Windows LAPS — migracja ze starego LAPS i przejście na Intune

Typ: procedura

Dotyczy: Windows 10/11, Windows Server 2019+ (natywnie Windows 11 23H2+ i Server 2025), Active Directory, Entra ID

Czas: ~45 min przygotowania domeny plus pilotaż na jednej jednostce organizacyjnej

Efekt: hasła lokalnych administratorów rotuje wbudowany Windows LAPS, a nie przestarzały pakiet MSI; schemat AD jest rozszerzony, komputery mają prawo zapisywać własne hasła, odczyt jest ograniczony do wskazanej grupy, a dla każdego urządzenia hybrydowego wiadomo, czy jego hasło leży w AD, czy w Entra ID.

Skróty użyte na tej stronie (7)

Skrót	Co znaczy
AD	Active Directory: katalog kont, komputerów i zasad w domenie Windows
CSP	Configuration Service Provider: interfejs ustawień Windows sterowany przez MDM, np. Intune
DSRM	Directory Services Restore Mode: tryb odzyskiwania kontrolera domeny z własnym hasłem
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
LAPS	Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów
MSI	Microsoft Installer: format pakietu instalacyjnego Windows
OU	Organizational Unit: jednostka organizacyjna w Active Directory

Fiszka

TYLKO ODCZYT

Czy system ma wbudowany Windows LAPS: moduł LAPS

```
# polecenie pomocnicze
Get-Command -Module LAPS | Select-Object Name
```

Windows LAPS trafił do systemu przez Windows Update **11 kwietnia 2023** (Windows 10, 11, Server 2019 i 2022), a natywnie jest w Windows 11 23H2+ i Server 2025. Jeśli moduł `LAPS` jest dostępny, maszyna nie potrzebuje żadnego dodatkowego pakietu. Stary Microsoft LAPS w postaci MSI jest przestarzały od 23H2, a nowsze wersje systemu blokują jego instalację.

LAPS = Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów · **MSI** = Microsoft Installer: format pakietu instalacyjnego Windows

TYLKO ODCZYT

Czy komputer korzysta jeszcze ze starego LAPS: atrybut ms-Mcs-AdmPwd

```
# polecenie pomocnicze; moduł ActiveDirectory
Get-ADComputer -Filter * -SearchBase "OU=Stacje,DC=firma,DC=local" -Properties 'ms-Mcs-AdmPwd' |
    Where-Object { $_.'ms-Mcs-AdmPwd' } |
    Select-Object Name
```

Stary LAPS zapisuje hasło w atrybucie `ms-Mcs-AdmPwd` obiektu komputera. Lista komputerów z wypełnionym atrybutem to zakres migracji. Polecenie odczytuje hasła starego LAPS, więc uruchamiamy je kontem, które i tak ma do nich prawo — i nie wypisujemy samych haseł na ekran.

LAPS = Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów

TYLKO ODCZYT

Kto może czytać hasła w jednostce organizacyjnej: Find-LapsADExtendedRights

```
# polecenie pomocnicze; moduł LAPS
Find-LapsADExtendedRights -Identity "OU=Stacje,DC=firma,DC=local"
```

Przed migracją i po niej sprawdzamy, którym kontom i grupom przysługuje rozszerzone prawo odczytu haseł w danej jednostce organizacyjnej. Hasło lokalnego administratora to klucz do każdej maszyny z tej jednostki — lista powinna być krótka i znana z nazwy.

TYLKO ODCZYT

Odczyt hasła z AD: Get-LapsADPassword

```
# polecenie pomocnicze; moduł LAPS
Get-LapsADPassword -Identity NAZWA-KOMPUTERA -AsPlainText
```

Pobieramy aktualne hasło lokalnego administratora zapisane przez Windows LAPS w AD — na przykład przed naprawą relacji zaufania na maszynie, która przestała logować konta domenowe (Machine Identity Isolation po KB5124008). Parametr `-AsPlainText` Microsoft opisuje jako ryzyko bezpieczeństwa i zaleca tylko do wsparcia i testów: bez niego hasło wraca jako `SecureString`. Nie używamy go w skryptach, nie zapisujemy wyniku do plików ani dzienników i nie uruchamiamy go przy udostępnionym ekranie. Hasła urządzeń, które zapisują kopię w Entra ID, odczytujemy z portalu Intune albo Entra, nie tym poleceniem.

AD = Active Directory: katalog kont, komputerów i zasad w domenie Windows · **LAPS** = Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów

Gdzie Windows LAPS trzyma hasło

Urządzenie	Miejsce kopii hasła
tylko Entra ID (Entra joined)	Entra ID
tylko AD (przyłączone do domeny)	AD
hybrydowe (Entra hybrid joined)	**albo Entra ID, albo AD — nigdy oba**
kontroler domeny	hasło DSRM, w AD

Poza samą rotacją Windows LAPS daje szyfrowanie hasła w AD, historię haseł, **tryb emulacji starego Microsoft LAPS** do migracji stopniowej, wykrywanie przywrócenia obrazu (image rollback) i — od Windows 11 24H2 i Server 2025 — automatyczne zarządzanie kontem. Na urządzeniach hybrydowych decyzja AD kontra Entra ID jest jednorazowa dla urządzenia i idzie w parze z decyzją hybrid join czy Entra join dla nowych maszyn, opisaną na stronie Windows 11 w firmie 2026 — przegląd zmian.

Zanim zaczniemy

Ustalamy katalog docelowy: dla floty w domenie, która na razie zostaje hybrydowa, najprostsze jest AD; dla maszyn, które przejdą na Entra join, — Entra ID. Mieszanie w obrębie jednego urządzenia nie jest możliwe.

Rozszerzenie schematu wymaga konta z grupy Schema Admins i jest zmianą całego lasu — robimy ją w oknie serwisowym, po sprawdzeniu, że mamy aktualną kopię zapasową stanu systemu kontrolerów domeny, i po uzgodnieniu z właścicielem AD. Wybieramy jedną jednostkę organizacyjną pilotażową z kilkoma stacjami, najlepiej już objętymi starym LAPS, i grupę, która będzie mogła czytać hasła (np. helpdesk).

Spisujemy istniejące GPO starego LAPS — ich usunięcie jest ostatnim, a nie pierwszym krokiem migracji.

Przebieg

1. Rozszerzenie schematu AD

◫◫ OSTROŻNIE · NIEODWRACALNE

Rozszerzenie schematu o atrybuty Windows LAPS: Update-LapsADSchema

```
# podgląd bez zmian
Update-LapsADSchema -WhatIf
# właściwe rozszerzenie: cmdlet pyta o zgodę przy każdym atrybucie
Update-LapsADSchema -Verbose
```

Pierwszy krok migracji według dokumentacji. Cmdlet domyślnie pyta o zgodę przed dodaniem każdego atrybutu — nie odpowiadamy hurtem „Yes to All” i nie dodajemy `-Confirm:$false`, dopóki nie przeczytamy listy z `-WhatIf`. Rozszerzenia schematu AD **nie da się cofnąć** — nowe atrybuty zostają w lesie na zawsze, niezależnie od tego, czy z nich skorzystamy. Samo rozszerzenie nie zmienia zachowania żadnego komputera; wykonujemy je raz, kontem z Schema Admins, na maszynie z modułem LAPS i łącznością z kontrolerem, który ma rolę wzorca schematu.

AD = Active Directory: katalog kont, komputerów i zasad w domenie Windows · **LAPS** = Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów

2. Uprawnienia komputerów do zapisu własnych haseł

ZMIENIA SYSTEM

Prawo zapisu hasła dla komputerów w OU: Set-LapsADComputerSelfPermission

```
Set-LapsADComputerSelfPermission -Identity "OU=Pilotaz-LAPS,OU=Stacje,DC=firma,DC=local"
```

Drugi krok z dokumentacji: komputery w jednostce organizacyjnej dostają prawo zapisu własnego hasła do nowych atrybutów. Bez tego polityka Windows LAPS rotuje hasło lokalnie, ale nie może go zapisać w AD. Parametr `-Identity` wskazuje jednostkę organizacyjną (składnia zgodna z dokumentacją modułu LAPS; cmdlet obsługuje też `-WhatIf`).

AD = Active Directory: katalog kont, komputerów i zasad w domenie Windows · **LAPS** = Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów · **OU** = Organizational Unit: jednostka organizacyjna w Active Directory

ZMIENIA SYSTEM

Prawo odczytu haseł dla wybranej grupy: Set-LapsADReadPasswordPermission

```
# polecenie pomocnicze; moduł LAPS
Set-LapsADReadPasswordPermission -Identity "OU=Pilotaz-LAPS,OU=Stacje,DC=firma,DC=local"
-AllowedPrincipals "FIRMA\Helpdesk"
```

Nadajemy prawo odczytu konkretnej grupie, a nie pojedynczym osobom. Po zmianie sprawdzamy wynik kartą z `Find-LapsADExtendedRights` w Fiszce.

3. Polityka Windows LAPS

Politykę tworzymy w GPO **System\LAPS** (Konfiguracja komputera → Szablony administracyjne) albo w Intune przez **CSP LAPS** — i dla danego urządzenia wybieramy jedno z nich. Wskazujemy

katalog kopii (AD albo Entra ID), konto zarządzane i wymagania co do hasła. Jeśli migrujemy stopniowo i część narzędzi helpdesku wciąż czyta hasła starym sposobem, na czas przejścia włączamy **tryb emulacji starego Microsoft LAPS** — Windows LAPS zachowuje się wtedy jak poprzednik, a my mamy czas na przełączenie procedur odczytu. Politykę podpinamy na razie tylko do pilotażowej jednostki organizacyjnej.

4. Pierwsze przetworzenie polityki na maszynie pilotażowej

◫◫ ZMIENIA SYSTEM

Wymuszenie przetworzenia polityki: Invoke-LapsPolicyProcessing

```
# polecenia pomocnicze; moduł LAPS
gpupdate /force
Invoke-LapsPolicyProcessing
```

Uruchamiamy na maszynie pilotażowej w PowerShellu jako administrator. `Invoke-LapsPolicyProcessing` przetwarza politykę od razu, bez czekania na cykl w tle; według dokumentacji sam niczego nie wymusza — hasło zmienia się tylko wtedy, gdy wynika to z polityki (np. pierwsze przetworzenie nowej polityki albo hasło po terminie). Cmdlet zwraca niewiele informacji: wynik sprawdzamy w dzienniku zdarzeń Windows LAPS. Jeśli ktoś ma otwartą sesję kontem zarządzanym, po rotacji stare hasło przestaje działać przy następnym logowaniu.

◫◫ OSTROŻNIE · NIEODWRACALNE

Natychmiastowa rotacja hasła: Reset-LapsPassword

```
# moduł LAPS; uruchamiamy na maszynie, której hasło rotujemy
Reset-LapsPassword
```

`Reset-LapsPassword` rotuje hasło konta zarządzanego natychmiast, niezależnie od terminu wygaśnięcia. Microsoft przewiduje go na rzadkie sytuacje, np. reakcję na incydent, i odradza częste użycie. Karta jest czerwona, bo poprzedniego hasła nie da się przywrócić — przed rotacją sprawdzamy, że polityka zapisuje kopię w katalogu (karta z `Get-LapsADPassword` w Fiszce albo portal Entra), a po niej od razu odczytujemy nowe hasło i logujemy się nim lokalnie. Na maszynie bez łączności z katalogiem nie rotujemy wcale. Wynik sprawdzamy w dzienniku zdarzeń Windows LAPS.

5. Kontrolery domeny

Na kontrolerach domeny Windows LAPS zarządza hasłem **DSRM** i zapisuje je w AD. To hasło jest potrzebne wyłącznie przy odtwarzaniu kontrolera — sprawdzamy, że grupa z prawem odczytu jest dla kontrolerów węższa niż dla stacji.

6. Wygaszenie starego LAPS

Dopiero gdy wszystkie maszyny z zakresu migracji mają hasło w nowych atrybutach (karta z `Get-LapsADPassword`) i helpdesk korzysta z nowej ścieżki odczytu, wyłączamy tryb emulacji, odpinamy GPO starego LAPS i odinstalowujemy pakiet MSI tam, gdzie jeszcze jest. Na Windows 11 23H2 i nowszych problem rozwiązuje się sam: MSI nie da się tam zainstalować.

Weryfikacja

`Get-LapsADPassword -Identity NAZWA-KOMPUTERA -AsPlainText` zwraca hasło i datę jego ustawienia, a logowanie lokalnym kontem administratora tym hasłem na maszynie pilotażowej działa. Konto spoza grupy z prawem odczytu nie widzi hasła. `Find-LapsADExtendedRights` dla pilotażowej jednostki organizacyjnej pokazuje wyłącznie grupy, które tam świadomie wpisaliśmy. Dla urządzeń z kopią w Entra ID hasło jest widoczne w portalu przy obiekcie urządzenia.

Wycofanie zmian

Politykę Windows LAPS odpinamy od jednostki organizacyjnej albo usuwamy profil w Intune — maszyna przestaje rotować hasło, a ostatnie ustawione hasło zostaje w katalogu. Jeśli wycofujemy się w trakcie migracji, włączamy tryb emulacji i przywracamy GPO starego LAPS na maszynach, które jeszcze go mają (na 23H2+ nie da się już zainstalować MSI, więc tam wycofanie oznacza pozostanie przy Windows LAPS). **Rozszerzenia schematu z kroku 1 nie cofamy** — nowe atrybuty zostają, nieużywane.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
Hasło się rotuje, ale nie ma go w AD	brak prawa zapisu dla komputerów w jednostce organizacyjnej	krok 2 — `Set-LapsADComputerSelfPermission` dla właściwej OU

Objaw	Przyczyna	Naprawa
`Get-LapsADPassword` nic nie zwraca	polityka wskazuje Entra ID jako katalog kopii albo nie została jeszcze przetworzona	sprawdzić katalog w polityce; `Invoke-LapsPolicyProcessing` na maszynie
Urządzenie hybrydowe „ma dwa hasła”	próba zapisu jednocześnie do AD i Entra ID	niemożliwe z założenia — wybrać jeden katalog w jednej polityce (GPO albo CSP)
Instalator starego LAPS kończy się błędem	Windows 11 23H2+ blokuje instalację pakietu MSI	zachowanie zgodne z dokumentacją — przejście na wbudowany Windows LAPS
Helpdesk nie widzi haseł po migracji	narzędzia czytają atrybut `ms-Mcs-AdmPwd`, a emulacja jest wyłączona	przejściowo tryb emulacji; docelowo odczyt przez moduł LAPS albo portal
Po przywróceniu maszyny z obrazu stare hasło nie działa	Windows LAPS wykrył przywrócenie obrazu i zrotował hasło	odczytać bieżące hasło z katalogu

Powiązane: Windows 11 w firmie 2026 — przegląd zmian · Machine Identity Isolation po KB5124008 · Skrypty audytowe Active Directory · Poświadczenia i bezpieczne hasła w skryptach

Źródła: Windows LAPS overview — Microsoft Learn

Revision #3
Created 2026-09-27 17:44:20 UTC by Tomasz Konieczny
Updated 2026-10-18 23:00:54 UTC by Tomasz Konieczny