Profile konfiguracji: katalog ustawień zamiast GPO

Poziom: średniozaawansowany

Dotyczy: Intune, Windows 11, Group Policy analytics, Windows LAPS, BitLocker

Czas: ~60 min

Profil konfiguracji w Intune robi to samo co GPO: ustawia opcje Windows na komputerach z grupy. Strona pokazuje katalog ustawień, szablony administracyjne, przenoszenie polityk z GPO narzędziem Group Policy analytics oraz najważniejsze profile: BitLocker, LAPS, zaporę, ograniczenia USB, skrypty i Remediations.

Skróty użyte na tej stronie (16)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
ADMX	format plików szablonów administracyjnych GPO, następca starszego formatu ADM
CSP	w Windows: Configuration Service Provider, mechanizm, przez który MDM albo RMM zapisuje ustawienia systemu, na przykład profil VPN
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
HID	Human Interface Device: klasa urządzeń do obsługi komputera przez człowieka, czyli klawiatury, myszy i podobne urządzenia USB
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
LAPS	Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu
MDM	Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi
RMM	Remote Monitoring and Management: platforma do zdalnego zarządzania i monitorowania stacji roboczych
TPM	Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów
UEFI	Unified Extensible Firmware Interface: nowoczesne oprogramowanie firmowe płyty głównej albo maszyny wirtualnej, następca starszego BIOS-u, obsługuje między innymi Secure Boot

Skrót	Co znaczy
USB	Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
WinRE	Windows Recovery Environment: środowisko odzyskiwania Windows na osobnej partycji, potrzebne między innymi do szyfrowania BitLockerem
XML	eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Fiszka

Ścieżki w centrum administracyjnym podajemy po angielsku, tak jak w dokumentacji. Microsoft przenosi pozycje menu, więc w razie rozbieżności szukamy po nazwie ustawienia. Komendy wykonujemy w PowerShellu z uprawnieniami administratora.

□□ ZMIENIA SYSTEM

Utworzenie profilu w katalogu ustawień: Settings catalog

```
Microsoft Intune admin center → Devices → Manage devices → Configuration → Create → New policy
→ Platform: Windows 10 and later
→ Profile type: Settings catalog
→ Basics: nazwa, np. Windows-Przegladarka-Edge
→ Configuration settings → Add settings → wybieramy kategorię i ustawienia
→ Assignments: grupa pilotażowa
```

W oknie wyboru ustawień (settings picker) wybieramy kategorię, a w niej pojedyncze ustawienia albo cały zestaw przyciskiem Select all these settings. Katalog zawiera praktycznie wszystkie ustawienia, które da się wysłać do Windows przez MDM.

□□ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Configuration settings profilu Settings catalog z otwartym oknem Add settings, widoczna wyszukiwarka i lista kategorii, zaznaczone jedno ustawienie.

MDM = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi

KLIKAMY W INTERFEJSIE

Dodanie szablonów administracyjnych w katalogu ustawień: Add settings

```
Settings catalog → Configuration settings → Add settings
→ rozwijamy kategorię Administrative Templates
→ wybieramy ustawienia o tych samych ścieżkach, co w edytorze GPO
```

Ustawienia z oznaczeniem (User) dotyczą użytkownika i działają po zalogowaniu, pozostałe dotyczą komputera. Starszy profil Templates, Administrative Templates jest od wydania 2412 przestarzały i tylko do odczytu, więc nowe polityki tworzymy w katalogu ustawień. Własne i cudze pliki ADMX/ADML (np. Chrome, aplikacje własnego zespołu) można zaimportować.

ADMX = format plików szablonów administracyjnych GPO, następca starszego formatu ADM

TYLKO ODCZYT

Wyeksportowanie GPO do pliku XML: Get-GPOReport

```
Get-GPOReport -Name "NazwaGPO" -ReportType Xml -Path C:\Audyty\NazwaGPO.xml
```

> (gdzie `NazwaGPO` to nazwa obiektu zasad grupy, a `C:\Audyty` to katalog na pliki do analizy)

To samo można zrobić w Group Policy Management Console: prawy przycisk na GPO, Save Report, typ XML. Plik nie może przekraczać 4 MB, a kodowanie musi być poprawne dla Unicode.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **XML** = eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

KLIKAMY W INTERFEJSIE

Zaimportowanie GPO do analizy: Group Policy analytics

```
Microsoft Intune admin center → Devices → Manage devices → Group Policy analytics
→ Import → wskazujemy plik XML → Next
→ Scope tags: Default → Create
```

Po imporcie widzimy kolumny Group Policy name, Active Directory Target, MDM Support (procent ustawień obsługiwanych w Intune), Unknown Settings, Targeted in AD i Last imported. W szczegółach każde ustawienie ma wartość Yes, No albo Deprecated.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **MDM** = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

ZMIENIA SYSTEM

Przeniesienie wybranych ustawień do katalogu: Group Policy analytics, Migrate

```
Group Policy analytics → zaznaczamy GPO w kolumnie Migrate → przycisk Migrate
→ zakładka Settings to migrate: zaznaczamy ustawienia z MDM Support: Yes
→ Configuration: sprawdzamy wartości
→ Basics: nazwa, np. Windows: Imported Microsoft Edge GPOs
→ Assignments: grupa pilotażowa → Create
```

Wartości przenoszą się z GPO, a po utworzeniu polityki można je zmienić. Ustawienia AppLocker i zapory mają wyłączoną opcję Migrate, bo tworzymy je w Endpoint security (patrz niżej).

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: widok Group Policy analytics po imporcie GPO „Konfiguracja proxy przeglądarki", widoczna kolumna MDM Support z procentem i zakładka Settings to migrate z zaznaczonymi ustawieniami.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **MDM** = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi

TYLKO ODCZYT

Sprawdzenie, jakie GPO nałożyło ustawienia na komputerze: gpresult /h

```
gpresult /h C:\Temp\gpo.html
```

Raport HTML pokazuje, które GPO dotarły do komputera i użytkownika. Przydaje się, gdy ustawienie z Intune nie działa, a podejrzewamy, że GPO ustawia je inaczej.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **HTML** = HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce · **gpresult** = group policy result: które GPO trafiły na komputer

ZMIENIA SYSTEM

Utworzenie profilu BitLocker z kluczem w Entra ID: Disk encryption

```
Microsoft Intune admin center → Endpoint security → Disk encryption → Create policy
→ Platform: Windows → Profile: BitLocker
→ Require Device Encryption: Enabled
→ Allow Warning For Other Disk Encryption: Disabled
→ Allow Standard User Encryption: Enabled
→ Save BitLocker recovery information to Microsoft Entra ID: Enabled
→ Store recovery information in Microsoft Entra ID before enabling BitLocker: Required
→ Client-driven recovery password rotation: Enable rotation on Microsoft Entra ID and
hybrid joined devices
```

Ciche szyfrowanie (bez pytań do użytkownika) wymaga komputera Microsoft Entra joined albo hybrid joined, modułu TPM, trybu UEFI z włączonym Secure Boot i skonfigurowanego środowiska odzyskiwania Windows (WinRE). Allow Standard User Encryption włączamy, bo nasi użytkownicy nie są administratorami.

TPM = Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów · **UEFI** = Unified Extensible Firmware Interface: nowoczesne oprogramowanie firmowe płyty głównej albo maszyny wirtualnej, następca starszego BIOS-u, obsługuje między innymi Secure Boot · **WinRE** = Windows Recovery Environment: środowisko odzyskiwania Windows na osobnej partycji, potrzebne między innymi do szyfrowania BitLockerem

TYLKO ODCZYT

Sprawdzenie warunków szyfrowania na komputerze: reagentc /info

```
reagentc /info
manage-bde -status C:
Confirm-SecureBootUEFI
```

Pierwsze polecenie sprawdza, czy WinRE jest włączone, drugie pokazuje stan szyfrowania, trzecie stan Secure Boot.

WinRE = Windows Recovery Environment: środowisko odzyskiwania Windows na osobnej partycji, potrzebne między innymi do szyfrowania BitLockerem · **reagentc** = Recovery Agent Command: pokaż i włącz środowisko odzyskiwania Windows (WinRE) · **manage-bde** = BitLocker Drive Encryption: zarządzanie szyfrowaniem dysków

ZMIENIA SYSTEM

Dograne istniejącego klucza do Entra ID: manage-bde, BackupToAAD-BitLockerKeyProtector

```
manage-bde -protectors -get C:
BackupToAAD-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId
"{NumerGuidProtektora}"
```

> (gdzie `{NumerGuidProtektora}` to identyfikator protektora typu hasło odzyskiwania, odczytany pierwszym poleceniem)

Dla komputerów zaszyfrowanych, zanim profil istniał. Polecenie `BackupToAAD-BitLockerKeyProtector` zapisuje klucz w Microsoft Entra ID, a odpowiednik dla Active Directory opisuje strona o BitLockerze z kluczem w AD.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **manage-bde** = BitLocker Drive Encryption: zarządzanie szyfrowaniem dysków

KLIKAMY W INTERFEJSIE

Odczyt klucza odzyskiwania w Intune: Recovery keys

```
Microsoft Intune admin center → Devices → All devices → wybrany komputer
→ Monitor → Recovery keys → Show Recovery Key
```

□□ KLIKAMY W INTERFEJSIE

Włączenie Windows LAPS w Microsoft Entra ID: Device settings

```
Microsoft Entra admin center → Entra ID → Devices → Overview → Device settings
→ Enable Local Administrator Password Solution (LAPS): Yes → Save
```

Wymaga roli co najmniej Cloud Device Administrator. Windows LAPS z hasłem w Entra ID działa na komputerach Entra joined i hybrid joined, a nie działa na zarejestrowanych (registered).

□□ **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

□□ ZMIENIA SYSTEM

Utworzenie profilu Windows LAPS: Account protection

```
Microsoft Intune admin center → Endpoint security → Account protection → Create policy
→ Platform: Windows → Profile: Local admin password solution (Windows LAPS)
→ Backup Directory: katalog docelowy (Microsoft Entra ID albo Active Directory)
→ Administrator Account Name, Password Age Days, Password Complexity, Password Length
→ Post Authentication Actions, Post Authentication Reset Delay
```

Wybór katalogu to najważniejsza decyzja: dla komputerów, które często są poza domeną, wybieramy Microsoft Entra ID, a dla stacji, które na stałe siedzą w biurze i mają już skonfigurowany LAPS z AD, zostajemy przy dotychczasowym rozwiązaniu opisanym na stronie o Windows LAPS i przenosimy je w fali 5.

□□ **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu ·**AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

□□ KLIKAMY W INTERFEJSIE

Odczyt hasła lokalnego administratora z Intune: Local admin password

```
Microsoft Intune admin center → Devices → All devices → wybrany komputer
→ Monitor → Local admin password → Show
→ ponowna rotacja: menu ... → Rotate Local admin password
```

Do odczytu potrzebujemy uprawnienia `microsoft.directory/deviceLocalCredentials/password/read` (mają je m.in. Cloud Device Administrator i Intune Administrator), a do ręcznej rotacji prawa Remote tasks: Rotate Local Admin Password w Intune.

KLIKAMY W INTERFEJSIE

Utworzenie profilu zapory Windows: Firewall

```
Microsoft Intune admin center → Endpoint security → Firewall → Create policy
→ Platform: Windows → Profile: Windows Firewall
→ ustawienia profili Domain, Private, Public: stan zapory i domyślne działanie dla ruchu przychodzącego
```

Osobny profil Windows Firewall rules definiuje reguły (do 150 niestandardowych na profil). Profil Windows Firewall nie koliduje z profilem reguł, ale dwa profile Windows Firewall mogą ze sobą kolidować, więc trzymamy jeden.

TYLKO ODCZYT

Ograniczenie urządzeń USB: Device Installation

```
Settings catalog → Add settings → Administrative Templates → System → Device Installation
→ Device Installation Restrictions
→ Allow installation of devices using drivers that match these device setup classes: Enabled
   (dopisujemy klasy: klawiatura, mysz, HID, USB Bus)
→ Prevent installation of devices not described by other policy settings: Enabled
```

Klasy konfiguracji do dopisania: klawiatura `{4d36e96b-e325-11ce-bfc1-08002be10318}`, mysz `{4d36e96f-e325-11ce-bfc1-08002be10318}`, urządzenia HID `{745a17a0-74d3-11d0-b6fe-00a0c90f57da}`, magistrala USB `{36fc9e60-c465-11cf-8056-444553540000}`. Poprawną listę klas budujemy na pilotażu, bo zbyt wąska lista wyłączy także klawiaturę i mysz.

USB = Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne · **HID** = Human Interface Device: klasa urządzeń do obsługi komputera przez człowieka, czyli klawiatury, myszy i podobne urządzenia USB

TYLKO ODCZYT

Znalezienie klasy zablokowanego urządzenia: setupapi.dev.log

```
Select-String -Path "$env:windir\inf\setupapi.dev.log" -Pattern "Restricted installation of devices not described by policy"
```

Dziennik `setupapi.dev.log` w pobliżu tego wpisu zawiera linię `Class GUID of device changed to: {GUID}`. Ten identyfikator dopisujemy do dozwolonych klas.

GUID = Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera

TYLKO ODCZYT

Dodanie skryptu PowerShell do wykonania na komputerach: Platform scripts

```
Microsoft Intune admin center → Devices → Scripts and remediations → Platform scripts
→ Add → Windows 10 and later
→ Script location: plik .ps1 (poniżej 200 KB)
→ Run this script using the logged on credentials: No (kontekst systemowy)
→ Enforce script signature check: No (gdy skrypt nie jest podpisany)
→ Run script in 64-bit PowerShell Host: Yes
→ Assignments: grupa
```

Skrypt wykonuje się po przypisaniu do urządzenia i po zmianie skryptu, nie przy każdym logowaniu. Limit czasu to 30 minut. Agent Intune Management Extension instaluje się sam przy pierwszym przypisanym skrypcie, a wynik wykonania zapisuje w `C:\ProgramData\Microsoft\IntuneManagementExtension\Logs\AgentExecutor.log`.

ZMIENIA SYSTEM

Utworzenie pakietu Remediations: Scripts and remediations

```
Microsoft Intune admin center → Devices → Manage devices → Scripts and remediations
→ Remediations → Create
→ Detection script file, Remediation script file
→ Run this script using the logged-on credentials: wg potrzeb
→ Run script in 64-bit PowerShell: Yes
→ Schedule: Once, Hourly albo Daily
```

Skrypt wykrywania kończy się kodem `1`, gdy wykryje problem, i wtedy uruchamia się skrypt naprawy. Każdy inny kod oznacza, że problemu nie ma. Remediations wymagają licencji, których nasz pakiet Business Premium nie obejmuje (patrz niżej), a skrypt możemy uruchomić na żądanie akcją Run remediation z poziomu urządzenia.

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Środa, 10:15. Tomek wdraża na swoim laptopie pilotażowym politykę „blokuj nieznane urządzenia USB" i po restarcie mysz USB i skaner kodów pożyczony od Marka przestają działać. W `setupapi.dev.log` znajduje wpisy „Restricted installation of devices not described by policy" i klasę `{745a17a0-74d3-11d0-b6fe-00a0c90f57da}`, czyli HID, której nie dopisał do listy dozwolonych. Dopisuje klasę, Sync, restart i wszystko działa. Dobrze, że to był pilotaż, a nie magazyn o 6:00.

Jak to działa

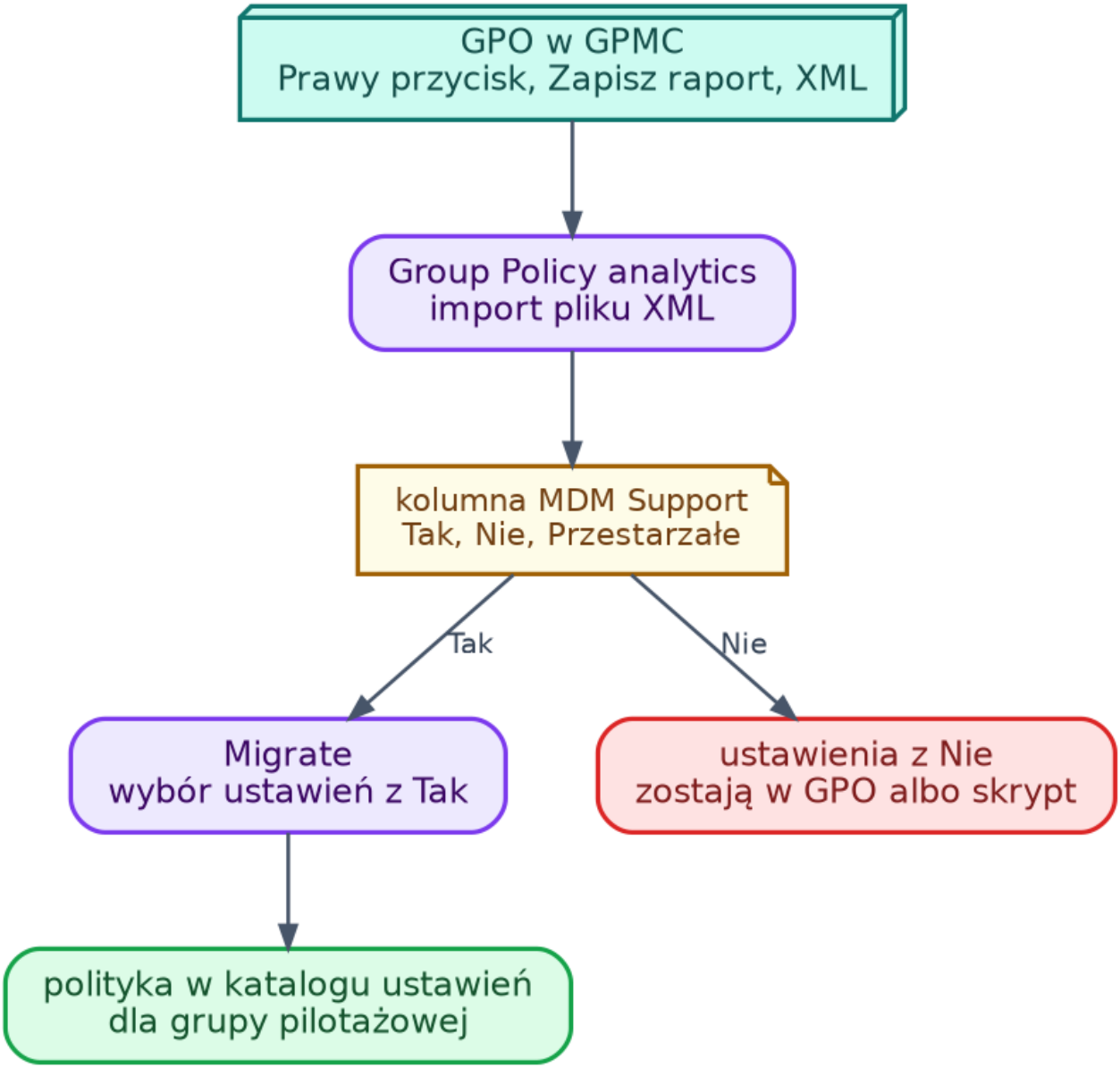
□□ Rozwiń: jak to działa pod spodem

Pojęcie: CSP. Configuration Service Provider: wbudowany w Windows odbiornik ustawień. Intune wysyła polecenie do konkretnego CSP (np. do CSP zapory), a Windows wykonuje je tak samo, jak zrobiłaby to zasada grupy. Nazwy ustawień w katalogu Intune pochodzą z tych CSP.

Pojęcie: katalog ustawień (Settings catalog). Pełna, przeszukiwalna lista ustawień Windows, z której składamy profil. Zastępuje starsze szablony tam, gdzie je zastąpiono, ale szablony typu Wi-Fi, VPN i trusted certificate nadal istnieją i nadal służą do swoich zadań.

Pojęcie: polityki zabezpieczeń punktu końcowego (Endpoint security). Osobna część Intune, w której tworzymy polityki per funkcja: dyski (BitLocker), zapora, ochrona konta (LAPS), antywirus. Ustawienia są te same co w katalogu, ale ekran jest ułożony

wokół funkcji.



GPO z domeny przechodzi przez eksport XML do Group Policy analytics, ustawienia z MDM Support Yes migrują do katalogu ustawień dla grupy pilotażowej, reszta zostaje w GPO (kliknięcie otwiera pełny rozmiar)

Gdzie ląduje każda polityka z audytu

Strona o audycie GPO podzieliła polityki Zielonej na trzy decyzje. Tabela pokazuje, jakim narzędziem w Intune realizujemy to, co migruje.

Polityka z audytu GPO	Narzędzie w Intune	Fala
Instalacja oprogramowania	aplikacje Win32 (strona o aplikacjach)	1
Autorejestracja certyfikatów	profile certyfikatów (strona o certyfikatach)	2
Konfiguracja proxy przeglądarki	katalog ustawień, import z Group Policy analytics	3
Mapowanie dysków sieciowych	skrypt PowerShell z Platform scripts	4
Ustawienia Defendera, BitLockera, zapory, LAPS	Endpoint security	5
Polityka haseł domeny, polityka audytu	zostają w AD i GPO	bez migracji

Co Group Policy analytics potrafi, a czego nie

Narzędzie importuje plik XML i dla każdego ustawienia sprawdza, czy ma odpowiednik w katalogu. Wynik Yes oznacza istniejące ustawienie, No brak odpowiednika, a Deprecated ustawienie starszej wersji systemu lub oprogramowania. Obsługuje ustawienia z CSP Policy, PassportForWork, BitLocker, Firewall i AppLocker oraz preferencje GPO. Ma też ograniczenia, które znamy z dokumentacji:

- dla ustawień spoza ADMX liczy poprawnie tylko pliki w języku angielskim,
- jeśli kilka GPO ustawia to samo inaczej, w migracji wybieramy jedną wartość,
- ustawienia z wynikiem No zostają w GPO albo przenosimy je skryptem,
- po migracji sprawdzamy powiadomienia (Notifications), bo ustawienia z nietypowym formatem wartości mogą zgłosić błąd.

GPO i Intune na jednym komputerze

Komputer hybrid joined dostaje i GPO, i profile z Intune. Gdy oba ustawiają to samo, wynik zależy od typu ustawienia. Windows ma ustawienie `ControlPolicyConflict/MDMWinsOverGP`: przy wartości 1 polityka MDM blokuje odpowiednik z GPO. Ma ograniczenia: dotyczy tylko ustawień z CSP Policy i tylko tych opartych na ADMX, a domyślnie jest wyłączone (wartość 0). Dlatego nie zostawiamy konfliktu losowi: dla każdego ustawienia wybieramy jedną metodę, a GPO

wyłączamy dopiero po potwierdzeniu, że profil dotarł (tak samo jak w planie wycofania).

Przenoszenie BitLockera i LAPS z Active Directory do Entra ID

BitLocker z kluczem w Microsoft Entra ID to tylko kopia klucza w innym miejscu niż Active Directory. Przy migracji z klucza w AD na klucz w Entra ID dokładamy klucz do Entra (fiszka wyżej) przed wyłączeniem GPO, żeby w razie awarii komputera było skąd go odczytać. Tak samo postępujemy z LAPS: wybieramy jeden katalog docelowy hasła i zapisujemy, w którym są hasła, żeby audytor i pomoc techniczna nie szukali ich w dwóch miejscach.

Skrypty i Remediations: co wymaga licencji

Funkcja	Czego wymaga	Uwaga
Platform scripts	Intune, agent IME instaluje się sam	ograniczenie 200 KB i 30 minut
Remediations	według dokumentacji: Windows Enterprise E3 lub E5 (m.in. w Microsoft 365 E3 i E5), Windows Education A3 lub A5 albo Windows Virtual Desktop Access na użytkownika	Business Premium nie jest tam wymieniony, więc przed użyciem sprawdzamy licencje w aktualnej dokumentacji i u dostawcy
Remediations, urządzenia	Entra joined albo hybrid joined, z rejestracją w Intune	komputery tylko zarejestrowane (registered) nie są obsługiwane

Częste błędy

Objaw	Przyczyna	Co robimy
Profil przypisany, a komputer nie zmienia ustawienia	komputer nie zgłosił się jeszcze do Intune albo ustawienie koliduje z GPO	Sync na komputerze (Company Portal, Settings, Sync), `gpresult /h`, wybór jednej metody
Group Policy analytics pokazuje niski procent MDM Support	stare ustawienia, spoza ADMX albo w polskim systemie	czytamy listę ustawień, nie sam procent, i ręcznie dobieramy odpowiedniki w katalogu

Objaw	Przyczyna	Co robimy
Przycisk Migrate niedostępny dla ustawień zapory i AppLocker	te ustawienia migrują się przez Endpoint security	tworzymy politykę Firewall w Endpoint security
BitLocker nie szyfruje po cichu	brak TPM, UEFI, Secure Boot albo WinRE	`reagentc /info`, `Confirm-SecureBootUEFI`, sprawdzamy firmware
W Intune nie widać klucza odzyskiwania	klucz nie został zapisany w Entra ID	`BackupToAAD-BitLockerKeyProtector` dla istniejących protektorów, politykę z wymogiem zapisu przed szyfrowaniem dla nowych
Brak zakładki Local admin password albo puste hasło	LAPS wyłączony w Entra, komputer registered albo polityka nie dotarła	sprawdzamy ustawienie w Device settings, typ dołączenia i przypisanie profilu
Po polityce USB nie działa klawiatura albo mysz	lista dozwolonych klas jest za wąska	`setupapi.dev.log`, dopisujemy klasę z linii Class GUID of device changed to
Skrypt platformy nie uruchamia się drugi raz	skrypty wykonują się tylko po zmianie skryptu lub przypisania	zmieniamy skrypt albo przypisanie, a dla powtarzalnych zadań używamy Remediations ze stałym harmonogramem

□□ Ćwiczenia

1. W Group Policy analytics ustawienie ma wartość No w kolumnie MDM Support. Co z nim robimy?

Odpowiedź

No oznacza, że w katalogu nie ma odpowiednika. Ustawienie zostaje w GPO (jeśli komputer widzi domenę), a gdy musi działać poza domeną, szukamy innej drogi, np. skryptu z Platform scripts. Nie migrujemy go na siłę.

1. Dlaczego przy przejściu BitLockera z klucza w AD na klucz w Entra ID zapisujemy klucz w Entra ID, zanim wyłączymy GPO?

Odpowiedź

Żeby w razie awarii komputera zawsze był klucz do odczytu. Po wyłączeniu GPO komputer przestaje dopisywać klucze do AD, a ten zapisany w Entra ID jest dostępny w Intune w Devices, All devices, Recovery keys.

1. Marek pyta, czy może mieć w magazynie skrypt, który raz na godzinę sprawdza usługę i ją naprawia. Czego użyjemy i czego potrzebujemy?

Odpowiedź

Remediations: skrypt wykrywania kończy się kodem 1, gdy usługa nie działa, a skrypt naprawy ją uruchamia. Harmonogram ustawiamy na Hourly. Potrzebujemy licencji spełniającej wymagania Remediations (dokumentacja nie wymienia Business Premium), a jeśli jej nie mamy, zadanie wykonuje zwykły skrypt platformy albo zadanie w RMM.

Powiązane: Intune obok domeny: audyt GPO i plan migracji · Windows LAPS: hasło lokalnego administratora w Active Directory · BitLocker z kluczem odzyskiwania w Active Directory · Zasady zgodności i dostęp warunkowy · GPO od środka: tworzenie, łączenie, kolejność i diagnostyka

Źródła: Microsoft Learn, „Create a policy using settings catalog in Microsoft Intune" (learn.microsoft.com/intune/device-configuration/settings-catalog) · „Use ADMX templates on Windows devices in Microsoft Intune" (learn.microsoft.com/intune/device-configuration/settings-catalog/configure-admx-templates-windows) · „Use Microsoft Intune to import and analyze group policies" (learn.microsoft.com/intune/device-configuration/import-group-policy-analytics) · „Migrate your imported group policy to a policy in Microsoft Intune" (learn.microsoft.com/intune/device-configuration/migrate-group-policy) · „Encrypt Windows devices with BitLocker using Intune" (learn.microsoft.com/intune/device-configuration/endpoint-security/encrypt-bitlocker-windows) · „Deploy Intune policies to manage Windows LAPS" (learn.microsoft.com/intune/device-security/laps/deploy-policy) · „Use Windows LAPS with Microsoft Entra ID" (learn.microsoft.com/entra/identity/devices/howto-manage-local-admin-passwords) · „Manage firewall settings with endpoint security policies" (learn.microsoft.com/intune/device-configuration/endpoint-security/firewall) · „Restrict USB devices using settings catalog" (learn.microsoft.com/intune/device-configuration/settings-catalog/restrict-usb) · „Add PowerShell scripts to Windows devices in Intune" (learn.microsoft.com/intune/device-management/tools/run-powershell-scripts-windows) · „Use Remediations to detect and fix support issues" (learn.microsoft.com/intune/device-management/tools/deploy-remediations) · „Policy CSP: ControlPolicyConflict" (learn.microsoft.com/windows/client-management/mdm/policy-csp-controlpolicyconflict)

Revision #19
Created 2026-10-03 11:23:05 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:14 UTC by Tomasz Konieczny