Hotpatch i Autopatch — aktualizacje Windows 11 z Intune

Typ: procedura

Dotyczy: Windows 11 24H2+ (hotpatch: Enterprise/Education), Pro+ (polityki klienta Windows Update), Intune, współzarządzanie z ConfigMgr

Czas: ~60 min konfiguracji plus jeden pełny cykl pilotażu

Efekt: aktualizacjami maszyn objętych Intune steruje jedno źródło — polityki w Intune i Autopatch — a nie równolegle GPO Windows Update; pierścienie są ustawione świadomie, hotpatch jest włączony albo wyłączony z wyboru, a nie domyślnie; wiemy, które maszyny się do niego kwalifikują i skąd biuro pobierze bajty aktualizacji.

Skróty użyte na tej stronie (15)

Skrót	Co znaczy
AD	Active Directory: katalog kont, komputerów i zasad w domenie Windows
CHPE	Compiled Hybrid PE: binaria x86 przyspieszone kodem Arm64 w Windows na Arm
gMSA	group Managed Service Account: konto usługi z hasłem zarządzanym przez AD
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
HVCI	Hypervisor-protected Code Integrity: w interfejsie „Integralność pamięci”; sprawdza sterowniki przed jądrem
IoT	Internet of Things: urządzenia wbudowane i specjalizowane, np. kioski i terminale
LTSC	Long-Term Servicing Channel: wydanie z długim wsparciem i bez nowych funkcji
MCC	Microsoft Connected Cache: lokalny serwer podręczny treści Microsoftu
RAM	Random Access Memory: pamięć operacyjna
RBAC	Role-Based Access Control: uprawnienia przydzielane według ról
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
VBS	Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows

Skrót	Co znaczy
VDA	Virtual Desktop Access: licencja Windows na dostęp do pulpitów wirtualnych
WSL	Windows Subsystem for Linux: podsystem uruchamiający Linuksa w Windows
WSUS	Windows Server Update Services: lokalny serwer zatwierdzania i dystrybucji aktualizacji

Fiszka

□□ TYLKO ODCZYT

Czy maszyna kwalifikuje się do hotpatch

```
# polecenie pomocnicze; wymagania i klucz CHPE z dokumentacji Microsoftu (hotpatch)
$cv = Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion'
$dg = Get-CimInstance -Namespace root\Microsoft\Windows\DeviceGuard -ClassName
Win32_DeviceGuard
$mm = Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management' -ErrorAction SilentlyContinue
[pscustomobject]@{
    Edycja               = $cv.EditionID
    Wydanie              = $cv.DisplayVersion
    Kompilacja           = "$($cv.CurrentBuild).$($cv.UBR)"
    VBSDziala            = ($dg.VirtualizationBasedSecurityStatus -eq 2)
    Architektura         = $env:PROCESSOR_ARCHITECTURE
    HotPatchRestrictions = $mm.HotPatchRestrictions
}
```

Warunki hotpatch: Windows 11 **24H2 lub nowszy** na aktualnym baseline (kompilacja 28000, czyli 26H1, się nie kwalifikuje), **włączone VBS** — najczęstsza przyczyna, dla której urządzenia x64 odpadają — i zarządzanie przez Intune. Na `ARM64` dochodzi wyłączone CHPE, czyli `HotPatchRestrictions` = 1. Według Pureinfotech hotpatch działa tylko na edycjach Enterprise i Education; w dokumentacji Microsoftu tego zdania wprost nie znalazłem, więc `EditionID` = `Professional` traktujemy jako podejrzane, nie jako wykluczające. Urządzenie, które warunków nie spełnia, po prostu dostaje zwykłą aktualizację zbiorczą.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
Edycja               : Enterprise
Wydanie              : 25H2
Kompilacja           : 26200.9550
VBSDziala            : True
Architektura         : AMD64
HotPatchRestrictions :
```

CHPE = Compiled Hybrid PE: binaria x86 przyspieszone kodem Arm64 w Windows na Arm · **VBS** = Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows

TYLKO ODCZYT

Czy maszynę obejmuje też GPO Windows Update: gpresult

```
# polecenie pomocnicze
gpresult /scope computer /r
```

Szukamy w wyniku GPO konfigurujących Windows Update (Konfiguracja komputera → Szablony administracyjne → Składniki systemu Windows → Windows Update → Manage updates offered from Windows Update). Maszyna hybrydowa, którą obejmuje jednocześnie takie GPO i profil aktualizacji w Intune, ma dwa źródła prawdy; ustawienie `ControlPolicyConflict/MDMWinsOverGP` rozstrzyga konflikt tylko dla części polityk, więc na nim nie polegamy.

GPO = Group Policy Object: obiekt zasad grupy w Active Directory

TYLKO ODCZYT

Skąd maszyna pobiera aktualizacje: Delivery Optimization

```
# polecenia pomocnicze
Get-DeliveryOptimizationStatus
Get-DeliveryOptimizationPerfSnap
```

Pierwsze polecenie pokazuje bieżące i niedawne pobrania, drugie — podsumowanie: ile bajtów przyszło z internetu, ile od innych komputerów w sieci, ile z serwera pamięci podręcznej. Delivery Optimization obsługuje pobrania Windows Update, Sklepu, aplikacji Win32 z Intune, Microsoft 365 Apps i Defendera, a od wersji 25122.1415.3698.6812 także Teams. Jeśli w biurze stoi Microsoft Connected Cache, tu widać, czy maszyny faktycznie z niego korzystają.

Nazwy, licencje i warunki

1 kwietnia 2025 „Windows Update for Business” przemianowano na **polityki klienta Windows Update** (Windows Update client policies); dokumentacja z lat 2021–2024 używa starej nazwy. Usługa wdrożeniowa i raporty weszły do marki **Windows Autopatch** w Intune (zakładki Update Policies, Update Groups, Update Status, Update Reports), a opóźnienie raportów spadło z ponad doby do najwyżej czterech godzin. Same polityki klienta są bezpłatne, działają w Pro, Pro for Workstations, Education i Enterprise (w tym LTSC i IoT) i dają **odroczenie aktualizacji funkcji do 365 dni, jakościowych do 30 dni, wstrzymanie do 35 dni**, terminy z okresem karencji i kanały przedpremierowe.

Warunek	Autopatch (stan na IX 2026)	Hotpatch
Licencje	Microsoft 365 Business Premium; Windows Education A3/A5; Windows Enterprise E3/E5 (także w M365 F3/E3/E5); Windows Enterprise E3/E5 VDA — od IV 2025 bez osobnej aktywacji funkcji	Windows 11 Enterprise E3/E5, Microsoft 365 F3, Windows 11 Education A3/A5, Microsoft 365 Business Premium, Windows 365 Enterprise
Dodatkowo	Entra ID P1/P2 i Intune; Entra ID jako źródło tożsamości albo synchronizacja z AD aktualnym Entra Connect; Entra hybrid join wspierany	zarządzanie przez Intune, polityka aktualizacji jakościowych z hotpatch = Allow albo ustawienie tenantowe
System i edycja	Windows 10/11 Pro, Education, Enterprise, Pro Education, Pro for Workstations, IoT Enterprise; kanał ogólny; LTSC tylko w zakresie aktualizacji jakościowych	Windows 11 24H2+ na aktualnym baseline, nie 26H1; VBS włączone; na Arm64 wyłączone CHPE; według prasy — Enterprise/Education
ConfigMgr	obciążenia „Windows Update policies” i „Device configuration” na Intune albo Pilot Intune	jw.
Tylko E3+ i F3	zgłoszenia serwisowe do zespołu Autopatch (Service Engineering Team)	—

Wszystkie uprawnione licencje dostają w Autopatch: RBAC, pierścienie, Autopatch groups, polityki jakościowe (cel: co najmniej 95% urządzeń na najnowszej), hotpatch, wielofazowe aktualizacje funkcji, sterowniki i firmware, Microsoft 365 Apps (cel: co najmniej 90% na Monthly Enterprise Channel), Edge, Teams, raporty i alerty. Od 2025 roku Autopatch nie jest usługą, w której Microsoft przejmuje tenanta, tylko zestawem funkcji w Intune — grupy i fazy ustawia administrator. Pierwotny model, w którym system sam wstrzymywał albo wycofywał wdrożenie w pierścieniach Test → First → Fast → Broad, budził zarzut oddania kontroli nad tym, kiedy i co zostanie zainstalowane (analitycy Tanium); w obecnym kształcie ten zarzut stracił część ostrza. Ocena autora, niepotwierdzona źródłowo: dla średniej firmy różnica między Autopatch a ręcznie zrobionymi pierścieniami w Intune jest w 2026 roku głównie różnicą raportowania i automatyzacji grup.

> Przy Business Premium hotpatch oznaczałby w praktyce aktywację subskrypcyjną do Enterprise — jeśli prawdziwe jest zdanie Pureinfotech, że hotpatch działa tylko na Enterprise i Education. Żadnego z tych dwóch zdań nie ma wprost w dokumentacji Microsoftu; rozstrzygamy to na pilotażu, a nie na papierze.

Jak działa hotpatch

Miesiąc	Co przychodzi	Restart
styczeń, kwiecień, lipiec, październik	**baseline** — pełna aktualizacja zbiorcza	tak
pozostałe dwa miesiące każdego kwartału	**hotpatch** — wyłącznie poprawki bezpieczeństwa	nie
dowolny miesiąc, poza planem	nieplanowany baseline, gdy poprawki nie da się zastosować „na gorąco”	tak

Czyli **cztery planowe restarty bezpieczeństwa rocznie zamiast dwunastu**; Microsoft: „przez osiem miesięcy z dwunastu nie trzeba restartować urządzenia, żeby aktualizacja zabezpieczeń zadziałała”. Poprawki niezwiązane z bezpieczeństwem i nowe funkcje przychodzą tylko w baseline'ach. Ogólna dostępność: x64 (Intel i AMD) od 2 kwietnia 2025, Arm64 od lipca 2025.

> **Pojęcie: hotpatch domyślnie włączony (MC1248388).** Od majowej aktualizacji zabezpieczeń 2026 Autopatch włącza hotpatch dla wszystkich kwalifikujących się urządzeń Intune. Ustawienie tenantowe „When available, apply updates without restarting the device ('Hotpatch')” jest w Intune → Tenant admin → Windows Autopatch → Tenant Management → Tenant settings, domyślnie Allow, i obowiązuje **tylko dla urządzeń bez przypisanej polityki aktualizacji jakościowych** — polityka urządzenia ma pierwszeństwo; można je wyłączyć dla całego tenanta. Microsoft uzasadnia zmianę tym, że urządzenia zabezpieczają się średnio o trzy do pięciu dni szybciej.

Zanim zaczniemy

Sprawdzamy licencje i edycje z tabeli wyżej, a na próbce maszyn — kartę gotowości z Fiszki. Decyzja „hotpatch-ready” to w praktyce decyzja o VBS i HVCI na całej flocie, a VBS ma dwa koszty: wydajnościowy (opisany na stronie serii o Windows 11) i domenowy — Credential Guard z Machine Identity Isolation, patrz Machine Identity Isolation po KB5124008.

Wydzielamy grupę pilotażową, a obok niej grupę maszyn krytycznych, które dostaną maksymalne odroczenie. Nawet w firmie na trzydzieści maszyn: pilotaż, grupa właściwa, grupa krytyczna. Laptopy ze Snapdragonem X2 i wydaniem 26H1 idą do osobnej grupy — nie dostaną hotpatch i nie przejdą do 26H2.

Robimy kopię zapasową GPO Windows Update, które za chwilę odepniemy (polecenie pomocnicze, moduł GroupPolicy):

```
# katalog docelowy musi istnieć przed wykonaniem kopii
Backup-GPO -Name "Windows Update - stacje" -Path C:\GPOBackup
```

Przebieg

1. Współzarządzanie: obciążenia na Intune

W konsoli Configuration Manager przełączamy obciążenia **„Windows Update policies”** i **„Device configuration”** na Intune albo na Pilot Intune dla kolekcji pilotażowej. To warunek Autopatch i jedyny sposób, żeby ConfigMgr i Intune się nie nadpisywały.

2. Odpięcie GPO Windows Update od maszyn objętych Intune

◫◫ ZMIENIA SYSTEM

Usunięcie powiązania GPO Windows Update z jednostką organizacyjną

```
# polecenie pomocnicze; moduł GroupPolicy
Remove-GPLink -Name "Windows Update - stacje" -Target "OU=Pilotaz-
Intune,OU=Stacje,DC=firma,DC=local"
# na maszynie z pilotażu:
gpupdate /force
gpresult /scope computer /r
```

Maszyny pilotażowe przenosimy do osobnej jednostki organizacyjnej i odpinamy od niej GPO Windows Update — zamiast kasować GPO, które nadal obsługuje resztę floty. Uwaga na

dziedziczenie: `Remove-GPLink` usuwa wyłącznie powiązanie ustawione bezpośrednio na wskazanej jednostce. Jeśli GPO jest podpięte wyżej (np. do `OU=Stacje` albo do domeny), pilotażowa jednostka pod spodem nadal je dziedziczy, a polecenie zakończy się błędem braku powiązania — wtedy albo tworzymy jednostkę pilotażową poza gałęzią, do której GPO jest podpięte, albo w filtrowaniu zabezpieczeń GPO odbieramy grupie maszyn pilotażowych prawo „Zastosuj zasady grupy” (w konsoli GPMC, na zakładce Delegowanie → Zaawansowane). Blokowania dziedziczenia nie używamy, bo odcina też wszystkie inne GPO z góry. Po `gpupdate` sprawdzamy w `gpresult`, że GPO zniknęło z listy zastosowanych. Na tych maszynach jedynym źródłem ustawień aktualizacji jest od teraz Intune.

□□ **GPO** = Group Policy Object: obiekt zasad grupy w Active Directory

3. Pierścienie i Autopatch groups

W Intune tworzymy Update rings i Feature update policy albo — jeśli licencja pozwala — Autopatch groups, które robią to samo z automatycznym przydziałem urządzeń. Docelowa wersja: **25H2** dla maszyn 24H2 Home/Pro przed 13 października 2026 (pakiet włączający, jeden restart) i dla maszyn 23H2 Enterprise/Education przed 10 listopada 2026 (pełna aktualizacja). Odroczenia mieszczą się w limitach: funkcje do 365 dni, jakościowe do 30, wstrzymanie do 35. Grupa krytyczna dostaje najdłuższe odroczenie jakościowe, pilotaż — zero.

4. Hotpatch: polityka i ustawienie tenantowe

W polityce aktualizacji jakościowych dla grup, które mają dostawać hotpatch, ustawiamy „When available, apply without restarting the device ("Hotpatch")” = Allow; dla grup, które nie mają go dostawać, tworzymy politykę bez tej zgody. Następnie w Intune → Tenant admin → Windows Autopatch → Tenant Management → Tenant settings podejmujemy decyzję dla ustawienia tenantowego: domyślne Allow obejmuje każde kwalifikujące się urządzenie **bez przypisanej polityki jakościowej**. Kto chce, żeby hotpatch trafiał wyłącznie tam, gdzie go przypisał, wyłącza ustawienie tenantowe albo pilnuje, żeby każde urządzenie miało politykę.

5. Arm64: wyłączenie CHPE

□□ ZMIENIA SYSTEM

HotPatchRestrictions = 1 na urządzeniach Arm64

```
# klucz i wartość z dokumentacji Microsoftu (hotpatch)
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management' `
    -Name HotPatchRestrictions -Value 1 -Type DWord
Restart-Computer
```

Hotpatch nie serwisuje binariów w `%SystemRoot%\SyChpe32`, dlatego na Arm64 wymaga wyłączenia CHPE — czyli spowolnienia 32-bitowych aplikacji x86, żeby uniknąć restartów. Na flocie zamiast rejestru można użyć polityki CSP `System/DisableCHPE`, którą dokumentacja hotpatch wskazuje jako alternatywę; flagę ustawia się raz. To decyzja per grupa urządzeń: na laptopach, na których użytkownicy korzystają głównie z aplikacji natywnych Arm64 albo x64, zysk z hotpatch przeważa; tam, gdzie kluczowa aplikacja jest 32-bitowa x86, sprawdzamy jej wydajność na pilotażu. Zmiana wymaga restartu.

CHPE = Compiled Hybrid PE: binaria x86 przyspieszone kodem Arm64 w Windows na Arm

6. Lokalne źródło bajtów: Delivery Optimization i Connected Cache

Microsoft Connected Cache for Enterprise and Education (MCC), ogólnie dostępny od lipca 2025, to programowy serwer podręczny treści Microsoftu w sieci firmowej, zarządzany z portalu Azure albo z wiersza poleceń. Buforuje aktualizacje funkcji i jakościowe, Microsoft 365 Apps, aplikacje z Intune i Sklepu oraz sygnatury Defendera; obsługuje Autopilot, klientów współzarządzanych i urządzenia tylko-Intune. To następca WSUS jako lokalnego ***źródła bajtów*** — nie zatwierdzeń, które przechodzą do polityk w Intune.

Wymaganie MCC	Stan na IX 2026
Host Windows	Windows 11 (kompilacja co najmniej 22631.3296), Windows Server 2022 (co najmniej 20348.2227) i 2025 — przez WSL 2; konto usługi gMSA, lokalne albo domenowe
Host Linux	Ubuntu Server 24.04; RHEL 8.x lub 9.x z silnikiem **Moby zamiast domyślnego Podmana**; **RHEL 10 nie jest na liście**
Sprzęt	od 4 rdzeni, 8 GB RAM i 100 GB (oddział, 10–50 urządzeń) do 16 rdzeni, 32 GB i dwóch dysków 200–500 GB (500–5 000 urządzeń)
Sieć	porty 80 i 443 przychodzące i wychodzące; jedna karta sieciowa na host

Wymaganie MCC	Stan na IX 2026
Licencja	Windows Enterprise E3/E5 (w M365 F3/E3/E5), Education A3/A5, Windows Enterprise per device; subskrypcja Azure pay-as-you-go potrzebna do utworzenia zasobu, bez obciążenia — **Business Premium na liście nie ma**

Obok istnieją osobne MCC w Configuration Manager (na punkcie dystrybucji) i MCC dla operatorów. Redmondmag pisał o dostępności „bez dodatkowych kosztów” także dla Pro, co jest sprzeczne z dokumentacją — trzymamy się dokumentacji.

> **WSUS jest przestarzały, a nie wyłączony.** We wrześniu 2024 Microsoft wpisał go na listę funkcji „no longer actively developed” przy Windows Server 2025, a planowane na 18 kwietnia 2025 wyłączenie synchronizacji sterowników 7 kwietnia 2025 odłożono bezterminowo. WSUS działa i dostaje treści — zostawiamy go dla maszyn spoza Intune i utrzymujemy według strony WSUS — czyszczenie i utrzymanie.

Weryfikacja

W Intune, w zakładkach Autopatch Update Status i Update Reports, maszyny pilotażowe raportują się z opóźnieniem najwyżej czterech godzin. W miesiącu hotpatch (poza styczniem, kwietniem, lipcem i październikiem) maszyny z grupy hotpatch instalują poprawkę bezpieczeństwa bez żądania restartu — lokalnie sprawdzamy to przez historię aktualizacji i stan oczekującego restartu, jak na stronie Windows Update z wiersza poleceń (`Get-WUHistory`, `Get-WURebootStatus`). Maszyny z `VBSDziala` = `False` w karcie gotowości dostają zwykłą aktualizację zbiorczą z restartem — to zachowanie oczekiwane, nie błąd. `gpresult` na maszynach pilotażowych nie pokazuje GPO Windows Update.

Wycofanie zmian

Hotpatch wyłączamy w polityce aktualizacji jakościowych danej grupy albo dla całego tenanta w ustawieniach tenantowych Autopatch; kolejne miesiące przychodzą wtedy jako zwykłe aktualizacje zbiorcze. Na Arm64 ustawiamy `HotPatchRestrictions` = `0` (tak opisuje to dokumentacja hotpatch) i restartujemy — to ponownie włącza CHPE i przywraca stan sprzed kroku 5.

GPO Windows Update przywracamy, podpinając je z powrotem do jednostki organizacyjnej (`New-GPLink -Name "Windows Update - stacje" -Target "OU=…"`, polecenie pomocnicze) albo odtwarzając z kopii (`Restore-GPO`). Obciążenia współzarządzania przełączamy z powrotem na ConfigMgr w jego konsoli. Nie zostawiamy maszyny w stanie pośrednim, w którym obie strony konfigurują Windows

Update.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
Maszyna nie dostaje hotpatch, tylko zwykłą aktualizację zbiorczą	VBS wyłączone, wydanie 26H1, maszyna nie jest na aktualnym baseline albo — według prasy — edycja Pro	karta gotowości z Fiszki; włączenie VBS i HVCI, doprowadzenie do bieżącego baseline, edycja Enterprise
Arm64 z hotpatch = Allow nadal restartuje co miesiąc	CHPE nie jest wyłączone	krok 5
Restart mimo hotpatch w lutym, maju, sierpniu albo listopadzie	nieplanowany baseline — poprawki nie dało się zastosować „na gorąco”	zachowanie zgodne z dokumentacją; restart zgodnie z terminem z polityki
Hotpatch pojawił się na maszynach, na których nikt go nie włączał	ustawienie tenantowe domyślnie Allow od V 2026, urządzenie bez polityki jakościowej	krok 4: polityka dla grupy albo wyłączenie ustawienia tenantowego
Ustawienia aktualizacji „skaczą” między wartościami	GPO Windows Update i Intune konfigurują tę samą maszynę	krok 2; nie polegamy na `MDMWinsOverGP`
Konflikt ConfigMgr i Intune przy Autopatch	obciążenie „Windows Update policies” nie jest na Intune	krok 1
Laptop ze Snapdragonem X2 nie przechodzi na 26H2	26H1 bazuje na innym rdzeniu Windows i nie ma ścieżki do kolejnej aktualizacji funkcji	zachowanie zgodne z dokumentacją; osobna grupa urządzeń
MCC nie instaluje się na RHEL	domyślny Podman zamiast Moby albo RHEL 10	Moby na RHEL 8 lub 9; RHEL 10 nie jest wspierany — Ubuntu Server 24.04 albo Windows z WSL 2

Powiązane: Windows 11 w firmie 2026 — przegląd zmian · Windows Update z wiersza poleceń · Standardowa aktualizacja systemu produkcyjnego (Windows) · WSUS — czyszczenie i utrzymanie · Machine Identity Isolation po KB5124008

Źródła: Windows Update client policies · Windows Autopatch overview · Autopatch prerequisites · Hotpatch updates · MC1248388 · Peter van der Woude — hotpatch domyślnie · Securing devices faster with hotpatch updates on by default · Pureinfotech — edycje · Petri — zmiana nazwy WUfB · Petri — hotpatch na Arm64 · BleepingComputer — WSUS · What's new in Delivery Optimization · MCC overview · MCC prerequisites · MCC FAQ · Redmondmag — MCC

Revision #2
Created 2026-09-27 17:44:19 UTC by Tomasz Konieczny
Updated 2026-09-27 17:44:31 UTC by Tomasz Konieczny