Intune obok domeny: audyt GPO i plan migracji

Poziom: zaawansowany
Dotyczy: Microsoft Entra ID, Intune, Active Directory na dc01/dc02 **Czas: ~40 min**

Domena Active Directory i Intune przez jakiś czas rządzą tymi samymi komputerami naraz, zanim zdecydujemy, co zostaje po staremu, a co przechodzi do chmury. Audytujemy istniejące GPO politykę po polityce i układamy plan migracji w falach, zamiast przenosić wszystko naraz.

Skróty użyte na tej stronie (8)

Skrót	Co znaczy
BYOD	Bring Your Own Device: pracownik używa prywatnego urządzenia do pracy
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
MDM	Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi
PKI	Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
XML	eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Fiszka

KLIKAMY W INTERFEJSIE

Objęcie istniejącego komputera Intune bez reinstalacji: hybrid join i GPO

```
dc01: Group Policy Management → GPO dla jednostki z komputerami pilotażu
→ Computer Configuration → Administrative Templates → Windows Components → MDM
→ Enable automatic MDM enrollment using default Microsoft Entra credentials → Enabled
→ poświadczenia: User Credential
```

Komputer zostaje w domenie `ad.zielona.example` dokładnie tak jak wcześniej. Entra Connect przenosi jego obiekt do Microsoft Entra ID (hybrid join), a GPO każe mu samemu zapisać się do Intune. To droga bez reinstalacji z pełnym zarządzaniem. Szczegóły i warunki (licencja, zakres MDM, synchronizacja) opisuje strona Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot.

> Samo „Połącz” w Ustawienia → Konta → Uzyskaj dostęp do pracy lub szkoły na komputerze firmowym robi z niego urządzenie `Entra registered`. Ta droga jest przewidziana dla prywatnych urządzeń (BYOD) i nie daje pełnego zarządzania komputerem przez Intune, więc w Zielonej nie używamy jej dla floty.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **MDM** = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi · **BYOD** = Bring Your Own Device: pracownik używa prywatnego urządzenia do pracy

TYLKO ODCZYT

Sprawdzenie stanu rejestracji na komputerze

```
dsregcmd /status
```

Po hybrid join wiersze `AzureAdJoined` i `DomainJoined` mówią `YES`. Sam wiersz `WorkplaceJoined : YES` przy `AzureAdJoined : NO` oznacza rejestrację `Entra registered`, czyli drogę dla prywatnych urządzeń, a nie to, czego chcemy na komputerze firmowym. Sprawdzamy to polecenie zaraz po zmianie, zamiast zakładać, że przeszła poprawnie.

dsregcmd = Device Registration Command: pokaż, czy komputer jest dołączony do Entra ID, domeny albo zarejestrowany, i zdiagnozuj rejestrację

TYLKO ODCZYT

Eksport wszystkich GPO do audytu

```
Get-GPOReport -All -ReportType Html -Path C:\Audyty\wszystkie-gpo.html
```

Jeden raport HTML ze wszystkimi politykami w domenie, do przeczytania i przedyskutowania z zespołem, zanim zdecydujemy, co z każdą polityką robimy. Wariant zapisujący każde GPO do osobnego pliku XML, wygodny do dalszego przeszukiwania automatem, opisaliśmy już na stronie Skrypty audytowe Active Directory.

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 · **XML** = eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Z życia wzięte

Z ŻYCIA WZIĘTE

Prezes, pan Zbigniew, wraca z urlopu z nowym laptopem kupionym w sklepie i pyta, kiedy będzie mógł na nim pracować. Wcześniej odpowiedź brzmiałaby: za dwa dni, po dojechaniu do serwerowni w Pamiątkowie i dołączeniu do domeny kablem. Teraz Tomek wysyła mu link do rejestracji konta pracy, pan Zbigniew loguje się sam z hotelu, a polityki Intune same dokładają Defendera i VPN, zanim laptop w ogóle zobaczy sieć biurową.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: Microsoft Entra ID. Chmurowy katalog tożsamości Microsoftu, następca nazwy Azure Active Directory. Osobny byt od domenowego Active Directory na `dc01`/`dc02`: konta, urządzenia i polityki mogą tam istnieć niezależnie od domeny, choć da się je też ze sobą zsynchronizować.

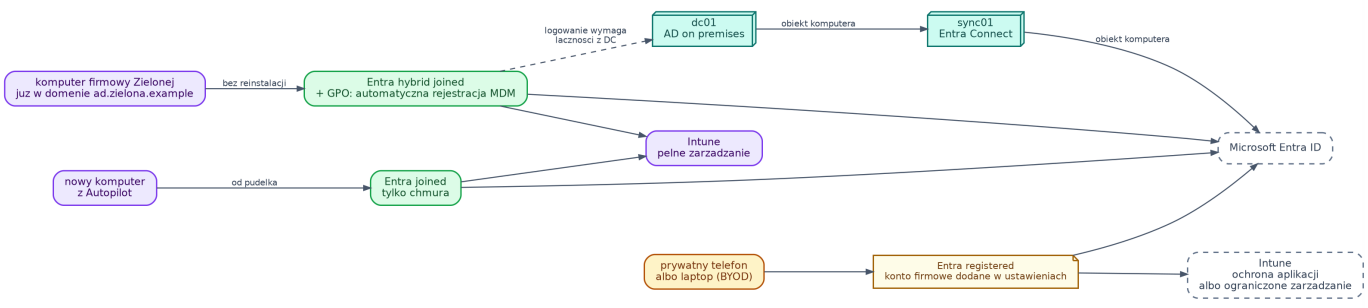
Pojęcie: Intune. Chmurowa platforma do zarządzania urządzeniami, oparta na Microsoft Entra ID zamiast na GPO: instaluje aplikacje, wymusza szyfrowanie i hasła, i

pilnuje zgodności komputera z polityką bezpieczeństwa, niezależnie od tego, czy komputer ma akurat łączność z siecią firmową, czy siedzi w hotelu na drugim końcu świata.

Pojęcie: Microsoft Defender. Wbudowany w Windows pakiet ochrony przed złośliwym oprogramowaniem, którego pełną konfigurację (skanowanie, ochronę przed manipulacją, reguły redukcji powierzchni ataku) da się scentralizować przez Intune tak samo, jak wcześniej przez GPO.

Pojęcie: Entra registered kontra Entra joined kontra hybrid joined. Trzy różne sposoby, w jaki komputer wiąże się z Microsoft Entra ID, i każdy inny stopień zależności od domeny:

Tryb	Co się dzieje	Wymaga reinstalacji istniejącego PC	Zależność od `dc01` / `dc02`
Entra registered	urządzenie (zwykle prywatne) dostaje tożsamość w Entra ID po dodaniu konta firmowego; droga dla BYOD, bez pełnego zarządzania komputerem	nie	brak
Entra hybrid joined	komputer jest jednocześnie w domenie i w pełni rozpoznany w Entra ID, zwykle przez synchronizację Entra Connect	zwykle nie, o ile już jest w domenie	tak, logowanie i część operacji wymaga łączności z kontrolerem domeny
Entra joined	komputer należy tylko do Entra ID, bez powiązania z domeną on premises	tak, istniejący komputer dołączony do domeny wymaga zresetowania Windowsa	brak

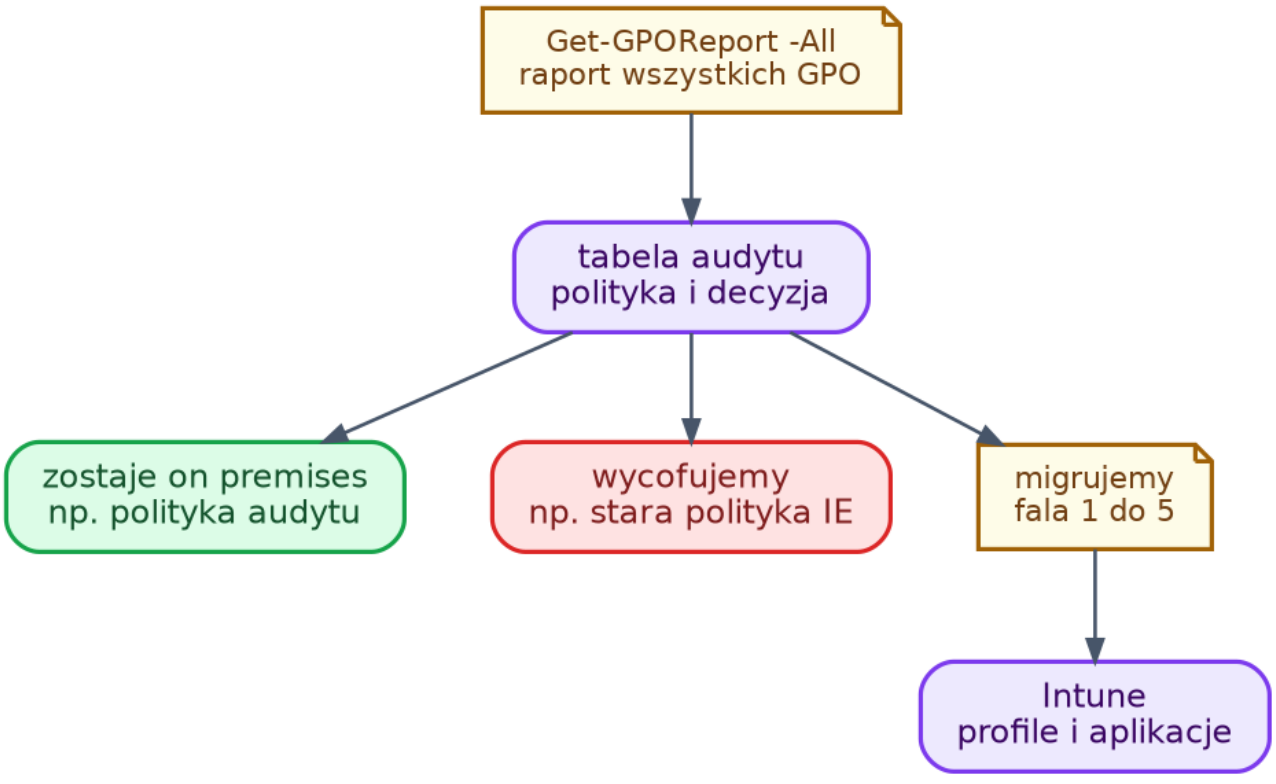


Rysunek. Trzy drogi do Entra ID: firmowy komputer w domenie przechodzi na hybrid join z automatyczną rejestracją MDM bez reinstalacji, nowy komputer dołącza do Entra ID przez Autopilot, a prywatne urządzenie jest tylko zarejestrowane i nie dostaje pełnego zarządzania (kliknięcie otwiera pełny rozmiar)

W Zielonej wybieramy `hybrid joined` z automatyczną rejestracją MDM przez GPO dla istniejącej floty: nie wymaga resetowania 180 komputerów naraz i daje pełne zarządzanie przez Intune. `Entra joined` (najlepiej przez Autopilot) zostaje wyborem dla nowych komputerów kupowanych od tej pory. `Entra registered` zostawiamy dla prywatnych telefonów i laptopów pracowników. Wcześniejsza wersja tej strony zalecała `Entra registered` dla floty; to była pomyłka, bo ta droga nie obejmuje komputera pełnym zarządzaniem.

Audyt GPO: metoda

Zamiast zgadywać, które z kilkudziesięciu GPO w domenie wciąż mają sens, przechodzimy przez pełny raport `Get-GPOReport -All` i każdą politykę przypisujemy do jednej z trzech grup, z uzasadnieniem, nie tylko z etykietą.



Raport wszystkich GPO trafia do tabeli audytu, z ktorej kazda polityka idzie do jednej z trzech decyzji (kliknięcie otwiera pełny rozmiar)

Polityka	Co robi	Decyzja	Dlaczego
Polityka haseł domeny	wymusza długość i złożoność hasła dla kont domenowych	zostaje on premises	konta domenowe i logowanie Kerberos wciąż istnieją, dopóki istnieje domena
Polityka audytu bezpieczeństwa	włącza logowanie zdarzeń logowania i zmian w AD	zostaje on premises	dotyczy samej domeny, nie stacji roboczych, Intune tego nie zastąpi
Instalacja oprogramowania (GPO Software Installation)	instaluje pakiety MSI przy starcie komputera z udziału sieciowego	migrujemy, fala 1	zależy od łączności z domeną przy każdym starcie, w Intune aplikacja instaluje się też poza siecią firmową
Stara polityka konfiguracji Internet Explorera	ustawia strony startowe i zabezpieczenia przeglądarki wycofanej z Windowsa	wycofujemy, fala 1	przeglądarka, której polityka dotyczy, już nie istnieje w obsługiwanych wersjach Windows
Autorejestracja certyfikatów użytkownika	prosi urząd certyfikacji `CA-Zielona` o certyfikat przy każdym logowaniu	migrujemy, fala 2	wymaga łączności z `dc01`, a komputery poza biurem łączą się przez zawodny VPN
Mapowanie dysków sieciowych działów	podłącza litery dysków do udziałów na `fs01`	migrujemy, fala 4	odtwarzalne skryptem logowania z Intune, ale nie jest pilne jak aplikacje i certyfikaty
Konfiguracja proxy przeglądarki	wymusza adres serwera proxy w ustawieniach systemowych	migrujemy, fala 3	prosty profil konfiguracyjny w Intune, korzyść z przeniesienia bez większego ryzyka

> Po przenosinach urzędu według strony Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona nowe certyfikaty wystawia `Zielona-CA01` na `ca01`, więc wszędzie, gdzie dziś ufamy tylko `CA-Zielona`, dokładamy zaufanie do `Zielona-Root-CA`.

Dlaczego instalacja aplikacji i autorejestracja certyfikatów schodzą z GPO najpierw

Obie polityki mają wspólną cechę: działają tylko wtedy, gdy komputer ma w danej chwili łączność z domeną, a nasz `AlwaysOn VPN` nie działa dziś niezawodnie na całej flocie. Komputer offline nie dostanie aktualizacji oprogramowania z GPO ani nie odnowi certyfikatu przy wygaśnięciu, i będzie tak działać do najbliższego podłączenia do sieci biurowej, czasem tygodniami. Intune instaluje aplikacje i odnawia certyfikaty przez internet, niezależnie od tego, czy komputer widzi akurat kontroler domeny, więc te dwie polityki idą do migracji w pierwszej kolejności, zanim zajmiemy się mniej pilnymi.

Plan migracji w pięciu falach

1. **Fala 1: aplikacje i porządki.** Migracja instalacji oprogramowania do Intune, usunięcie przestarzałej polityki Internet Explorera.
2. **Fala 2: certyfikaty.** Wybór między Certificate Connector a Cloud PKI (porównanie niżej) i migracja autorejestracji certyfikatów użytkownika.
3. **Fala 3: konfiguracja podstawowa.** Proxy, Wi-Fi, ustawienia przeglądarki i inne proste profile konfiguracyjne bez zależności od domeny.
4. **Fala 4: zasoby działowe.** Mapowanie dysków sieciowych, drukarki, skrypty logowania przeniesione na skrypty Intune uruchamiane przy logowaniu.
5. **Fala 5: zabezpieczenia i sprzątanie.** Migracja polityk Defendera i BitLockera do profili bezpieczeństwa punktu końcowego Intune, wyłączenie w pełni zmigrowanych GPO i końcowy przegląd tego, co świadomie zostaje on premises na stałe.

Certificate Connector kontra Cloud PKI

Kryterium	Certificate Connector	Cloud PKI
Gdzie działa urząd certyfikacji	on premises, dziś `AD CS` na `dc01`	w pełni w chmurze Microsoftu
Wymagana infrastruktura on premises	tak: serwer `NDES` plus zainstalowany łącznik Certificate Connector, oba z łącznością wychodzącą do Intune	żadna: bez serwera łącznika i bez własnego `AD CS`
Wykorzystuje istniejący urząd `CA-Zielona`	tak, to jego główna zaleta w Zielonej	nie, wymaga nowej hierarchii CA założonej w Intune

Kryterium	Certificate Connector	Cloud PKI
Zależność od łączności komputera z domeną przy odnawianiu	pośrednio tak: łącznik i `NDES` muszą widzieć `dc01`, choć sam klient łączy się przez SCEP z Intune	nie, cały przepływ certyfikatu idzie przez chmurę
Typowe zastosowanie	firmy z już działającym `AD CS`, które nie chcą budować nowego CA	wdrożenia od zera albo urządzenia bez żadnej łączności z siecią on premises

W Zielonej `AD CS` na `dc01` już działa i wydaje certyfikaty od lat, więc Certificate Connector pozwala odzyskać autorejestrację certyfikatów bez budowania nowego urzędu. Cloud PKI staje się bardziej naturalnym wyborem, gdyby docelowo domena on premises miała zniknąć całkiem, a nie tylko stracić część swoich dotychczasowych zadań: ta decyzja w Zielonej pozostaje otwarta do czasu zamknięcia fali 2.

Częste błędy

Objaw	Przyczyna	Co robimy
`dsregcmd /status` pokazuje `WorkplaceJoined : YES` i `AzureAdJoined : NO`, a komputer nie dostaje profili Intune	ktoś zrobił „Połącz” w ustawieniach konta, więc komputer jest tylko `Entra registered`, a hybrid join jeszcze nie przeszedł	usuwamy konto szkolne lub służbowe z ustawień, sprawdzamy synchronizację obiektu komputera w Entra Connect i GPO z automatyczną rejestracją MDM
Autorejestracja certyfikatów przestaje działać zaraz po pierwszej migracji z GPO	GPO wyłączone, zanim profil certyfikatu w Intune faktycznie doszedł do komputera	wyłączamy politykę GPO dopiero po potwierdzeniu, że nowy certyfikat z Intune faktycznie jest na komputerze
Audyt GPO trwa bardzo długo, bo trzeba ręcznie przeklikać dziesiątki polityk w konsoli	audyt liczony politykę po polityce w interfejsie graficznym zamiast masowym raportem	uruchamiamy `Get-GPOReport -All -ReportType Html` raz i czytamy jeden plik zamiast klikać po konsoli
Komputer po rejestracji w Entra ID prosi o dodatkowe logowanie przy każdym uruchomieniu aplikacji firmowej	użytkownik zalogował się do aplikacji lokalnym kontem Microsoft zamiast kontem pracy dodanym przy rejestracji	sprawdzamy w aplikacji, czy używane jest konto `imie.nazwisko@zielona.example`, nie prywatne konto Microsoft

□□ Ćwiczenia

1. Dlaczego w Zielonej wybieramy `hybrid joined` z GPO dla istniejącej floty 180 komputerów, a nie `Entra registered` ani od razu `Entra joined`?

Odpowiedź

`Entra joined` na komputerze, który już jest dołączony do domeny on premises, wymaga wyjścia z domeny i zwykle resetu Windowsa: przy 180 komputerach naraz to masowa, ryzykowna operacja. `Entra registered` jest drogą dla prywatnych urządzeń i nie daje pełnego zarządzania komputerem. `Hybrid joined` z automatyczną rejestracją MDM zostawia komputer w domenie i obejmuje go Intune bez reinstalacji, a `Entra joined` zostaje wyborem dla nowych komputerów.

1. Polityka mapowania dysków sieciowych trafia w naszym audycie do fali 4, a nie do fali 1 razem z instalacją oprogramowania. Jakim kryterium z tej strony to uzasadniamy?

Odpowiedź

Fala 1 obejmuje polityki, które zależą od stałej łączności z domeną i realnie psują się na komputerach korzystających głównie z zawodnego VPN, czyli instalację oprogramowania i autorejestrację certyfikatów. Mapowanie dysków sieciowych też korzysta z łączności domenowej, ale nie jest tak pilne: brak dostępu do udziału sieciowego jest od razu widoczny dla użytkownika i łatwy do obejścia ręcznie, więc migrujemy je później, gdy pilniejsze polityki są już bezpiecznie po drugiej stronie.

Powiązane: Windows LAPS: hasło lokalnego administratora w Active Directory · Entra Connect i Cloud Sync: synchronizacja ad.zielona.example z Entra ID · Skrypty audytowe Active Directory

Źródła: Microsoft Learn, „Join your cloud native endpoints to Microsoft Entra" · Microsoft Learn, „What is a Microsoft Entra hybrid joined device" · Microsoft Learn, „How Microsoft Entra device registration works" · Microsoft Learn, „Microsoft Cloud PKI for Microsoft Intune" · Microsoft Learn, „Types of certificate that are supported by Microsoft Intune" · `Get-Help Get-GPOReport`

Revision #29
Created 2026-09-28 06:15:02 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:51 UTC by Tomasz Konieczny