Aktualizacje Windows i raporty: pierścienie, Autopatch, zgodność floty

Poziom: średniozaawansowany

Dotyczy: Intune, Windows Update for Business, Windows Autopatch, Windows 11

Czas: ~50 min

Intune nie instaluje poprawek sam, tylko mówi komputerom, kiedy i jak mają je pobrać z Windows Update. Strona pokazuje pierścienie aktualizacji, polityki funkcji i sterowników, hotpatch i Autopatch (z wymaganiami licencyjnymi), raporty oraz zdalne akcje na komputerze: Sync, wipe, retire i fresh start.

Skróty użyte na tej stronie (9)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
ASAP	As Soon As Possible: jak najszybciej, nazwa trybu udostępniania aktualizacji funkcji bez czekania na wybraną datę
BYOD	Bring Your Own Device: pracownik używa prywatnego urządzenia do pracy
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
MDM	Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi
OOBE	Out-of-Box Experience: ekrany pierwszego uruchomienia Windows, na których komputer dołącza się do Entra ID i dostaje konfigurację z Autopilot
VBS	Virtualization-Based Security: zabezpieczenia oparte na wirtualizacji, jeden z wymogów hotpatch w Windows 11
WSUS	Windows Server Update Services: firmowy serwer aktualizacji Windows

Fiszka

Ścieżki w centrum administracyjnym podajemy po angielsku, tak jak w dokumentacji. Menu aktualizacji bywa opisane na dwa sposoby: Devices, Windows updates albo Devices, By platform, Windows, Manage updates, Windows updates. To ta sama część Intune, więc szukamy po nazwie. Komendy wykonujemy w PowerShellu na komputerze.

□□ KLIKAMY W INTERFEJSIE

Utworzenie pierścienia aktualizacji: Update rings

```
Microsoft Intune admin center → Devices → By platform → Windows → Manage updates →
Windows updates
→ zakładka Update rings → Create profile
→ Basics: nazwa, np. Pierscien-Pilot
→ Update ring settings → Assignments: grupa urządzeń → Review + create
```

Pierścień przypisujemy grupom urządzeń, nie użytkowników, bo wtedy polityka działa bez czyjegokolwiek logowania.

□□ ZMIENIA SYSTEM

Ustawienie odroczeń i terminów: Update ring settings

```
Update ring settings → Update settings
→ Quality update deferral period (days): 0 do 30
→ Feature update deferral period (days): zostawiamy 0, wersją steruje polityka funkcji
→ Microsoft product updates: Allow
→ Windows drivers: Allow albo Block

Update ring settings → User experience settings
→ Automatic update behavior: Auto install and restart at a scheduled time
→ Scheduled install day / Scheduled install time
→ Active hours start / Active hours end
→ Use deadline settings: Allow
→ Deadline for quality updates: 2 do 30 dni
→ Grace period: 0 do 7 dni
→ Auto reboot before deadline: Yes albo No
```

Ustawienie Automatic update behavior ma też wartości: Notify download, Auto install at maintenance time, Auto install and restart at maintenance time i Auto install and reboot without end-user control. Wartości dla poszczególnych pierścieni Zielonej podajemy w tabeli niżej.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Update ring settings pierścienia Pierscien-Krytyczny, widoczne Quality update deferral period (days): 14, Deadline for quality updates: 5, Grace period: 2 i Auto reboot before deadline: No.

ZMIENIA SYSTEM

Utworzenie polityki aktualizacji funkcji: Feature updates

```
Microsoft Intune admin center → Devices → Windows → Windows updates → Feature updates → Create profile
→ Deployment settings: Name, Feature update to deploy: wersja Windows 11
→ Update availability: Make available as Required (wymusza instalację)
→ Rollout options: Make update available as soon as possible / on a specific date / gradually
→ Assignments: grupa urządzeń
```

Polityka funkcji przypina komputery do wskazanej wersji i trzyma je na niej do chwili zmiany polityki, ale nie obniża wersji, jeśli komputer jest już nowszy. Wersja Optional (użytkownik sam wybiera) wymaga licencji Windows Autopatch, wersja Required nie.

KLIKAMY W INTERFEJSIE

Włączenie hotpatch w polityce aktualizacji jakościowych: Quality updates

```
Microsoft Intune admin center → Devices → Windows updates → Quality updates tab
→ Create → Windows quality update policy
→ Settings: When available, apply without restarting the device ('Hotpatch'): Allow
→ Assignments → Create
```

Hotpatch instaluje poprawki bez restartu w miesiącach, które nie są miesiącami bazowymi. Wymaga komputerów z Windows 11 w wersji 24H2 lub nowszej, włączonego VBS

(zabezpieczeń opartych na wirtualizacji) i zarządzania przez Intune. Szczegóły i licencje w sekcji niżej.

VBS = Virtualization-Based Security: zabezpieczenia oparte na wirtualizacji, jeden z wymogów hotpatch w Windows 11

KLIKAMY W INTERFEJSIE

Wstrzymanie, wznowienie i wydłużenie pierścienia: Pause, Resume, Extend

```
Devices → By platform → Windows → Manage updates → Windows updates → Update rings
→ wybieramy pierścień → Pause / Resume / Extend / Uninstall / Delete
```

Pause chwilowo wstrzymuje instalację poprawek z tego pierścienia, Extend przedłuża terminy, Uninstall usuwa poprawki, a Delete przestaje wymuszać ustawienia pierścienia. Wstrzymanie to nasz zawór bezpieczeństwa, gdy po Patch Tuesday okaże się, że poprawka psuje kluczowy program.

TYLKO ODCZYT

Sprawdzenie poprawek zainstalowanych na komputerze: Get-HotFix

```
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5 HotFixID,
Description, InstalledOn
cmd /c ver
```

Pierwsza komenda pokazuje pięć ostatnich poprawek, druga numer wersji systemu.

Przykład:

```
HotFixID  Description      InstalledOn
--------  -----------      -----------
KB5000001 Security Update  14.10.2026 00:00:00
```

KLIKAMY W INTERFEJSIE

Sprawdzenie, skąd komputer bierze polityki aktualizacji: Configured update policies

```
Settings → Windows Update → Advanced options → Configured update policies
→ typ polityki: Mobile Device Management (nie Group Policy)
```

```
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\PolicyManager\current\device\Update"
gpresult /h C:\Temp\gpo.html
```

Intune zapisuje ustawienia aktualizacji w gałęzi rejestru `PolicyManager\current\device\Update`. Jeśli polityka na komputerze ma typ Group Policy, albo `gpresult` pokazuje GPO z ustawieniem WSUS, to GPO nadpisuje pierścień.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **WSUS** = Windows Server Update Services: firmowy serwer aktualizacji Windows · **HKLM** = HKEY_LOCAL_MACHINE: gałąź rejestru Windows z ustawieniami całego komputera, a nie pojedynczego użytkownika · **gpresult** = group policy result: które GPO trafiły na komputer

KLIKAMY W INTERFEJSIE

Odczyt zdarzeń aktualizacji w dzienniku systemu: WindowsUpdateClient

```
Event Viewer → Applications and Services Logs → Microsoft → Windows →
WindowsUpdateClient
Event Viewer → Applications and Services Logs → Microsoft → Windows
→ DeviceManagement-Enterprise-Diagnostics-Provider → Admin
```

Pierwszy dziennik opisuje samo pobieranie i instalację poprawek, drugi dostarczenie polityk z Intune.

ZMIENIA SYSTEM

Przegląd raportów aktualizacji: Reports, Windows updates

```
Microsoft Intune admin center → Reports → Windows updates
→ Per update ring deployment state
→ Windows 10 and later feature updates
→ Feature update policies with alerts
→ Expedited quality update policies with alerts
→ Driver update policies with alerts
```

Dla pojedynczego pierścienia widok Update rings → wybrany pierścień pokazuje trzy raporty: Device and user check-in status, Device assignment status i Per setting status.

□□ TYLKO ODCZYT

Przegląd raportów zgodności floty: Reports, Device compliance

```
Microsoft Intune admin center → Reports → Device compliance
→ Noncompliant devices
→ Devices without compliance policy
→ Setting compliance
→ Windows hardware attestation report

Microsoft Intune admin center → Reports → Device configuration
→ Device encryption status
→ Profile configuration status
```

Każdy raport można wyeksportować, a eksport zachowuje filtry i wyszukiwanie. Raport Noncompliant devices z filtrem systemu Windows i frazą z nazwy komputerów da nam listę do rozesłania do działów.

□□ KLIKAMY W INTERFEJSIE

Wykonanie zdalnej akcji na komputerze: All devices

```
Microsoft Intune admin center → Devices → All devices → wybrany komputer
→ pasek akcji: Sync / Restart / Retire / Wipe / Fresh Start / Autopilot reset
→ ... → Rotate BitLocker keys / Rotate Local admin password / Collect diagnostics / Run remediation
→ Quick Scan / Full Scan / Update Windows Defender security intelligence
```

Akcje zbiorcze (Bulk device actions w Devices, All devices) obejmują Autopilot reset, Collect diagnostics, Delete, Rename, Restart, Retire, Sync i Wipe dla najwyżej 100 urządzeń naraz.

□□ KLIKAMY W INTERFEJSIE

Wybór opcji Wipe: Wipe

```
Wipe → opcje:
→ (bez opcji): przywraca ustawienia fabryczne, usuwa dane, ustawienia i polityki MDM
→ Wipe device, but keep enrollment state and associated user account
→ Wipe device, and continue to wipe even if device loses power
```

Ostatnia opcja może doprowadzić do urządzenia, które nie startuje, więc używamy jej tylko na komputerach firmowych, gdy zależy nam na bezpowrotnym usunięciu danych (np. po kradzieży). Bez opcji, przerwana operacja próbuje wrócić do stanu sprzed wipe, a gdy się nie uda, komputer może być bezużyteczny.

Z życia wzięte

Z ŻYCIA WZIĘTE

Środa 28 października, 7:50, pierwszy z trzech dni zamknięcia miesiąca. Windows na komputerach księgowości restartuje się po terminie ostatecznym instalacji poprawki z 13 października, bo pierścień Krytyczny ma te same terminy co pierścień Szeroki. Pani Halina ma w Optimie otwarte rozliczenie, zapisuje je w ostatniej chwili i dzwoni do Tomka z jedną prośbą: „nie w tym tygodniu". Tomek przestawia dla pierścienia Krytyczny Auto reboot before deadline na No, ustala restart nocą w niedzielę i wpisuje zamknięcia miesiąca do kalendarza zmian.

Jak to działa

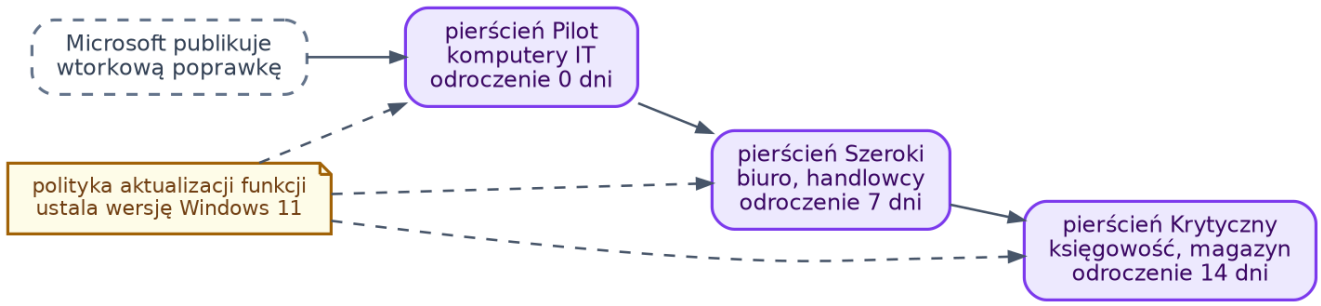
Rozwiń: jak to działa pod spodem

Pojęcie: Windows Update for Business. Mechanizm w Windows, który pozwala sterować tym, kiedy komputer pobiera poprawki z serwerów Microsoftu: odroczeniami, terminami, godzinami aktywności. Intune jest tylko panelem do ustawiania tych zasad, nie hostuje poprawek. Komputer pobiera je bezpośrednio z Windows Update.

Pojęcie: pierścień aktualizacji. Zestaw ustawień (odroczenia, terminy, zachowanie restartu) przypisany grupie komputerów. Różne grupy dostają poprawki o różnych

porach, więc ewentualna wadliwa poprawka najpierw dotknie niewielkiej grupy.

Pojęcie: polityka aktualizacji funkcji. Osobna polityka, która wskazuje wersję Windows (np. wersja Windows 11), na której komputery mają być. Nadpisuje odroczenia funkcji z pierścienia, więc trzymamy je w jednym miejscu. Dokumentacja radzi, żeby przy polityce funkcji nie używać odroczeń funkcji w pierścieniu, a pierścień zostawić tylko do ustawień doświadczenia użytkownika.



Poprawka Microsoftu trafia najpierw do pierścienia Pilot, potem Szeroki, potem Krytyczny, a polityka aktualizacji funkcji wskazuje wersję Windows dla wszystkich (kliknięcie otwiera pełny rozmiar)

Pierścienie w Zielonej

Poniższe wartości to propozycja startowa w zakresach, które pozwala ustawić Intune (odroczenie jakościowe 0 do 30 dni, termin 2 do 30 dni, karencja 0 do 7 dni). Dostrajamy je do kalendarza awarii.

Pierścień	Grupa	Odroczenie jakościowe	Termin (deadline)	Karencja	Restart
Pilot	komputery IT	0 dni	2 dni	0 dni	Auto install and restart at maintenance time
Szeroki	biuro Pamiątkowo, handlowcy	7 dni	3 dni	2 dni	Auto install and restart at a scheduled time, w nocy

Pierścień	Grupa	Odroczenie jakościowe	Termin (deadline)	Karencja	Restart
Krytyczny	księgowość, magazyn Swarzędz	14 dni	5 dni	2 dni	Auto install and restart at a scheduled time, noc niedzieli; Auto reboot before deadline: No

Pierścień Pilot dostaje poprawki jako pierwszy. Przy odroczeniu Krytycznego 14 dni ewentualne problemy zdążą ujawnić się wcześniej niż w księgowości i w magazynie. W ostatnich trzech dniach roboczych miesiąca i w okresie zakazu zmian (od 15 listopada do 6 stycznia) przed Patch Tuesday przeglądamy terminy i w razie potrzeby wstrzymujemy pierścień Krytyczny (Pause) po uzgodnieniu z Markiem i panią Haliną. Dokumentacja Intune opisuje wstrzymanie jako akcję na pierścieniu.

Aktualizacje funkcji, sterowniki, hotpatch

Polityka aktualizacji funkcji ma trzy tryby udostępniania: jak najszybciej, w wybranym dniu albo stopniowo (z wielkością grupy). Dla Zielonej: Pilot ASAP, Szeroki w wybranym dniu po tygodniu, Krytyczny po miesiącu. Przy kilku politykach funkcji na jednym komputerze Windows Update oferuje jedną, zawsze najnowszą z pasujących.

Sterowniki z Windows Update obsługuje osobna polityka sterowników, a w pierścieniu przełącznik Windows drivers (Allow albo Block) decyduje, czy pierścień w ogóle je dostarcza.

Hotpatch to poprawki bezpieczeństwa bez restartu. Wymaga:

- licencji z listy dokumentacji (w tym Microsoft 365 Business Premium, Windows 11 Enterprise E3 lub E5, Microsoft 365 F3, Windows 11 Education A3 lub A5, Windows 365 Enterprise),
- Windows 11 w wersji 24H2 lub nowszej, na najnowszym wydaniu bazowym,
- włączonego VBS (zabezpieczeń opartych na wirtualizacji),
- Intune do zarządzania (polityka z fiszki wyżej).

Cykl jest kwartalny: miesiące bazowe z restartem to styczeń, kwiecień, lipiec i październik, a w pozostałych miesiącach (luty, marzec, maj, czerwiec, sierpień, wrzesień, listopad, grudzień) poprawki wchodzą bez restartu. Włączenie hotpatch nie zmienia terminów, odroczeń ani godzin aktywności. W Zielonej październik 2026 jest miesiącem bazowym, więc poprawka z 13 października wymaga restartu mimo hotpatch.

Windows Autopatch krótko

> **Pojęcie: Windows Autopatch.** Usługa Microsoftu, która sama układa komputery w grupy wdrażania i rozkłada poprawki, zamiast ręcznie utrzymywanych pierścieni. Nazwa obejmuje też funkcje (hotpatch, raporty), z których część widać w Intune jako polityki aktualizacji.

Wymagania według dokumentacji (stan na październik 2026), do potwierdzenia przy zakupie:

Wymaganie	Wartość
Licencje	Microsoft 365 Business Premium, Windows 10 lub 11 Enterprise E3 lub E5, Education A3 lub A5, Enterprise E3 lub E5 VDA
Tożsamość	Microsoft Entra ID P1 lub P2, Intune, komputery Entra joined albo hybrid joined
Urządzenia	Windows 11 lub 10 (Pro, Enterprise, Education i pokrewne), tylko firmowe, kanał General Availability
Dane diagnostyczne	co najmniej poziom Required
Intune	urządzenie zarejestrowane w Intune i zgłaszające się w ciągu ostatnich 28 dni, z dostępem do internetu
Polityki oparte na Autopatch	licencja z uprawnieniem Autopatch, usługa Microsoft Account Sign-In Assistant włączona, dane diagnostyczne Required; urządzenia registered nie są obsługiwane

Dla Zielonej Autopatch to opcja do rozważenia po pilotażu pierścieni ręcznych, bo najpierw chcemy zrozumieć, jak wyglądają nasze komputery.

Intune i WSUS

Komputery z GPO wskazującym `wsus01` (ustawienie Specify intranet Microsoft update service location) szukają poprawek na serwerze WSUS, nie w Windows Update, więc pierścień nie zadziała tak, jak zakładamy. W dokumentacji rozwiązywania problemów pierścieni wśród częstych konfliktów wymieniono właśnie GPO, WSUS i polityki Configuration Managera. Ustawienie `ControlPolicyConflict` nie obejmuje CSP aktualizacji, więc nie rozstrzygnie takiego konfliktu. Zanim przypiszemy grupie pierścień, usuwamy z niej GPO WSUS albo wyłączamy go dla jej jednostki organizacyjnej.

Raporty i zgodność floty

Raport mówi, jak jest, a pierścień mówi, jak ma być. Przeglądamy raporty co tydzień według listy:

Pytanie	Raport
Które komputery nie mają poprawki, mimo że termin minął?	Per update ring deployment state, Windows 10 and later feature updates
Które polityki aktualizacji mają ostrzeżenia?	Feature update policies with alerts, Driver update policies with alerts
Które komputery są niezgodne i z jakiego powodu?	Noncompliant devices, Setting compliance
Które komputery nie mają zasady zgodności?	Devices without compliance policy
Które komputery nie są zaszyfrowane?	Device encryption status

Zdalne akcje: co robią i czym grożą

Akcja	Co robi	Uwaga
Sync	wymusza zgłoszenie komputera do Intune	pierwsza rzecz po zmianie polityki
Restart	restartuje komputer	użytkownik traci niezapisaną pracę
Retire	usuwa dane i ustawienia firmowe, zostawia dane osobiste	dla komputerów, które zostają w użyciu
Wipe	przywraca ustawienia fabryczne, usuwa wszystkie dane	przed akcją sprawdzamy, czy klucz BitLockera jest zapisany
Delete	usuwa urządzenie z Intune, usuwa dane firmowe i wycofuje je	nie usuwa obiektu komputera z Active Directory
Fresh Start	instaluje najnowszą wersję Windows i usuwa aplikacje producenta	z opcją Retain user data komputer zostaje dołączony do Entra ID i sam rejestruje się ponownie, bez niej wraca do stanu po OOBE
Autopilot reset	przywraca ustawienia z usuwaniem plików osobistych, aplikacji i ustawień	dla komputerów rejestrowanych przez Autopilot
Rotate BitLocker keys, Rotate local admin password	zmiana klucza odzyskiwania i hasła administratora	po użyciu klucza lub hasła w pomocy technicznej
Quick Scan, Full Scan, Update Windows Defender security intelligence	skan i aktualizacja sygnatur	przy podejrzeniu infekcji

Retire, Wipe i Delete mają pierwszeństwo przed wszystkimi innymi akcjami. W tenancie obowiązują dzienne limity: wipe 500, retire 1000 i delete 1000 urządzeń.

> ⚠ Fresh Start usuwa aplikacje producenta, ale też wszystkie aplikacje zainstalowane przez użytkownika. Bez opcji Retain user data komputer prywatny (BYOD) jest przy okazji usuwany z Microsoft Entra ID i z MDM, a komputer firmowy wraca do stanu po OOBE z wbudowanym kontem administratora.

Częste błędy

Objaw	Przyczyna	Co robimy
Pierścień przypisany, a komputer nie dostaje poprawek	GPO z ustawieniem WSUS albo inne GPO o aktualizacjach nadpisuje pierścień	`gpresult /h`, Configured update policies, wyłączamy konfliktowe GPO dla tej grupy
Komputer restartuje się w złym momencie	pierścień ma Auto reboot before deadline ustawiony na Yes albo za krótki termin	Auto reboot before deadline: No, restart w oknie serwisowym, terminy dopasowane do kalendarza
Polityka funkcji nie przenosi komputera na nową wersję	komputer ma już nowszą wersję albo odroczenia funkcji w pierścieniu konfliktują z polityką	trzymamy wersję w polityce funkcji, odroczenia funkcji w pierścieniu zostawiamy na 0
Hotpatch nie jest oferowany	brak VBS, wersja Windows starsza niż 24H2, brak wydania bazowego	sprawdzamy wymagania, instalujemy najnowszy baseline
Polityki oparte na Autopatch nie działają na jednym komputerze	komputer jest Entra registered, prywatny albo ma wyłączone dane diagnostyczne	rejestracja jako firmowy (hybrid lub Entra joined), dane diagnostyczne Required
Raport pokazuje „Conflict" dla ustawienia	to samo ustawienie z dwóch źródeł (GPO, drugi pierścień, katalog ustawień)	zostawiamy jedną metodę, usuwamy duplikaty
Wipe się nie wykonuje	komputer jest wyłączony albo bez łączności	akcja czeka w kolejce, wykona się po włączeniu komputera i zgłoszeniu do Intune
Po Fresh Start komputer prywatny zniknął z Entra ID	akcja bez Retain user data usuwa urządzenia BYOD z Entra ID	przed akcją wybieramy Retain user data, a na prywatnych używamy Retire

Ćwiczenia

1. Dlaczego odroczenie funkcji w pierścieniu zostawiamy na 0, gdy używamy polityki aktualizacji funkcji?

Odpowiedź

Polityka funkcji nadpisuje odroczenia funkcji z pierścienia i trzyma komputery na wskazanej wersji, a mieszanie obu mechanizmów dodaje złożoności i potrafi zablokować albo opóźnić aktualizacje. Dokumentacja radzi, żeby pierścień obsługiwał tylko doświadczenie użytkownika (restarty, powiadomienia), a wersję ustawiała polityka funkcji.

1. Komputer pana Zbigniewa dostał pierścień, ale `Configured update policies` pokazuje Group Policy. Co robimy?

Odpowiedź

Uruchamiamy `gpresult /h C:\Temp\gpo.html` i szukamy GPO, które ustawia aktualizacje (zwykle Specify intranet Microsoft update service location z `wsus01`). Wyłączamy to GPO dla jednostki organizacyjnej z komputerem, żeby zdecydował pierścień z Intune. Ustawienie `ControlPolicyConflict` tutaj nie pomoże, bo nie obejmuje CSP aktualizacji.

1. Kasia zgubiła służbowy laptop w pociągu. Jaką akcję wybieramy i co sprawdzamy najpierw?

Odpowiedź

Wipe, z opcją kontynuowania nawet po utracie zasilania, bo to firmowy komputer i zależy nam na usunięciu danych. Najpierw sprawdzamy, czy klucz BitLockera jest zapisany w Entra ID albo AD i czy laptop jest zaszyfrowany. Jeśli komputer jest wyłączony, akcja wykona się po jego włączeniu i połączeniu z internetem, więc dodatkowo blokujemy konto i unieważniamy sesje.

Powiązane: Windows Update z wiersza poleceń · WSUS: czyszczenie i utrzymanie · Zasady zgodności i dostęp warunkowy · Profile konfiguracji: katalog ustawień zamiast GPO · BitLocker z kluczem odzyskiwania w Active Directory

Źródła: Microsoft Learn, „Windows update management overview" (learn.microsoft.com/intune/device-updates/windows) · „Update ring policy settings" (learn.microsoft.com/intune/device-updates/windows/ref-update-ring-settings) · „Manage Windows update rings" (learn.microsoft.com/intune/device-updates/windows/manage-update-rings) · „Configure Windows feature update policies" (learn.microsoft.com/intune/device-updates/windows/configure-feature-update-policy) · „Hotpatch updates" (learn.microsoft.com/windows/deployment/windows-autopatch/manage/windows-autopatch-hotpatch-updates) · „Windows Autopatch prerequisites" (learn.microsoft.com/windows/deployment/windows-autopatch/prepare/windows-autopatch-prerequisites) · „Troubleshoot update ring policies" (learn.microsoft.com/troubleshoot/mem/intune/device-protection/troubleshoot-update-rings) ·

„Microsoft Intune reports" (learn.microsoft.com/intune/device-management/reports/overview) · „Device actions" (learn.microsoft.com/intune/device-management/actions) · „Device action: Wipe" i „Device action: Fresh Start" (learn.microsoft.com/intune/device-management/actions/wipe, .../fresh-start)

Revision #16
Created 2026-10-03 11:23:08 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:18 UTC by Tomasz Konieczny