Intune: zarządzanie komputerami, które nie wracają do biura

Poziom: podstawy **Dotyczy: Microsoft Intune, Microsoft Entra ID, Windows 11**

Czas: ~15 min

Ta strona otwiera książkę o Intune: skąd wzięło się zarządzanie komputerami z chmury, czym różni się od zasad grupy w naszej domenie i dlaczego Zielona wdraża je właśnie teraz. Dalej idziemy stronami po kolei, od planu do certyfikatów.

Skróty użyte na tej stronie (9)

Skrót	Co znaczy
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
FAQ	Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
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
NT	pierwotnie kryptonim N-Ten, od procesora, dla którego system miał powstać; popularnie dziś odczytywane jako New Technology, choć to rozwinięcie nie jest oficjalne: rdzeń dzisiejszego Windows Server
PKI	Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów
SMS	Short Message Service: krótka wiadomość tekstowa na telefon, która dociera także bez internetu
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Skąd się wzięło

W 1994 roku Microsoft wypuścił Systems Management Server, w skrócie SMS, razem z Windows NT Server 3.5. Program robił to, czego potrzebuje każda firma z setką komputerów: rozsyłał oprogramowanie, zbierał spis sprzętu i programów, dokładał poprawki i pozwalał zdalnie przejąć pulpit. W 2007 roku zmieniono mu nazwę na System Center Configuration Manager, między innymi dlatego, że skrót SMS wszystkim kojarzył się już z wiadomościami tekstowymi w telefonie. Nazwa zmieniała się potem jeszcze dwa razy, aż do dzisiejszego Microsoft Configuration Manager, ale pomysł został ten sam: serwer w firmie, agent na każdym komputerze, administrator przy konsoli.

Równolegle od Windows 2000 działały zasady grupy (GPO), czyli ustawienia przechowywane w Active Directory, które komputer sam pobiera z kontrolera domeny przy starcie i logowaniu. Do roku 2010 firmowy komputer niemal zawsze siedział w biurowej sieci, więc obie metody działały bez zarzutu.

Potem komputery wyszły z biur. W 2011 roku Microsoft wprowadził Windows Intune (wersja testowa pojawiła się rok wcześniej): usługę, w której serwer zarządzający stoi w chmurze Microsoftu, a komputer łączy się z nim zwykłym internetem, skądkolwiek. W 2014 roku usługa dostała nazwę Microsoft Intune, bo nauczyła się też zarządzać telefonami i tabletami. W 2023 roku katalog użytkowników Azure Active Directory przemianowano na Microsoft Entra ID, a Intune sprzedaje się dziś w kilku wariantach: Plan 1, Plan 2 i Intune Suite.

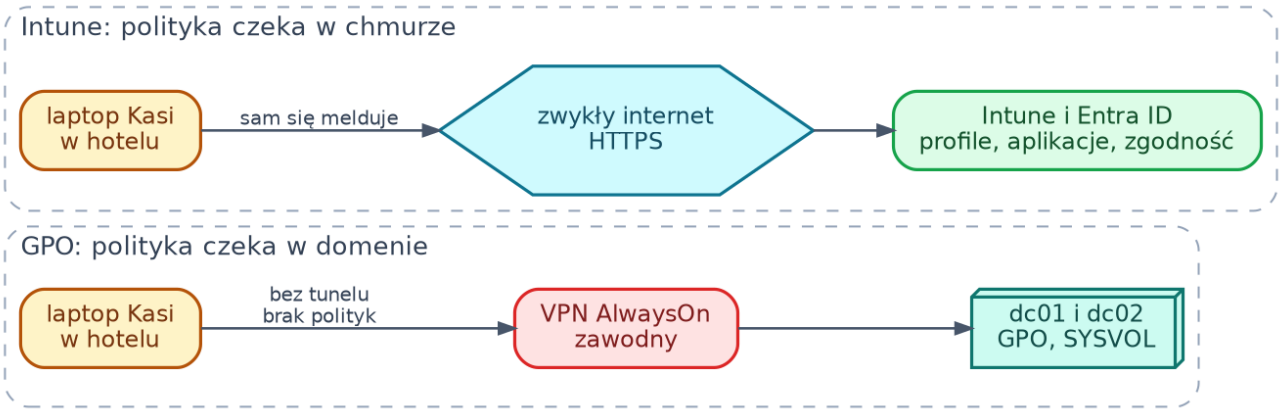
Jak to działa w jednym obrazku

> **Pojęcie: MDM.** Mobile Device Management, czyli zarządzanie urządzeniami przez usługę, do której urządzenie samo się zgłasza i pobiera z niej polecenia. Windows ma wbudowanego klienta MDM, więc nie instalujemy nic dodatkowego, żeby komputer zaczął słuchać Intune.

> **Pojęcie: Microsoft Entra ID.** Chmurowy katalog kont, grup i urządzeń. Intune opiera się na nim tak, jak zasady grupy opierają się na Active Directory: to z niego bierze informację, kto i jaki komputer należy do jakiej grupy.

> **Pojęcie: Intune.** Usługa w chmurze, która przechowuje profile, aplikacje i zasady zgodności i wydaje je komputerom zarejestrowanym w Entra ID.

Różnica między dwoma światami jest prosta: zasada grupy czeka w domenie, a polityka Intune czeka w chmurze.



Laptop w hotelu: zasady grupy wymagają tunelu do dc01, Intune wystarcza zwykły internet (kliknięcie otwiera pełny rozmiar)

Zasady grupy nie znikają. Domena `ad.zielona.example` dalej obsługuje logowanie, udziały na `fs01` i drukarki, a część polityk zostaje na stałe w GPO. Intune dokładamy obok i przenosimy tam to, co ma działać także wtedy, gdy komputer nie widzi biura. Szczegółowy podział polityk opisuje strona Intune obok domeny: audyt GPO i plan migracji.

Dlaczego Zielona

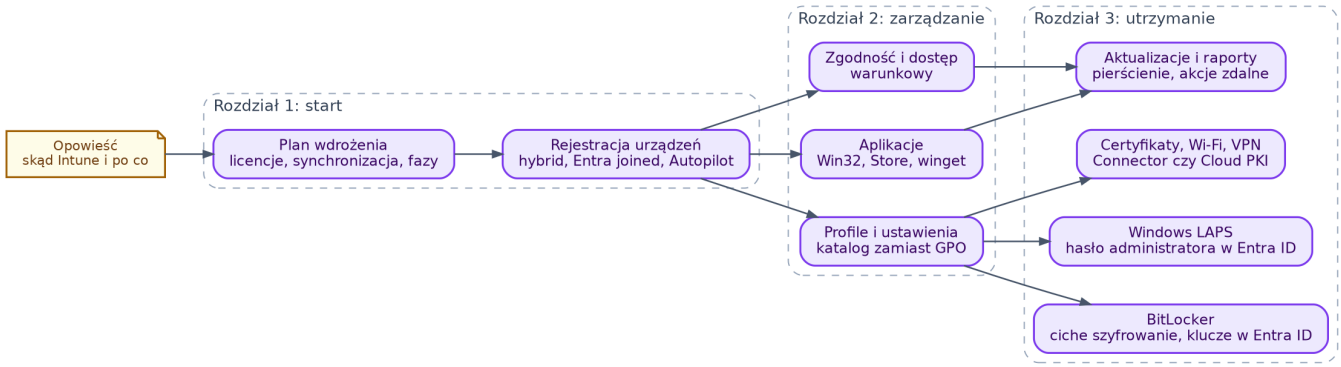
> **Z ŻYCIA WZIĘTE**
>
> Kasia jedzie na targi do Wrocławia. W hotelowej sieci VPN AlwaysOn łączy się raz na trzy próby, a tego dnia wcale. We wtorek po Patch Tuesday jej laptop nie ma nowej wersji programu do faktur, bo instalacja z GPO wymaga widoczności `dc01`, i nie ma odnowionego certyfikatu do VPN, bo jego autorejestracja też wymaga domeny. Kasia dzwoni do Tomka w środę o 8:10, a Tomek nie ma jak jej pomóc inaczej niż przez telefon.

To jest dokładnie ten problem, który rozwiązuje Intune: pięciu handlowców w terenie i sto kilkadziesiąt komputerów w Pamiątkowie i Swarzędzu, z których część widzi domenę rzadko albo wcale. Pan Zbigniew dorzuca swoje: wraca z urlopu z nowym laptopem i chce na nim pracować od razu, nie po dwóch dniach w serwerowni.

Plan Zielonej wygląda tak. Startujemy od Microsoft Entra ID, bo konta mamy już w domenie i wystarczy je zsynchronizować. Licencje bierzemy z pakietu Microsoft 365 Business Premium, w którym według dokumentacji są Intune Plan 1, Microsoft Entra ID P1 i Microsoft Defender for Business (skład sprawdzamy przy zakupie, bo pakiety się zmieniają). Istniejące komputery rejestrujemy bez reinstalacji, nowe od pierwszego włączenia konfiguruje Autopilot. Wdrażanie aplikacji i certyfikatów schodzi z GPO do Intune. Metody wydawania certyfikatów (Certificate

Connector z naszego AD CS albo Cloud PKI) jeszcze nie wybraliśmy, więc strona o certyfikatach porównuje obie.

Mapa tej książki



Mapa książki: opowieść, potem plan i rejestracja, następnie zgodność, profile i aplikacje, na końcu aktualizacje, certyfikaty, Windows LAPS i BitLocker (kliknięcie otwiera pełny rozmiar)

Rozdział	Strona	Na jakie pytanie odpowiada
1	Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy	Co kupujemy, co synchronizujemy i w jakiej kolejności obejmujemy działy
1	Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot	Jak komputer trafia pod zarządzanie i jak sprawdzamy, że trafił
2	Zasady zgodności i dostęp warunkowy	Jak sprawić, żeby poczta i SharePoint wpuszczały tylko zdrowe komputery
2	Profile konfiguracji: katalog ustawień zamiast GPO	Jak przenieść ustawienia z GPO, szyfrowanie, LAPS i zaporę
2	Aplikacje w Intune: Win32, Store, winget i zależności	Jak spakować i rozesłać program oraz co robić, gdy się nie instaluje
3	Aktualizacje Windows i raporty: pierścienie, Autopatch, zgodność floty	Jak rozłożyć poprawki w czasie i jak zdalnie naprawić komputer
3	Certyfikaty, Wi-Fi i VPN z Intune: Certificate Connector czy Cloud PKI	Skąd komputer w terenie bierze certyfikat i jak go używa
3	Windows LAPS z Intune: hasło lokalnego administratora w Entra ID albo AD	Jak każdy komputer dostaje inne hasło administratora, kto je czyta i jak przechodzimy z GPO
3	BitLocker z Intune: ciche szyfrowanie i klucze odzyskiwania w Entra ID	Jak szyfrujemy dyski bez pytań i skąd bierzemy klucz, gdy komputer zażąda odblokowania

Powiązane: Intune obok domeny: audyt GPO i plan migracji · Windows LAPS: hasło lokalnego administratora w Active Directory · BitLocker z kluczem odzyskiwania w Active Directory · AlwaysOn VPN: tunel użytkownika z ProfileXML

Źródła: en.wikipedia.org/wiki/Microsoft_Configuration_Manager · en.wikipedia.org/wiki/Microsoft_Intune · en.wikipedia.org/wiki/Group_Policy · Microsoft Learn, „Microsoft Intune licensing" (learn.microsoft.com/intune/intune-service/fundamentals/licenses) · Microsoft Learn, „Microsoft 365 Business Premium security FAQ" (learn.microsoft.com/microsoft-365/admin/security-and-compliance/m365bp-security-faq) · Microsoft Learn, „Add Defender Suite to Business Premium" (learn.microsoft.com/microsoft-365/admin/security-and-compliance/add-defender-suite-business-premium)

Revision #18
Created 2026-10-03 11:22:58 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:08 UTC by Tomasz Konieczny