

Začínáme s Intune



Petr Vlk



KPCS





View all photos

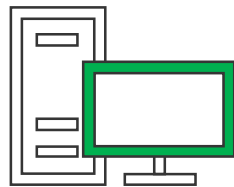


Search the web and Windows



VS





Tradiční správa a nasazení

Licencování zařízení



Active Directory



Firemní instalační obraz



Firemní síť



WSUS



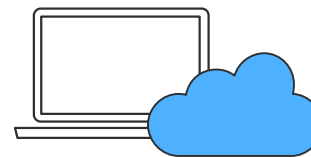
Manuální instalace



Configuration Manager



Další bezpečnostní nástroje



Moderní správa a nasazení



Licencování uživatelů



Azure Active Directory



Dynamický balíček



Jakékoliv připojení



Windows Update for Business



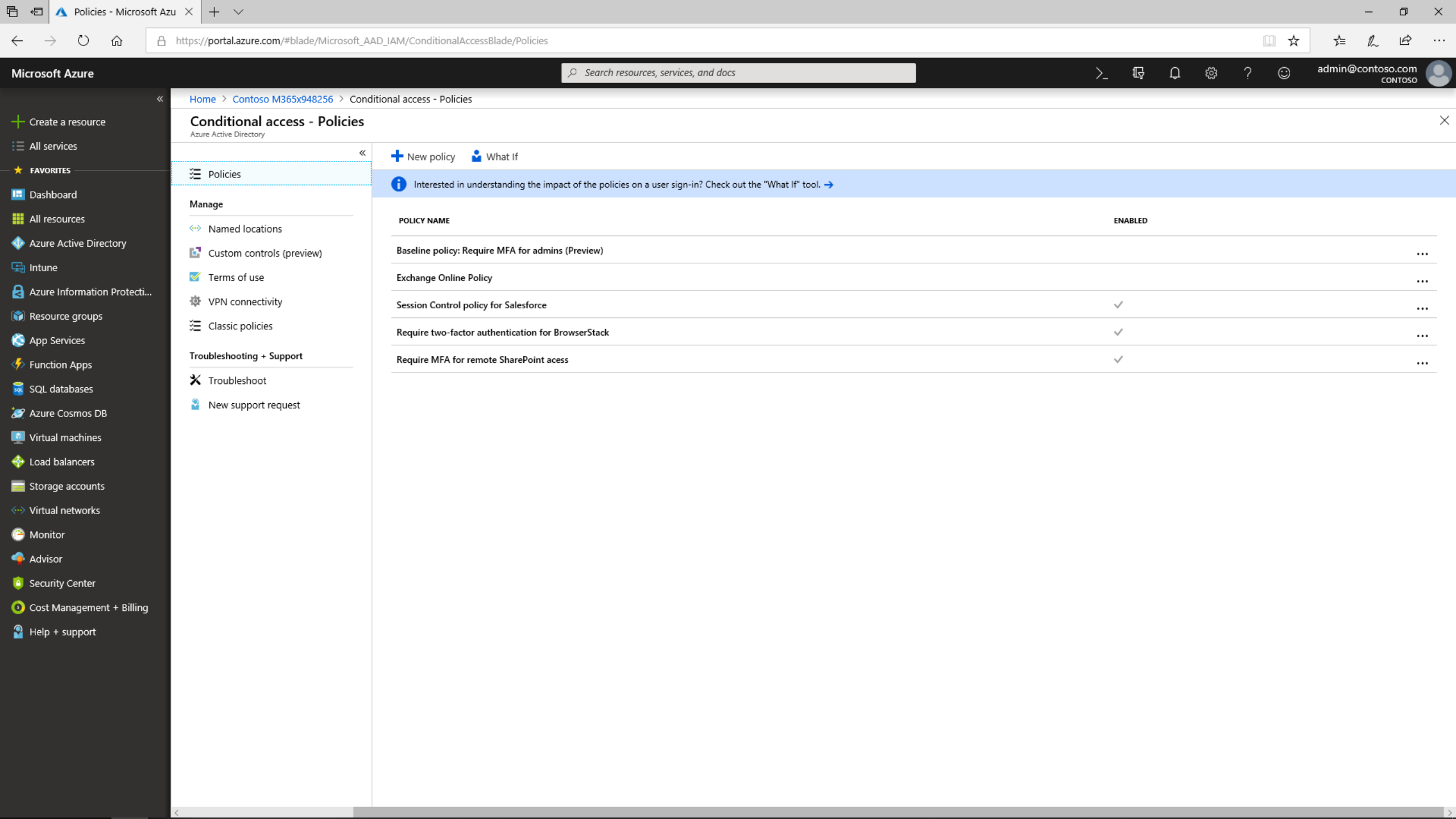
Microsoft Store for Business



Intune



Advanced Threat Protection (ATP)



Conditional access - Policies

Azure Active Directory

[+ New policy](#) [What If](#)

i Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. [→](#)

- ☰ Policies
- Manage**
- ↔ Named locations
- 📄 Custom controls (preview)
- ✉ Terms of use
- ⚙️ VPN connectivity
- ☰ Classic policies
- Troubleshooting + Support**
- ✖ Troubleshoot
- 🗣 New support request

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)		...
Exchange Online Policy		...
Session Control policy for Salesforce	✓	...
Require two-factor authentication for BrowserStack	✓	...
Require MFA for remote SharePoint access	✓	...

- + Create a resource
- ☰ All services
- ★ FAVORITES
- 🏠 Dashboard
- 📊 All resources
- 🔗 Azure Active Directory
- 📁 Intune
- 🔒 Azure Information Protecti...
- 📁 Resource groups
- 🌐 App Services
- ⚡ Function Apps
- 🗄 SQL databases
- 🌌 Azure Cosmos DB
- 🖥 Virtual machines
- ⚙️ Load balancers
- 📁 Storage accounts
- ↔ Virtual networks
- 📊 Monitor
- 🗣 Advisor
- 🛡 Security Center
- 💰 Cost Management + Billing
- 🗣 Help + support

- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Azure Active Directory
- Intune
- Azure Information Protecti...
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

New

Info

* Name
Expensify location policy ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps ⓘ
1 app included >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ
0 controls selected >

Enable policy

On Off

Create

Conditions

Info

Sign-in risk ⓘ
Not configured >

Device platforms ⓘ
Not configured >

Locations ⓘ
Not configured >

Client apps (preview) ⓘ
Not configured >

Device state (preview) ⓘ
Not configured >

Done

Locations

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes No

Include Exclude

Any location
 All trusted locations
 Selected locations

Select >
None

Done



- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Azure Active Directory
- Intune
- Azure Information Protecti...
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

New

Info

* Name
Expensify location policy ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps ⓘ
1 app included >

Conditions ⓘ
1 condition selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ
0 controls selected >

Enable policy

On Off

Create

Grant

Select the controls to be enforced.

Block access
 Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

For multiple controls

Require all the selected controls
 Require one of the selected controls

Select





isaiahI@m365x948256.onmicrosoft.com

You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

[Sign out and sign in with a different account](#)

[More details](#)

Contoso

Režimy MDM

- Office 365 MDM
 - Obsaženo v ceně
 - Online konzole
 - iOS a Android (EAS)
 - Politiky souladu
- Intune
 - Placená licence
 - Online konzole
 - iOS, Android, Windows
 - Politiky souladu
 - Konfigurační politiky
 - Nasazení aplikací
 - Napojení na AAD
- Co-Management
 - Vyžaduje SCCM
 - Dvě konzole
 - Windows (iOS, Android)
 - Politiky souladu
 - Konfigurační politiky
 - Nasazení aplikací
 - Napojení na AD i AAD

Vlastnictví zařízení

- Soukromá (BYOD)
 - Ochrana aplikací MAM
 - Enrollment do MDM
 - ◆ Profile Owner
- Firemní
 - Ochrana aplikací MAM
 - Enrollment do MDM
 - ◆ Firemní
 - Kiosek
 - Device Owner
 - Device Owner with Profile Owner

Základní konfigurace v pár minutách

Microsoft Admin center

Setup
Microsoft 365 Business

Step 1
Personalize sign-in

Step 2
Add users

Step 3
Protect data & devices

Admin

Set Windows 10 device configuration

When a user connects a Windows 10 device to your organization, they'll automatically receive the settings you configure below. You can also make sure that users get the latest version of Office installed on their devices. We recommend that you start with the default settings and adjust your configuration later. [Learn more about configuring Windows 10](#)

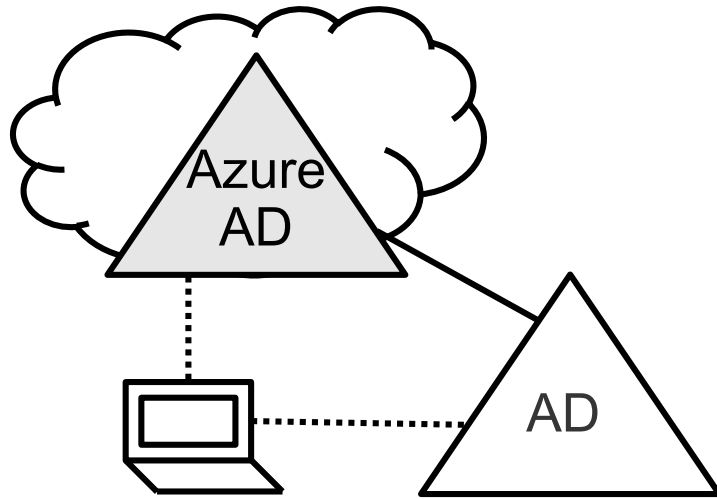
- Secure Windows 10 devices ⓘ
- Help protect PCs from viruses and other threats using Windows Defender Antivirus On
 - Help protect PCs from web-based threats in Microsoft Edge On
 - Turn off device screen when idle for ▾
 - Allow users to download apps from Windows Store On
 - Allow users to access Cortana On
 - Allow users to receive Windows tips and advertisements from Microsoft On
 - Keep Windows 10 devices up to date automatically On
- [Restore default settings](#)
- Install Office on Windows 10 devices ⓘ No



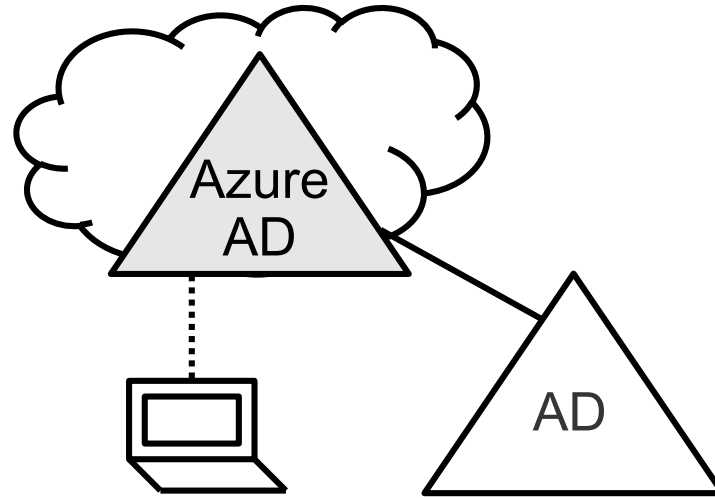
Podporované operační systémy

- Apple
 - iOS 10.0 a novější
 - macOS 10.12 a novější
- Google
 - Android 4.4 a novější (Android Device Manager)
 - Android 5.0 a novější (Android Enterprise)
- Microsoft
 - Surface Hub
 - Windows 10
 - Windows 10 Mobile
 - Windows 10 IoT
 - Windows Phone 8.1, Windows 8.1 RT a Windows 8.1 a Windows 7

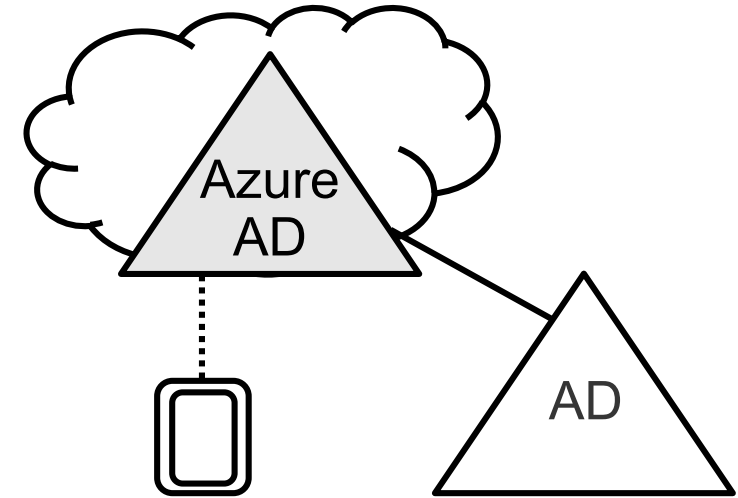
Azure AD a Intune



Hybrid Azure AD joined



Azure AD joined



Azure AD registered

Zařízení v Azure AD a Intune

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPLIANT
Win10-2	✔ Yes	Windows...	10.0 (150...	Hybrid Azure AD joined	N/A	None	N/A
DESKTOP-4D7A...	✔ Yes	Windows	10.0.1713...	Azure AD joined	TU1	Microsoft Intune	✔ Yes
CONTENTLIBSAN	✔ Yes	Windows...	10.0 (143...	Hybrid Azure AD joined	N/A	None	N/A
WIN10-5	✔ Yes	Windows...	10.0 (1713...	Hybrid Azure AD joined	N/A	Microsoft Intune	✔ Yes
INT-1	✔ Yes	Windows	10.0.1776...	Azure AD registered	INT-1	None	N/A
MININT-P6A4R...	✔ Yes	Windows...	10.0 (150...	Hybrid Azure AD joined	N/A	None	N/A
<input checked="" type="checkbox"/> Win10-6	✔ Yes	Windows...	10.0 (1713...	Hybrid Azure AD joined	N/A	None	N/A

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPLIANT
Win10-2	✔ Yes	Windows...	10.0 (150...	Hybrid Azure AD joi...	N/A	None	N/A
DESKTOP-4D7A...	✔ Yes	Windows	10.0.1713...	Azure AD joined	TU1	Microsoft Intune	✔ Yes
CONTENTLIBSAN	✔ Yes	Windows...	10.0 (143...	Hybrid Azure AD joi...	N/A	None	N/A
<input checked="" type="checkbox"/> WIN10-5	✔ Yes	Windows...	10.0 (1713...	Hybrid Azure AD joi...	N/A	Microsoft Intune	✔ Yes

Metody registrace do Intune

		Local Admin Rights	MDM User Scope enabled in AAD	DNS CNAME Registration	Service Connection Point (SCP)	Automatic Enrolment GPO	Minimum OS Version	Hardware	AAD Device Trust Type	Intune Device Owner	AAD Owner	
		Requirements						Device Properties				
User Driven	1 Add work or School (User Driven)	Y	Y	Y					Workplace	Personal	User that Enrolled device	
	2 Modern App Sign-in (User Driven)	Y	Y	Y					Workplace	Personal	User that Enrolled device	
	3 Enrol in MDM Only (User Driven)	Y		Y					null	Personal	None	
	4 Azure AD Join (OOBE)	Y*	Y						AzureAD	Corporate	User that Enrolled device	
	5 Azure AD Join (Autopilot)		Y						AzureAD	Corporate	User that Enrolled device	
	6 Hybrid Azure AD Join (Autopilot)		Y				1809+		ServerAD	Corporate	User that Enrolled device	
IT Driven	7 Enrol in MDM Only (Device Enrollment Manager)	Y		Y					null	Corporate	None	
	8 Hybrid AADJ + Automatic Enrolment GPO				Y	Y	1709+		ServerAD	Corporate	N/A	
	9 SCCM Co-management				Y				ServerAD	Corporate	N/A	
	10 Azure AD Join (Bulk Enrolment)		Y						AzureAD	Corporate	Package_[token GUID]	
	11 Azure AD Join (AutoPilot Self Deploying Mode)		Y				1809+	TPM 2.0	AzureAD	Corporate	None	

* User performing OOBE Setup and Enrollment will end up being a local administrator for the device

CSP a GPO

- Configuration Service Provider

- Jedno nebo druhé
- Ale i oboje zároveň
- Někdo vyhrát musí
- Pozor na verzi OS!

- GPO -> CSP

Computer Policies

(-) SUPPORTED: Security Account Policies

These Security policies are fully supported by MDM. It should be possible to directly migrate these settings to MDM.

Policy Name	State	GPO Name	Feedback?
MaximumPasswordAge	42	Default Domain Policy	<input type="checkbox"/>
MinimumPasswordLength	7	Default Domain Policy	<input type="checkbox"/>
PasswordHistorySize	24	Default Domain Policy	<input type="checkbox"/>
MaximumPasswordAge	19	AccountLocalServicesRegistry	<input type="checkbox"/>
PasswordHistorySize	19	AccountLocalServicesRegistry	<input type="checkbox"/>

(-) SUPPORTED: ADMX backed policies

These System ADMX policies are fully supported by MDM. It should be possible to directly migrate these settings to MDM.

Policy Name	State	GPO Name	Feedback?
Network/Network Provider/Hardened UNC Paths	Disabled	ADMX1	<input type="checkbox"/>
System/Remote Assistance/Turn on session logging	Enabled	ADMX1	<input type="checkbox"/>
Windows Components/AutoPlay Policies/Turn off Autoplay	Disabled	ADMX1	<input type="checkbox"/>
Windows Components/Windows Error Reporting/Consent/Customize consent settings	Enabled	ADMX1	<input type="checkbox"/>
Windows Components/Windows Error Reporting/Consent/Customize consent settings	Enabled	Complex ADMX Policies	<input type="checkbox"/>

(-) NOT SUPPORTED: Security Account Policies

These Security settings that are configured on the target but not supported by MDM.

Policy Name	State	GPO Name	Feedback?
ClearTextPassword	False	Default Domain Policy	<input type="checkbox"/>
MinimumPasswordAge	1	Default Domain Policy	<input type="checkbox"/>
MaxClockSkew	5	Default Domain Policy	<input type="checkbox"/>
MaxRenewAge	7	Default Domain Policy	<input type="checkbox"/>

Nechte si poradit

Pomůžeme nejen s nasazením správy mobilních zařízení pomocí **Microsoft 365**



KPCS CZ

Přední český poskytovatel řešení postavených na infrastruktuře a cloudových službách společnosti Microsoft. Naši špičkoví konzultanti jsou tím, co nás činí unikátními nejen v České republice, ale po celé Evropě a USA.

Jsme autory jedinečné služby ATOM dohlížející komplexně na celé prostředí po stránce dostupnosti, ale především bezpečnosti.

Nabízíme konzultace, implementace, migrace, kontroly zabezpečení, školení, adopční kampaně i zajištění technické podpory a pronájem licencí pro celé spektrum portfolia společnosti Microsoft.

Naši konzultanti vás provedou nejen světem online služeb Microsoft 365 a Azure, ale také tradičními lokálními serverovými produkty společnosti Microsoft, tedy Exchange, SharePoint a Windows Server.

obchod@kpcs.cz | www.kpcs.cz | www.atom.ms

