O Securing security info registration	O Block legacy authentication	O Require multifactor authentication for all users
Secure when and how users register for Azure AD multifactor authentication and self-service password reset. Learn more ID	Block legacy authentication endpoints that can be used to bypass multifactor authentication. Learn more 🖸	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 [2]
O View	O View	O View
Require multifactor authentication for guest access Require guest users perform multifactor authentication when accessing your company resources. Learn more [2]	 Require compliant or hybrid Azure AD joined device for admins Require privileged administrators to only access resources when using a compliant or hybrid Azure AD joined device. Learn more I2 	O Block access for unknown or unsupported device platform Users will be blocked from accessing company resources when the device type is unknown or unsupported. Learn more ☑
⑦ View ↓ Download JSON file	⑦ View ↓ Download JSON file	⑦ View ↓ Download JSON file
○ No persistent browser session Protect user access on unmanaged devices by preventing browser sessions from remaining signed in after the browser is closed and setting a sign-in frequency to 1 hour. Learn more □	 Require approved client apps or app protection policies To prevent data loss, organizations can restrict access to approved modern auth client apps with Intune app protection policies. Learn more I 	Use application enforced restrictions for O365 apps Block or limit access to O365 apps, including SharePoint Online, OneDrive, and Exchange Online content. This policy requires SharePoint admin center configuration. Learn more I
ত View 🞍 Download JSON file	O View ↓ Download JSON file	ত View 🞍 Download JSON file

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.**

Home > Conditional Access | Overview > Policies >

008 Use application enforced restrictions for O365 apps ...

_

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.	Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more c
Learn more @	Device platforms ①
008 Use application enforced restrictions fo	Locations ①
Assignments	Not configured
Users (i)	Client apps 🕕
All users included and specific users excluded	Not configured
Target resources (i)	Filter for devices ①
1 resource included	Not configured
Network NEW ①	Authentication flows 🕡
Not configured	Not configured
Conditions 🕕	
1 condition selected	
Access controls	

Grant ①

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

Device platforms \times
Apply policy to selected device platforms. Learn more 🖻
Configure ① Ves 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!

Apply policy to selected device platforms. Learn more
Configure
Ves
No
Include
Exclude
Android
IOS
Windows Phone
Windows
macOS
Linux

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.**

Microsoft Intune admin center			
*	Home >		
1 Home	📷 Windows Windows	s apps	
🖾 Dashboard			
E All services	₽ Search × «	+ Create () Refresh J. Export	Columns 🖂
Devices	Windows apps		
Apps	Monitor	Q Search	(i) Platform: Windows Type
ᠲ Endpoint security	✓ Manage apps		
Reports	🐯 Configuration	Nama A	
🚨 Users	Protection	Name T	Platform V
A Groups	S mode supplemental		
Tenant administration	policies		
X Troubleshooting + support	Policies for Microsoft 365 apps		
	App selective wipe		
	🚱 Quiet time		
	✓ Organize apps		
	📑 Assignment filters		
	App categories		

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

Home > Windows Windows apps >			
Add Microsoft 365 App Microsoft 365 Apps (Windows 10 and later)	ps ···		
· · · · · · · · · · · · · · · · · · ·			
App suite information O	onfigure app suite ③ Assignments ④ Review + create		
Suite Name * 🕡	ICTG_APP_01_M365		
Description *	Get help with markdown supported for descriptions.		
	Microsoft 365 Apps for Windows 10 and later		
	Preview		
	Microsoft 365 Apps for Windows 10 and later		
Publisher 🕕	Microsoft		
Category 🛈	Productivity ~		
Show this as a featured app in the Company Portal ①	Yes No		
Information URL ()	https://products.office.com/explore-office-for-home		
Privacy URL ①	https://privacy.microsoft.com/privacystatement		
Developer ①	Microsoft		
Owner i	Microsoft		
Notes ()			
Logo 🛈	Change image		
	Office		

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.

Home > Windows Windows apps >		
Add Microsoft 365 App Microsoft 365 Apps (Windows 10 and later)	S	
App suite information Conf	igure app suite ③ Assignments ④ Review + create	
Configuration settings format *	Configuration designer	\sim
Configure app suite		
Select Office apps 🕕	6 selected	\sim
Select other Office apps (license required)	Access	
App suite information	✓ OneNote	
These settings apply to all apps you have se	Outlook	
Architecture 🕕	PowerPoint	
Default file format *	Skype for Business	
Update channel * 🕕	✓ Teams	
Remove other versions ()	Vord	

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.

App suite information

These settings apply to all apps you have selected in the suite. Learn more

Architecture ③	32-bit 64-bit	
Default file format *	Office Open Document Format	\sim
Update channel * 🕕	Current Channel	\sim
Remove other versions ①	Yes No	
Version to install ①	Latest Specific	
Specific version	Latest version	\sim
Properties		
Use shared computer activation \bigcirc	Yes No	
Accept the Microsoft Software License Terms on behalf of users	Yes No	
Install background service for Microsoft Search in Bing ①	Yes No	
Languages 🕢	1 language(s) selected	

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).
Idd Microsoft 365 Apps icrosoft 365 Apps (Windows 10 and later)				
App suite information	오 Configure app suite	3 Assignments (4) Review + create		
Required 🗊				
Group mode	Group	Filter mode		
Included	All users	None		
r Add group 🛈 + Add all user	rs 🛈 + Add all devices 🛈			
Available for enrolled d	evices 🗊			
Group mode	Group	Filter mode		
No assignments				
Add group ① + Add all user	rs ()			
Uninstall 🕕				
Group mode	Group	Filter mode		
No assignments				
+ Add group 🛈 + Add all user	rs 🛈 + Add all devices 🛈			

Politiku zacílíme na všechny uživatele a máme hotovo.

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/~/pro tection

Microsoft Intune admin center	r	
«	Home > Apps	
숚 Home	Report Protection	
🚈 Dashboard		
E All services	✓ Search × «	i Did you know Microsoft Intune supports
🖵 Devices	(i) Overview	+ Create × () Refrech × Expor
Apps	All Apps	
🛼 Endpoint security	Monitor	iOS/iPadOS
Reports	\lor Platforms	Android
🙎 Users	Windows	Windows
A Groups	iOS/iPadOS	Windows Information Protection
Tenant administration	🖵 macOS	ICTG_APP_PROTECTION_02_iOS
🗙 Troubleshooting + support	Android	
	arsigma Manage apps	
	Configuration	
	Protection	

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

Home > Apps Protection >		
Create policy		\times
Sasics Apps 3 Data pro	(4) Access requirements (5) Conditional launch	
() Device type targeting has moved to the	Assignments step in policy creation. Learn more about assigning App Protection Policies	
Target policy to	All Apps	
	Selected apps	
We'll continue to add managed apps to yo	All Apps	
	All Microsoft Apps	
	Core Microsoft Apps	

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



Home > Apps | Protection >

Create policy

🛿 Basics 🔮 Apps 3 Data protection 🕘 Access requirements 💿 Conditional launch

This group includes the Data Loss Prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

Data Transfer		
Backup org data to iTunes and iCloud backups ①	Allow	Block
Send org data to other apps ①	Policy managed apps	\sim
Select apps to exempt	Select	
Select universal links to exempt	Select	
Select managed universal links	Select	
Save copies of org data ①	Allow	Block
Allow user to save copies to selected services \bigcirc	0 selected	\vee
Transfer telecommunication data to 🔅	Any dialer app	\checkmark
Dialer App URL Scheme		
Transfer messaging data to 🕕	Any messaging app	\checkmark
Messaging App URL Scheme		
Receive data from other apps $ \mathbb{O} $	All Apps	\checkmark
Open data into Org documents ①	Allow	Block
Allow users to open data from selected services ①	l selected	\vee
Restrict cut, copy, and paste between other apps ①	olicy managed apps with paste in	~
Cut and copy character limit for any app)	
Third party keyboards	Allow	Block
Encryption		
Encrypt org data 🛈	Require No	t required
Functionality		
Sync policy managed app data with native apps or add-ins \bigcirc	Allow	Block
Printing org data 🕕	Allow	Block
Restrict web content transfer with other apps ①	Any app	~
Unmanaged browser protocol 🕕		
Org data notifications ①	Allow	~
Previous Next		

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

Create policy			
🕑 Basics 🛛 Apps 🔗 Data protection	Access requirements	5 Conditional launch	
Configure the PIN and credential requirements that	users must meet to access apps i	n a work context.	
PIN for access (i)	Require	Not required	
PIN type ①	Numeric	Passcode	
Simple PIN 🛈	Allow	Block	
Select minimum PIN length 🕕	4	\checkmark	
Touch ID instead of PIN for access (iOS 8+/iPadOS) ①	Allow	Block	
Override biometrics with PIN after timeout ①	Require	Not required	
Timeout (minutes of inactivity)	0		
Face ID instead of PIN for access (iOS 11+/iPadOS) ①	Allow	Block	
PIN reset after number of days 🛈	Yes	No	
Number of days	0		
App PIN when device PIN is set 🕕	Require	Not required	
Work or school account credentials for access \bigcirc	Require	Not required	
Recheck the access requirements after (minutes of inactivity) \star	30		

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



Set the sign-in security requirements for your access protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company app. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single setting. Learn more about conditional launch actions.

App conditions

Setting	Value	Action
Max PIN attempts	5	Reset PIN ····
Offline grace period	1440	Block access (minutes) ••••
Offline grace period \checkmark	180 🗸	Wipe data (days) \checkmark …
Select one 🗸		

Device conditions

Configure the following conditional launch settings for device based conditions through your app protection policy.

Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices.

Setting	Value	Action	
Jailbroken/rooted devices		Block access	
Select one \checkmark			

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.



Data Transfer

Backup org data to Android backup services ①	Allow	Block	
Send org data to other apps 🕕	Policy managed apps		\sim
Select apps to exempt	Select		
Save copies of org data ①	Allow	Block	
Allow user to save copies to selected services $\ensuremath{}$	0 selected		\sim
Transfer telecommunication data to 🕠	Any dialer app		\sim
Dialer App Package ID			
Dialer App Name			
Transfer messaging data to 🕕	Any messaging app		\checkmark
Messaging App Package ID			
Messaging App Name			
Receive data from other apps 🕕	All Apps		\sim
Open data into Org documents 🔅	Allow	Block	\square
Allow users to open data from selected services ①	4 selected		\sim
Restrict cut, copy, and paste between other apps ①	Policy managed apps with paste in		\checkmark
Cut and copy character limit for any app *	0		
Screen capture and Google Assistant	Allow	Block	
Approved keyboards 🕕	Require	Not required	
Select keyboards to approve	Select		
Encryption			
Encrypt org data 🕕	Require	Not required	
Encrypt org data on enrolled devices 🕕	Require	Not required	
Functionality			
Sync policy managed app data with native apps or add-ins ①	Allow	Block	
Printing org data 🕕	Allow	Block	
Restrict web content transfer with other apps ①	Any app		\sim
Unmanaged Browser ID 🕕			
Unmanaged Browser Name			
Org data notifications ①	Allow		\sim
Start Microsoft Tuppel connection on			

Previous Next

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.

Create policy

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

PIN for access (i)	Require	Not required
PIN type ①	Numeric	Passcode
Simple PIN ①	Allow	Block
Select minimum PIN length 🕕	4	\sim
Biometrics instead of PIN for access 🕕	Allow	Block
Override biometrics with PIN after timeout ①	Require	Not required
Timeout (minutes of inactivity)	0	
Class 3 Biometrics (Android 9.0+) ①	Require	Not required
Override Biometrics with PIN after biometric updates ①	Require	Not required
PIN reset after number of days ①	Yes	No
Number of days	0	
Select number of previous PIN values to maintain * 🕕	0	
App PIN when device PIN is set $~$	Require	Not required
Work or school account credentials for access ①	Require	Not required
Recheck the access requirements after (minutes of inactivity) * ①	30	

Nastavení pinu nechávám velmi podobné jako u iOS.



Set the sign-in security requirements for your access protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company app. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single setting. Learn more about conditional launch actions.

App conditions

Setting	Value	Action
Max PIN attempts	5	Reset PIN ····
Offline grace period	1440	Block access (minutes) •••
Offline grace period \checkmark	180 🗸	Wipe data (days) \checkmark …
Select one 🗸 🗸		

Device conditions

Configure the following conditional launch settings for device based conditions through your app protection policy.

Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices.

Setting	Value	Action	
Jailbroken/rooted devices		Block access	
Select one \checkmark			

Toto nastavení je úplně stejné jako iOS.

Poté stačí zacílit na uživatele a máte hotovo!

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

~	Home > Devices	
1 Home	🖃 Devices Complian	ce ×
📶 Dashboard		
E All services		Delivies Notifications Detics poncompliant devices Compliance attings Covints Monitor
Devices	() Overview	Policies Notifications Retire noncompliant devices Compliance settings Scripts Monitor
Apps	All devices	🗟 Save 🗙 Discard
🕵 Endpoint security	🔎 Device query	These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device
🕎 Reports	Monitor	Compliance Policy , which is reflected in device monitoring.
L Users	✓ By platform	Mark devices with no compliance Not compliant policy assigned as ①
🎎 Groups	Windows	
Tenant administration	iOS/iPadOS	Compliance status validity period (days) ①
🗙 Troubleshooting + support	🖵 macOS	
	Android	
	🖂 Linux	
	Device onboarding	
	🗊 Windows 365	
	👩 Enrollment	
	V Manage devices	
	Configuration	
	Compliance	
	Conditional access	
	Scripts and remediations	
	· · · ·	

Home > Endpoint security

Endpoint security | Microsoft Defender for Endpoint \times ₽ Search X « 🕐 Refresh 🔚 Save 🔀 Discard 📋 Delete 🔄 All devices Connection status Last synchronized Security baselines 🕄 Not set up ---Security tasks ✓ Manage (4) O Antivirus Disk encryption 😞 Firewall Endpoint Privilege f) Some toggles are disabled and acting as "off" because Microsoft Defender for Endpoint is not actively communicating with Intune Management for this account. Please check the state of the connection in the Microsoft Defender for Endpoint admin console Endpoint detection and When the connection has returned to a healthy status (Active or Provisioned), the toggles will be re-enabled and any pre-existing setting state will be restored. response App Control for Business (Preview) **Endpoint Security Profile Settings** 🌒 Attack surface reduction Account protection Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations 🕕 Off On Device 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 (<u>security.microsoft.com</u>) 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 😳.

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!

Edit row ×
Locale *
Czech V
Subject *
Vaše zařízení nesplňuje požadavky!
Message 🛈
Raw HTML editor 🕦 💽 Off
1 Vaše zařízení nesplňuje požadavky nastavené vaším správcem IT
2 Restartujte počítač a kotaktujte správce.
Set to default locale

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.

 Device Health		
Microsoft Attestation Service evaluation	settings	
Use these settings to confirm that a dev	ice has protective measures enabled	at boot time. Learn more
Windows 10 and 11		
BitLocker	Require	Not configured
Secure Boot	Require	Not configured
Code integrity	Require	Not configured

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.

🕑 Basics 🛛 🕑 Compliand	ce settings 3 Actions fo	r noncompliance	(4) Assignments	5 Review + create		
Specify the sequence of actions	Specify the sequence of actions on noncompliant devices					
Action	Schedule (days after noncompliance) 🕕	Message template	Additiona	l recipients (
Mark device noncompliant	1 ~					
V	0					

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

*	Home > Devices Enrollment >
숚 Home	Device preparation policies
🖾 Dashboard	
E All services	
🛄 Devices	+ Create ✓ () Refresh ⊻ Export ⊨ Columns ✓
Apps	Automatic (Preview)
ᠲ Endpoint security	User Driven
Reports	Configure Windows Autopilot device preparation deployments from a singl
Lusers	
🐣 Groups	Priority Name
🍰 Tenant administration	1 CTG_AUTOPILOT_01_STREAMLINED
🗙 Troubleshooting + support	

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.

**	Home > Devices Enrollment > Device preparation policies >							
숚 Home	Create profile							
ZII Dashboard	lindows Autopilot device preparation policies							
E All services	Vertraduction Review Device group Configuration settings Scope tags Assignments							
Devices								
Apps	Name *							
퉋 Endpoint security	ICTG_AUTOPILOT_01_STREAMLINED_PROFILE							
Reports	Description							
🙎 Users	M365 apps							
A Groups								
Tenant administration								
🗙 Troubleshooting + support								

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 (<u>https://learn.microsoft.com/en-us/autopilot/device-</u>

preparation/tutorial/user-driven/entra-join-device-group). Poté co vytvoříme skupinu, tak ji přidáme do nastavení **Autopilota**.

«	Home > Devices Enrollment > Device preparation policies >
숨 Home	Create profile
🖾 Dashboard	Windows Autopilot device preparation policies
E All services	Alateaduction Regist Provide group Configuration activities Scone tage
📮 Devices	Introduction Scope tags
Apps	Select the Entra ID security group that will contain your Autopilot devices when they enroll. The policies, a to this group either explicitly or implicitly through the group's own memberships. Learn more about Auto
퉋 Endpoint security	
🚰 Reports	(i) Note: before you configure device groups, make sure that the Intune Provisioning Client service principal has been a
🔒 Users	Search by group name
A Groups	
ಶ Tenant administration	්ස් Group Group members
🗙 Troubleshooting + support	ICTG_G_SEC_DEV_AUTOPILOT_ST 0 devices, 0 users

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

Deployment settings		^
Deployment mode * (i)	User-driven	~ *
Deployment type *	Single user	~ *
Join type * (i)	Microsoft Entra joined	~ *
User account type * 🕕	Standard User	
Out-of-box experience settings		^
Minutes allowed before showing installation error	120	$\hat{\cdot}$
Custom error message (i)	Contact your organization's support person for help.	*
Allow users to skip setup after multiple attempts *	No No	
Show link to diagnostics *	Yes	

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.

Apps			^
Select u device s devices + Ad	up to 10 managed apps you want to refe security group you selected earlier. You in this deployment. Id — Remove	rence with this deplo can check the installa	oyment. These apps should be assigned to the ation status for these apps in the device details for
	Allowed Applications $\ \uparrow$	Publisher	Version
	ICTG_APP_01_REQUIRED_M365	Microsoft	

Scripty zatím žádné nemáme, takže jdeme dál.

Scope tag necháme už klasicky na Default a v záložce Assignments si přidáme

skupinu uživatelů.

Home > Devices	Enrollment >	Device preparation p	olicies >				
Create prof	ile vice preparation	policies					
Introduction	Sasics	Device group	✓ Configuration set	tings	Scope tags	Assignments	Review + cre
Search by group n	ame						
ೆಸ್ Group		Group mem	bers	Target typ	pe	Filter	
AU All users				Include		<u>Add assignn</u>	nent filter

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.

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**.

Microsoft Intune admin center	
«	Home > Endpoint security
숚 Home	📻 Endpoint security Disk encryption 👘
Z Dashboard	
E All services	P Search × ≪ + Create Policy Create Policy Export
Devices	✓ Overview
Apps	Overview Overview
🌷 Endpoint security	Policy name ↑↓ Policy type
Reports	Security baselines
🙎 Users	🥫 Security tasks
A Groups	✓ Manage
Tenant administration	Antivirus
🗙 Troubleshooting + support	Search Disk encryption
	🛖 Firewall
	Endpoint Privilege Management
	Endpoint detection and response

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SecurityManagement Menu/~/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

Create Policy

Sasics	Configur	ation settings		Scope tags	Assignments	I	Review + create	
\searrow Search settings by setting name		i						
BitLocker								^
Require Dev Encryption	ice	i)		Enabled				~
Allow Warni Disk Encrypt	ng For Other tion	(i)		Disabled				\sim
Allow Stan Encryption	dard User	(i)		Enabled				\sim
Configure R Password Ro	ecovery otation	(i)		Not configured	ł			\sim

Dále pod záložkou BitLocker Drive Encryption vyberte:

Pro první možnost – **Enabled**

Pro prostřední tři – XTS-AES 256-bit

A pro poslední – **Not configured**

BitLocker Drive Encryption		^
Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)	Enabled	~
Select the encryption method for fixed data drives:	XTS-AES 256-bit	~ *
Select the encryption method for operating system drives:	XTS-AES 256-bit	~ *
Select the encryption method for removable data drives:	XTS-AES 256-bit	~ *
Provide the unique identifiers for your (i) organization	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)

Operating System Drives		^
Enforce drive encryption type on operating system ① drives	Enabled	~
Select the encryption type: (Device)	Full encryption	~ 1
Require additional ① authentication at startup	Enabled	~
Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)	False	
Configure TPM startup key and PIN:	Do not allow startup key and PIN with TPM	~
Configure TPM startup key:	Do not allow startup key with TPM	~
Configure TPM startup PIN:	Do not allow startup PIN with TPM	~
Configure TPM startup:	Allow TPM	~
Configure minimum PIN () length for startup	Disabled (Default)	\sim
Allow enhanced PINs for startup	Disabled (Default)	\sim
Disallow standard users from changing the PIN or ① password	Not configured	\sim
Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN.	Not configured	\sim
Enable use of BitLocker authentication requiring preboot keyboard input on slates	Not configured	~
Choose how BitLocker- protected operating system drives can be recovered	Enabled	~
	Allow 256-bit recovery key	~ *
Configure user storage of BitLocker recovery information:	Allow 48-digit recovery password	~*
Allow data recovery agent	False	
Configure storage of BitLocker recovery information to AD DS:	Store recovery passwords and key packages	
Do not enable BitLocker until recovery information is stored to AD DS for operating system drives	True	
Omit recovery options from the BitLocker setup wizard	True	
Save BitLocker recovery information to AD DS for operating system drives	True	
Configure pre-boot recovery message and ① URL	Not configured	\sim

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.

Fixed Data Drives		^	
Enforce drive encryption type on fixed data drives	Enabled	\sim]
Select the encryption type: (Device)	Full encryption	\sim]*
Choose how BitLocker- protected fixed drives can (i) be recovered	Enabled	~]
	Allow 256-bit recovery key	\sim]*
Configure user storage of BitLocker recovery information:	Allow 48-digit recovery password	\sim	*
Allow data recovery agent	False		
Configure storage of BitLocker recovery information to AD DS:	Backup recovery passwords and key packages		
Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives	True		٦
Omit recovery options from the BitLocker setup wizard	True		
Save BitLocker recovery information to AD DS for fixed data drives	True		
Deny write access to fixed drives not protected by BitLocker	Not configured	\sim]

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!!!

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/~/Devices/DevicesMenuBlade/~/Devices/Devices/DevicesMenuBlade/~/Devices/Devic

Home > Devices	
کی Devices Device s ICT-GROUP s.r.o 365identity - Mic	crosoft Entra ID
Overview All devices	 Save X Discard R Got feedback? 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.
Manage	
② Device settings	Maximum number of devices per user ①
Enterprise State Roaming	Unlimited
BitLocker keys (Preview)	
Local administrator password recovery	Local administrator settings
Activity	Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview) 🕥
Audit logs	Yes No
Bulk operation results (Preview)	Registering user is added as local administrator on the device during Microsoft Entra join (Preview) ① All Selected None
Troubleshooting + Support	Selected
New support request	No member selected
🗙 Diagnose and solve problems	
	Manage Additional local administrators on all Microsoft Entra joined devices
	Enable Microsoft Entra Local Administrator Password Solution (LAPS)
	Other settings
	Restrict users from recovering the BitLocker key(s) for their owned devices ① Yes No

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.**

~	Home > Endpoint security			
🟫 Home	👩 Endpoint security	Account protect	ction	
🖾 Dashboard				
E All services		+ Create Policy 🖒	Refresh 🞍 Export	
Devices	✓ Overview			
Apps	 Overview 	Search by profile na	ime	
🅠 Endpoint security	All devices	Policy name	\uparrow_{\downarrow} Policy type	\uparrow_{\downarrow} Assigned
🚅 Reports	Security baselines	ICTG_05_CONFIG_HAP	RDEN_Windows_ Local admin passwor	d solution (Win Yes
📩 Users	🏮 Security tasks			
A Groups	\vee Manage			
Tenant administration	Antivirus			
🗙 Troubleshooting + support	Disk encryption			
	🛖 Firewall			
	Endpoint Privilege Management			
	Endpoint detection and response			
	App Control for Business (Preview)			
	🌒 Attack surface reduction			
	Q Account protection			
	🛃 Device compliance			
	Conditional access			
	\checkmark Monitor			
	Assignment failures			

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.

✓ Search settings by sett	ting name (
LAPS			^
Backup Directory (i)		Backup the password to Azure AD only	\sim
Password Age Days (i)		Configured 7	\$
Administrator Account Name	i	Configured VASEFIRMAlocalADM	
Password Complexity ()		Not configured	~
Password Length (i)		Configured	<>
Post Authentication Actions	(i)	Not configured	~
Post Authentication Reset Delay	0	Not Configured	
Automatic Account Management Enabled	0	Not configured	~

Scope tag je default.

Politiku zacílíme na skupinu zařízení spravovaných pomocí Intune.

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

1 Home	🧮 Devices Scripts an	nd remediations 📩
🖾 Dashboard		
≡ All services	₽ Search × «	Pomodiations Diatform scripts
Devices	Overview	. Platom scipts
Apps	All devices	Create and run script packages on devices to proactively fi
, Endpoint security	🔎 Device query	organization. Use this table to see the status of your deplo
🚰 Reports	Monitor	
💄 Users	By platform	+ Create 🕐 Refresh 🞍 Export 🗮 Columns ∨
🍰 Groups	Windows	
🍰 Tenant administration	iOS/iPadOS	🔎 Search 🚺 😨 Ar
🔀 Troubleshooting + support	🖵 macOS 🛛 📩	Script package pame Author
	Android	Script package name Author
	🦲 Linux	Restart stopped Office C2R svc Microsoft
	imes Device onboarding	ElanLAPS Roman Krutina
	🗊 Windows 365	HPConnectForMEM -SG_HP_Elit Roman Krutina - ADMIN
	🗔 Enrollment	ICTG_Windows_01_LAPS_SCRIPT GA JKrutina
	✓ Manage devices	Update stale Group Policies Microsoft
	Configuration	OneDrive Teams Mount Settings Roman Krutina
	Compliance	
	Onditional access	
	Scripts and remediations	1

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
  }
}/vmăăte VASEEIPMAlocalADM zo imóno. ktoró into postovili v LAN
```

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!!!

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 **EntralD 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.**

Settings picker	\times
Use commas "," among search terms to lookup settings by their keywords	
	Search
+ Add filter	
Browse by category	
Administrative Templates\Windows Components\Microsoft User Experience Virtualization\Applications	
FS Logix ODFC Containers	
Microsoft Office 2016\Miscellaneous	
OneDrive	

Setting name

Select a category to show settings

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)

^	OneDrive	Remove category
	1 76 of 86 settings in this category are not configured	
	Continue syncing on metered networks E nabled (User) ①	Θ
	Prevent users from redirecting their Enabled Windows known folders to their PC ①	Θ
	Silently move Windows known folders to Enabled OneDrive	Θ
	Desktop (Device) True	
	Documents (Device) True	
	Pictures (Device) True	
	Show notification to users after folders No have been redirected: (Device) *	~
	Tenant ID: (Device) Vase-Tenant-ID	~
	Silently sign in users to the OneDrive sync app with their Windows credentials	Θ
	Use OneDrive Files On-Demand 🕕 💽 Enabled	Θ

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!

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 ⁽²⁾). 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**

 Home Dashboard 	Home > Endpoint security	Endpoint detection and respon	se			Create a profile	×
All services All services Devices Apps Endpoint security Peports Users Users Users Tranat administration	Search x « Overview Search x a Search x and	Summary EDR Onboarding Status Defender for Endpoint Connector Status C Defender for Endpoint connector enabled		Windows devices onboarded to Defender for Endpoint C) Refresh Report generated 6/2/2025, 9:28:27 PM 16 / 19 Cheanded Not Onboarded 16 3		Platform Platform Platform Platform Platform Profile Endpoint detection and response Indepoint detection and response capabilities provide actions to remeative detections that are reletione and actionable. Security analysis can prioritize alerts effectively, gain visibility into the full scope of a breach, and take respon actions to remeative threads	
Troubleshooting + support	Los etcypion Firevall Finevall Findpoint Privilege Management Findpoint Privilege Indpoint election and Propone Propone Apc Control for Business (Preview) Attack surface reduction	Endpoint detection and response (EDR) policies + Create policy C Refresh Export E Search O Policy name KIG 01 EDR DETECTION RESEARCE	Columns ~ Policy type Endooint detectio	Assigned	Platforr	This policy applies to: Windows 10, Windo	ws II, and Windows Server to: MDM. MicrosoftSense supported devices
	Account protection Account protection Device compliance Conditional access Monitor Assignment failures Setup Microsoft Defender for Endpoint Help and support At the pand support					Cruste	

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.

Microsoft Defender for En	dpoint		^
Microsoft Defender for Endpoint client configuration package type	0	Auto from connector	~
Onboarding blob from Connector	0	•••••	*
Sample Sharing		All (Default)	\sim
[Deprecated] Telemetry Reporting Frequency	0	Not configured	\sim

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/SecurityManagement Menu/~/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)

Defender

Allow Archive Scanning	()	Allowed. Scans the archive files. (Default)	\sim
Allow Behavior () Monitoring		Allowed. Turns on real-time behavior monitoring. (Default)	\sim
Allow Cloud Protection	(i)	Allowed. Turns on Cloud Protection. (Default)	\sim
Allow Email Scanning	D	Allowed. Turns on email scanning.	\sim
Allow Full Scan On Mapped Network Drives	0		
Not allowed. Disables so	canning on mapped r	network drives. (Default)	
Allow Full Scan Removable Drive Scanning	(i)	Allowed. Scans removable drives.	\sim
[Deprecated] Allow Intrusion Prevention System	(i)	Not configured	\sim

 $\overline{}$

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	()	Allowed. (Default)	\sim
Allow Realtime Monitoring	()		
Allowed. Turns on and run	is the real-time monit	oring service. (Default) \sim	
Allow Scanning Network Files	()	Not allowed. Turns off scanning of network files. (Default)	\sim
Allow Script Scanning (Allowed. (Default)	\sim
Allow User UI Access ()		Allowed. Lets users access UI. (Default)	\sim
		Configured	
Avg CPU Load Factor ()		20	\sim
Archive Max Depth 🕕		Not Configured	
Archive Max Size ()		Not Configured	
Check For Signatures Before Running Scan	()	Disabled (Default)	\sim
Cloud Block Level 🕕		Default State (Default)	\sim
Cloud Extended Timeout	(i)	Not Configured	

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 fíčura

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	0	Not Configured
Disable Catchup Full Scan	0	Enabled (Default)
Disable Catchup Quick Scan	()	Enabled (Default)
Enable Low CPU Priority	D	Enabled ~
Enable Network Protection	(i)	Enabled (audit mode)

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!

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 ()
+ Add — Remove ← Import → Export
Excluded Extensions 1
xcluded Paths ()
+ Add — Remove ← Import → Export
Excluded Paths ↑
xcluded Processes ()
+ Add — Remove ← Import → Export
Excluded Processes ↑

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 ()						
Audit mode. Windows Defender will detect potentially unwanted applications, but take no action $$						
Real Time Scan Direction (i)	Not configured	\sim				
Scan Parameter ()	Quick scan (Default)	\sim				
Schedule Quick Scan	Configured					
Time	720	$\hat{\cdot}$				
Schedule Scan Day (i)	Every day (Default)	\sim				
Schedule Scan Time i	Not Configured					

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
+ Add — Remove ← Import → Export
Signature Update Fallback Order 1
Signature Update File Shares Sources (i)
+ Add — Remove ← Import → Export
Signature Update File Shares Sources ↑

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

		Configured	
Signature Update Interv	val 🕕	24	$\hat{\cdot}$
Submit Samples Consen	nt 🛈	Send safe samples automatically. (Default)	\sim
Disable Local Admin Merge	0	Disable Local Admin Merge	\sim
Allow On Access Protection	(i)	Allowed. (Default)	\sim

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

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

Threat Severity Default Action

Remediation action for Hig severity threats	h	Not configured	\sim
Remediation action for Seve threats	ere	Not configured	\sim
Remediation action for Low severity threats	,	Not configured	\sim
Remediation action for Moderate severity threats		Not configured	\sim
Allow Network Protection Down Level	(i)	Network protection will be disabled downlevel. (Default)	\sim
Allow Datagram Processing On Win Server	(i)	Datagram processing on Windows Server is disabled. (Default)	\sim
Disable Dns Over Tcp Parsing	0	DNS over TCP parsing is enabled (Default)	\sim
Disable Http Parsing ()		HTTP parsing is enabled (Default)	\sim
Disable Ssh Parsing ()		SSH parsing is disabled	\sim
Disable Tls Parsing ()		TLS parsing is enabled (Default)	\sim
[Deprecated] Enable Dns Sinkhole	Ū	Not configured	\sim

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

[ICT] GROUP

Engine Updates Channel	1)		
Not configured (Default).	The device will stay up	to date automatically during the gradual release $$	
Metered Connection Updates	(i)	Not configured	\sim
Platform Updates Channel	()		
Not configured (Default).	The device will stay up	to date automatically during the gradual release $ imes $	
Security Intelligence Updates Channel	(i)	Current Channel (Staged): Same as Current Channel (Broad).	\sim
Randomize Schedule Task Times	(i)	Not configured	\sim
Scheduler Randomization Time	(i)	Not Configured	
Disable Core Service ECS Integration	(i)	Not Configured	\sim
Disable Core Service Telemetry	()	Not Configured	\sim

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**).