Windows LAPS z Intune: hasło lokalnego administratora w Entra ID albo AD

◫◫ Poziom: średniozaawansowany

◫◫ Dotyczy: Windows LAPS, Microsoft Intune, Microsoft Entra ID, Windows 11 (automatyczne zarządzanie kontem od 24H2)

▯ Czas: ~50 min

Każdy komputer ma lokalne konto administratora, a jedno wspólne hasło na całej flocie to prezent dla każdego, kto je kiedyś pozna. Windows LAPS nadaje każdemu komputerowi inne, losowe hasło i sam je zmienia, a Intune pozwala ustawić to jedną polityką także na komputerach, które nie widzą `dc01`. Strona pokazuje, gdzie hasło ma leżeć (Entra ID albo AD), kto je czyta i jak przejść z GPO ze strony o Windows LAPS w Active Directory bez konfliktu.

> Microsoft często przemianowuje i przenosi pozycje w Intune i w Entra, więc ścieżki poniżej traktujemy jako wskazówkę, a w razie rozbieżności szukamy po nazwie ustawienia (na przykład Backup Directory). Stan dokumentacji, na którym oparliśmy stronę: październik 2026. Nazwy wartości w interfejsie (na przykład opisy opcji złożoności hasła) podajemy według dokumentacji, a na ekranie mogą brzmieć trochę inaczej. Numery zdarzeń i nazwy ustawień sprawdzamy na komputerze pilotażowym, zanim zbudujemy na nich procedurę.

◫◫ Skróty użyte na tej stronie (8)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
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

Skrót	Co znaczy
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
LAPS	Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

Polecenia PowerShell wykonujemy w podniesionym PowerShellu: te z fiszek o komputerze na samym komputerze, te o odczycie hasła na stanowisku pomocy technicznej. Ścieżki w centrach administracyjnych podajemy po angielsku, tak jak w dokumentacji.

□□ KLIKAMY W INTERFEJSIE

Włączenie Windows LAPS w Microsoft Entra ID: Device settings

```
Microsoft Entra admin center → Entra ID → Devices → Overview → Device settings
→ Enable Local Administrator Password Solution (LAPS): Yes → Save
```

Domyślnie Entra nie przyjmuje haseł z komputerów, więc ten przełącznik włączamy raz na tenant, zanim jakakolwiek polityka zadziała. Potrzebna jest rola co najmniej Cloud Device Administrator. Bez tego komputer z poprawną polityką nie zapisze hasła i w Intune zobaczymy pustą zakładkę.

□□ **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

□□ ZMIENIA SYSTEM

Utworzenie polityki Windows LAPS: Account protection

```
Microsoft Intune admin center → Endpoint security → Account protection → Create policy
→ Platform: Windows → Profile: Local admin password solution (Windows LAPS)
→ Basics: nazwa, np. LAPS-Entra-Hybrid
→ Backup Directory: Backup the password to Microsoft Entra ID only
```

```
→ Password Age Days: 30
→ Password Length: 20
→ Password Complexity: Large letters + small letters + numbers + special characters
→ Post Authentication Actions: Reset the password and logoff the managed account
→ Post Authentication Reset Delay: 24
→ Administrator Account Name: puste (wbudowany Administrator)
→ Assignments: grupa urządzeń Intune-Urzadzenia-Hybrid
```

Wartości to nasza propozycja startowa. Dokumentacja przypisywanie do grup urządzeń zaleca wprost, bo przypisanie do grup użytkowników powoduje konflikty, gdy użytkownik zmienia komputer. Do polityki dochodzi zasada jednej polityki na urządzenie, opisana niżej.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Configuration settings polityki LAPS-Entra-Hybrid w Intune admin center, widoczne Backup Directory ustawione na Microsoft Entra ID, Password Age Days 30, Password Length 20 i Post Authentication Actions.

LAPS = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

ZMIENIA SYSTEM

Utworzenie polityki z automatycznym kontem: Automatic Account Management

```
Microsoft Intune admin center → Endpoint security → Account protection → Create policy
→ Platform: Windows → Profile: Local admin password solution (Windows LAPS)
→ Basics: nazwa, np. LAPS-Entra-EntraJoined
→ Backup Directory: Backup the password to Microsoft Entra ID only
→ Automatic Account Management Enabled: Enabled
→ Automatic Account Management Target: Manage a new custom administrator account
→ Automatic Account Management Name Or Prefix: ZielonaAdm
→ Automatic Account Management Randomize Name: Enabled
→ Automatic Account Management Enable Account: Enabled
→ Assignments: grupa urządzeń Intune-Urzadzenia-EntraJoined
```

Te ustawienia działają tylko na Windows 11 24H2 i nowszym, a starsze wersje zarządzają wyłącznie kontem, które już istnieje. Przy losowaniu nazwy `ZielonaAdm` jest przedrostkiem (najwyżej 14 znaków), a system dokłada do niego sześć cyfr przy każdej rotacji. Grupa

`Intune-Urzadzenia-EntraJoined` to nasza propozycja: grupa dynamiczna z regułą `device.deviceTrustType -eq "AzureAD"`, taka sama konstrukcja jak grupa `Intune-Urzadzenia-Hybrid` ze strony z planem wdrożenia.

TYLKO ODCZYT

Sprawdzenie konta lokalnego na komputerze: Get-LocalUser

```
Get-LocalUser | Select-Object Name, Enabled, SID
```

Pokazuje, jakie konta lokalne ma komputer i czy są włączone. Wbudowany Administrator ma SID kończący się na `-500` i w Windows 11 jest domyślnie wyłączony, więc samo hasło w Entra nie wystarczy, żeby się nim zalogować.

Przykład:

```
Name               Enabled SID
----               ------- ---
Administrator        False S-1-5-21-3841260617-2217419984-1530621903-500
ZielonaAdm482731      True S-1-5-21-3841260617-2217419984-1530621903-1003
```

SID = w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta

TYLKO ODCZYT

Odczyt aktywnego źródła polityki: reg query

```
reg query "HKLM\Software\Microsoft\Policies\LAPS"
reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS"
```

Pierwsza ścieżka to polityka dostarczona z Intune (CSP), druga to polityka z GPO. Windows LAPS używa tylko pierwszego miejsca, w którym znajdzie choć jedno ustawienie, według kolejności: CSP, GPO, konfiguracja lokalna, stary Microsoft LAPS. Gdy oba polecenia coś zwracają, wygrywa Intune, a ustawienia z GPO nie uzupełniają jego polityki.

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 · **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu · **reg** = registry: narzędzie wiersza poleceń do odczytu i zmiany rejestru Windows, na przykład reg query · **HKLM** = HKEY_LOCAL_MACHINE: gałąź rejestru Windows z ustawieniami całego komputera, a nie pojedynczego użytkownika

□□ ZMIENIA SYSTEM

Wymuszenie przetworzenia polityki: Invoke-LapsPolicyProcessing

```
Invoke-LapsPolicyProcessing
```

Windows LAPS sprawdza politykę w tle co godzinę, a to polecenie robi to od razu. Używamy go po zmianie polityki w Intune, żeby nie czekać na najbliższy cykl.

□□ **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

□□ ZMIENIA SYSTEM

Wymuszenie zmiany hasła na komputerze: Reset-LapsPassword

```
Reset-LapsPassword
```

Zmienia hasło zarządzanego konta od razu i zapisuje nowe w katalogu. Używamy po przejściu z jednego katalogu na drugi i wtedy, gdy ktoś poznał hasło, które miał znać tylko chwilę. Dokumentacja ostrzega, że nadmiarowe wywoływanie może zostać ograniczone przez usługę w chmurze.

□□ TYLKO ODCZYT

Odczyt zdarzeń Windows LAPS: Event Viewer

```
Event Viewer → Applications and Services Logs → Microsoft → Windows → LAPS → Operational
→ 10004: przetwarzanie polityki zakończone powodzeniem
→ 10005: przetwarzanie polityki zakończone błędem (kod w treści)
→ 10029: hasło zapisane w Microsoft Entra ID
→ 10031: zablokowano próbę zmiany hasła zarządzanego konta przez coś innego niż LAPS
```

Numery pochodzą z dokumentacji Microsoftu o dzienniku zdarzeń Windows LAPS. Przy problemach z zapisem hasła szukamy najpierw zdarzenia 10005 i kodu błędu obok niego.

□□ **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

□□ KLIKAMY W INTERFEJSIE

Odczyt hasła w Intune: Local admin password

```
Microsoft Intune admin center → Devices → All devices → wybrany komputer
→ Local admin password → Show
```

Widać nazwę konta, jego SID, hasło (ukryte do czasu kliknięcia Show), datę ostatniej i następnej rotacji. Intune pokazuje wyłącznie hasła zapisane w Entra ID, a haseł z Active Directory tu nie zobaczymy. Do odczytu potrzebujemy uprawnienia `microsoft.directory/deviceLocalCredentials/password/read`.

SID = w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta

KLIKAMY W INTERFEJSIE

Odczyt hasła w Entra: Local administrator password recovery

```
Microsoft Entra admin center → Entra ID → Devices → Overview
→ Local administrator password recovery → wybieramy komputer → pokazanie hasła
```

To samo hasło, ten sam wymóg uprawnienia. Z tego miejsca korzystamy, gdy nie mamy roli w Intune, a mamy rolę w Entra.

ZMIENIA SYSTEM

Instalacja modułu Microsoft Graph PowerShell: Install-Module

```
Install-Module Microsoft.Graph -Scope CurrentUser
```

Polecenie Get-LapsAADPassword jest częścią modułu LAPS, który jest wbudowany w Windows, ale łączy się z Entra przez Microsoft Graph PowerShell, więc ten moduł instalujemy osobno, raz na stanowisku pomocy technicznej. Dokumentacja pokazuje instalację całego modułu `Microsoft.Graph`, więc przy węższych modułach sprawdzamy, czy wystarczą.

LAPS = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

TYLKO ODCZYT

Połączenie z Microsoft Graph: Connect-MgGraph

```
Connect-MgGraph -Scopes "DeviceLocalCredential.Read.All","Device.Read.All"
```

Zakres `DeviceLocalCredential.ReadBasic.All` wystarcza do metadanych (data wygaśnięcia, data zmiany), a do samego hasła potrzebny jest `DeviceLocalCredential.Read.All`. Przy pierwszym połączeniu Entra może poprosić o zgodę na zakresy, którą wyraża administrator.

TYLKO ODCZYT

Odczyt hasła z Entra w PowerShellu: Get-LapsAADPassword

```
Get-LapsAADPassword -DeviceIds NazwaKomputera -IncludePasswords -AsPlainText
```

Bez `-IncludePasswords` polecenie zwraca tylko metadane, a bez `-AsPlainText` hasło jako zaszyfrowany obiekt `SecureString`. Jawny tekst wybieramy tylko wtedy, gdy hasło musimy przepisać na konsoli. Parametr `-IncludeHistory` dokłada starsze hasła.

Przykład:

```
DeviceName             : lt-zarzad01
DeviceId               : 3f1c7a52-8e4b-4d0a-9b61-2c5d7e90a1b4
Account                : ZielonaAdm482731
Password               : kP9!qLm2Rz7#vTn4XeB8
PasswordExpirationTime : 02.11.2026 11:34:39
PasswordUpdateTime     : 03.10.2026 11:34:39
```

TYLKO ODCZYT

Odczyt hasła przez Graph: Get-MgDirectoryDeviceLocalCredential

```
Get-MgDirectoryDeviceLocalCredential -DeviceLocalCredentialInfoId
IdentyfikatorUrzadzenia -Property credentials
```

> (gdzie `IdentyfikatorUrzadzenia` to DeviceId komputera z Entra, widoczny też w `dsregcmd /status`; dokładny parametr sprawdzamy w `Get-Help`, bo moduł Graph zmienia się często)

Interfejs Graph zwraca hasło zakodowane w Base64 (w przykładzie z dokumentacji jako tekst Unicode), więc przy własnych skryptach je dekodujemy. Do codziennej pracy wystarcza `Get-LapsAADPassword`, który robi to za nas.

KLIKAMY W INTERFEJSIE

Ręczna rotacja hasła z Intune: Rotate local admin password

```
Microsoft Intune admin center → Devices → All devices → wybrany komputer
→ menu ... → Rotate local admin password
```

Do tej akcji potrzebna jest własna rola Intune z uprawnieniami Managed devices: Read, Organization: Read i Remote tasks: Rotate Local Admin Password, bo żadna wbudowana rola jej nie zawiera. Akcja działa na jednym komputerze naraz (nie ma jej w akcjach zbiorczych), a komputer Entra joined musi być w tej chwili online. Ręczna rotacja przesuwa też termin następnej zaplanowanej zmiany.

TYLKO ODCZYT

Odczyt hasła z Active Directory: Get-LapsADPassword

```
Get-LapsADPassword -Identity NazwaKomputera -AsPlainText
```

Dla komputerów, które zostają przy zapisie do AD (strona Windows LAPS: hasło lokalnego administratora w Active Directory). Gdy hasła w AD są szyfrowane, a nie mamy prawa odszyfrowania, wynik ma `DecryptionStatus : Unauthorized` i puste hasło mimo udanego zapytania.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

KLIKAMY W INTERFEJSIE

Przejrzenie wpisów audytu: Audit logs w Entra

```
Microsoft Entra admin center → Entra ID → Devices → Overview → Audit logs
→ szukamy: Recover device local administrator password
→ szukamy: Update device local administrator password
```

Pierwsza czynność to odczyt hasła przez człowieka albo skrypt, druga to zapis nowego hasła przez komputer. Odpowiednik dla komputerów z AD to dziennik zabezpieczeń kontrolera domeny, który opisaliśmy przy audycie na stronie o Windows LAPS w Active Directory.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **LAPS** = Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu

Z życia wzięte

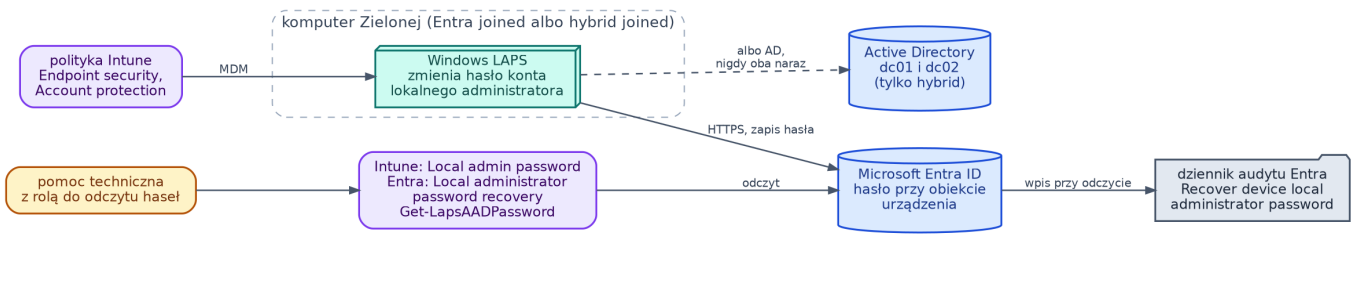
Z ŻYCIA WZIĘTE

Środa, 11:20. Laptop pana Zbigniewa, kupiony w sklepie i uruchomiony przez Autopilot, po aktualizacji sterownika zatrzymuje się na ekranie logowania i konto prezesa nie przechodzi. Laptop nie ma obiektu w AD, więc `Get-LapsADPassword` nic nie znajduje, ale Tomek pamięta, że to komputer Entra joined: otwiera w Intune zakładkę Local admin password i odczytuje nazwę konta `ZielonaAdm482731` wraz z hasłem. Po zalogowaniu naprawia sterownik, a po 24 godzinach LAPS sam zmienia hasło i wylogowuje to konto, więc nikt nie musi o nim pamiętać.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: Windows LAPS. Wbudowana w Windows funkcja, która ustawia lokalnemu kontu administratora losowe hasło, zmienia je co kilka dni i zapisuje w katalogu, z którego odczytują je tylko uprawnione osoby. LAPS to skrót od Local Administrator Password Solution. Zastąpiła starszy dodatek o tej samej nazwie, który trzymał hasło wyłącznie w Active Directory.



Polityka z Intune trafia na komputer, Windows LAPS zapisuje hasło w Entra ID (albo w AD na komputerze hybrid), pomoc techniczna odczytuje je w Intune lub PowerShellem, a każdy odczyt zostaje w dzienniku audytu (kliknięcie otwiera pełny rozmiar)

Windows LAPS kontra stary Microsoft LAPS

Cecha	Stary Microsoft LAPS (AdmPwd)	Windows LAPS
Skąd się bierze	osobny instalator MSI	wbudowany w system po aktualizacjach z 11 kwietnia 2023
Status	wycofany: 23 października 2023 ogłoszono jego deprecjację, Microsoft nie wprowadza zmian w kodzie, a MSI jest blokowany na nowszych systemach	wspierany, rozwijany (automatyczne zarządzanie kontem w 24H2)
Gdzie trzyma hasło	tylko Active Directory, atrybut `ms-Mcs-AdmPwd`	Active Directory (`msLAPS-Password`) albo Microsoft Entra ID
Polityka	GPO	GPO, Intune (CSP), rejestr, polityka lokalna
Wsparcie na starszych systemach	do końca cyklu życia tych systemów	Windows 10 i 11 po aktualizacjach z kwietnia 2023, Windows Server 2019 i nowszy

Według dokumentacji deprecjacja zaczyna się od nowszych wersji Windows 11 i Windows Server, a na starszych systemach stary dodatek jest wspierany do ich normalnego końca wsparcia. Dla nas wniosek jest prosty: nowe wdrożenia robimy tylko na Windows LAPS, a starego dodatku w Zielonej nie ma i nie instalujemy. Przed pierwszą zmianą sprawdzamy w dokumentacji, czy na komputerach nie został ślad starego dodatku (plik `AdmPwd.dll`), bo oba rozwiązania nie mogą zarządzać tym samym kontem.

Entra ID czy Active Directory: gdzie hasło ma leżeć

Komputer zapisuje hasło w jednym katalogu. Dla Entra joined jest tylko Entra ID, dla komputera w samej domenie tylko AD, a dla hybrid joined wybieramy jedno z dwóch, nigdy oba. Urządzenia Entra registered (prywatne, BYOD) nie są obsługiwane w żadnym trybie, co potwierdza też tabela ograniczeń na stronie o rejestracji urządzeń.

Kryterium	Microsoft Entra ID	Active Directory
Zależność od sieci biurowej	zapis przez HTTPS z dowolnego miejsca	komputer musi widzieć kontroler domeny
Widoczność w Intune	tak, zakładka Local admin password	nie, tylko narzędzia AD i PowerShell
Przygotowanie	jeden przełącznik w Entra	rozszerzenie schematu i uprawnienia (strona o LAPS w AD)
Kto czyta	role Entra z uprawnieniem do haseł	grupy AD z prawem odczytu i prawem odszyfrowania
Audyt odczytu	dziennik audytu Entra	dziennik zabezpieczeń kontrolera domeny
Zakres zmiany hasła	od 7 do 365 dni	od 1 do 365 dni

Licencyjnie wystarcza Intune Plan 1 z Business Premium, a Entra ID Free (rola niestandardowa do odczytu haseł wymaga P1, które też mamy w pakiecie). Propozycja dla Zielonej: Entra ID dla całej floty. Nowe komputery z Autopilota są Entra joined, więc nie mają wyboru, a komputery hybrid przenosimy w fali 5 planu wdrożenia, bo dzięki temu pomoc techniczna czyta hasła z jednego miejsca także wtedy, gdy VPN Kasi akurat nie działa. Do decyzji autora zostaje, czy komputery stale siedzące w biurze zostają przy AD, bo wtedy utrzymujemy dwa miejsca odczytu i dwie ścieżki audytu.

Konto zarządzane: wbudowany Administrator czy własne

Tryb	Co robi	Wymaga	Uwagi
Wbudowany Administrator (pole Administrator Account Name puste)	LAPS zmienia hasło konta o końcówce SID `-500`	każda wspierana wersja	konto bywa domyślnie wyłączone, wtedy hasło jest, ale logowanie nie
Własne, istniejące konto (podajemy jego nazwę)	LAPS zmienia hasło wskazanego konta	konto założone wcześniej	gdy nazwy nie ma na komputerze, żadne konto nie jest zarządzane
Automatyczne zarządzanie kontem	LAPS sam zakłada konto, włącza je lub wyłącza i może losować nazwę	Windows 11 24H2 lub nowszy	zalecany przez Microsoft: konto własne, a wbudowany Administrator zostaje wyłączony

LAPS zarządza jednym kontem na komputerze. W trybie automatycznym konto jest administratorem lokalnym, a opis wskazuje, że steruje nim LAPS, więc próby zmiany jego hasła z zewnątrz są odrzucane. Wyłączone konto chroni przed zgadywaniem haseł, ale przed użyciem trzeba je włączyć polityką, dlatego w Zielonej na komputerach Entra joined proponujemy konto

włączone z losową nazwą (do decyzji autora).

Rotacja hasła

Komputer co godzinę sprawdza w tle, czy hasło wygasło, a jeśli tak, generuje nowe, zapisuje je w katalogu i liczy nowy termin. Domyślnie hasło ma 14 znaków i zmienia się co 30 dni, a nasza propozycja to 20 znaków przy tym samym terminie. Dodatkowe uruchomienia to ręczna rotacja (`Reset-LapsPassword`, akcja w Intune) i rotacja po użyciu konta.

Ustawienie Post Authentication Actions mówi, co robimy po tym, jak ktoś użył zarządzanego konta: domyślnie po 24 godzinach hasło jest zmieniane, a konto wylogowywane. Dzięki temu odczytane hasło jest ważne najwyżej dobę. Opcje ostrzejsze, czyli ponowne uruchomienie komputera i zakończenie wszystkich procesów (to drugie wymaga Windows 11 24H2), planujemy ostrożnie, bo przerywają pracę użytkownika.

W Windows 11 24H2 doszły też hasła w formie fraz złożonych ze słów (opcje złożoności od 6 do 8) oraz złożoność z poprawioną czytelnością. Dla konta, które pomoc techniczna czasem przepisuje z ekranu, to wygodne, ale wymaga 24H2 na wszystkich komputerach objętych polityką.

Kto może odczytać hasło

Rola Entra	Hasło	Metadane
Cloud Device Administrator	tak	tak
Intune Administrator	tak	tak
Helpdesk Administrator	nie	tak
Security Administrator	nie	tak
Security Reader	nie	tak

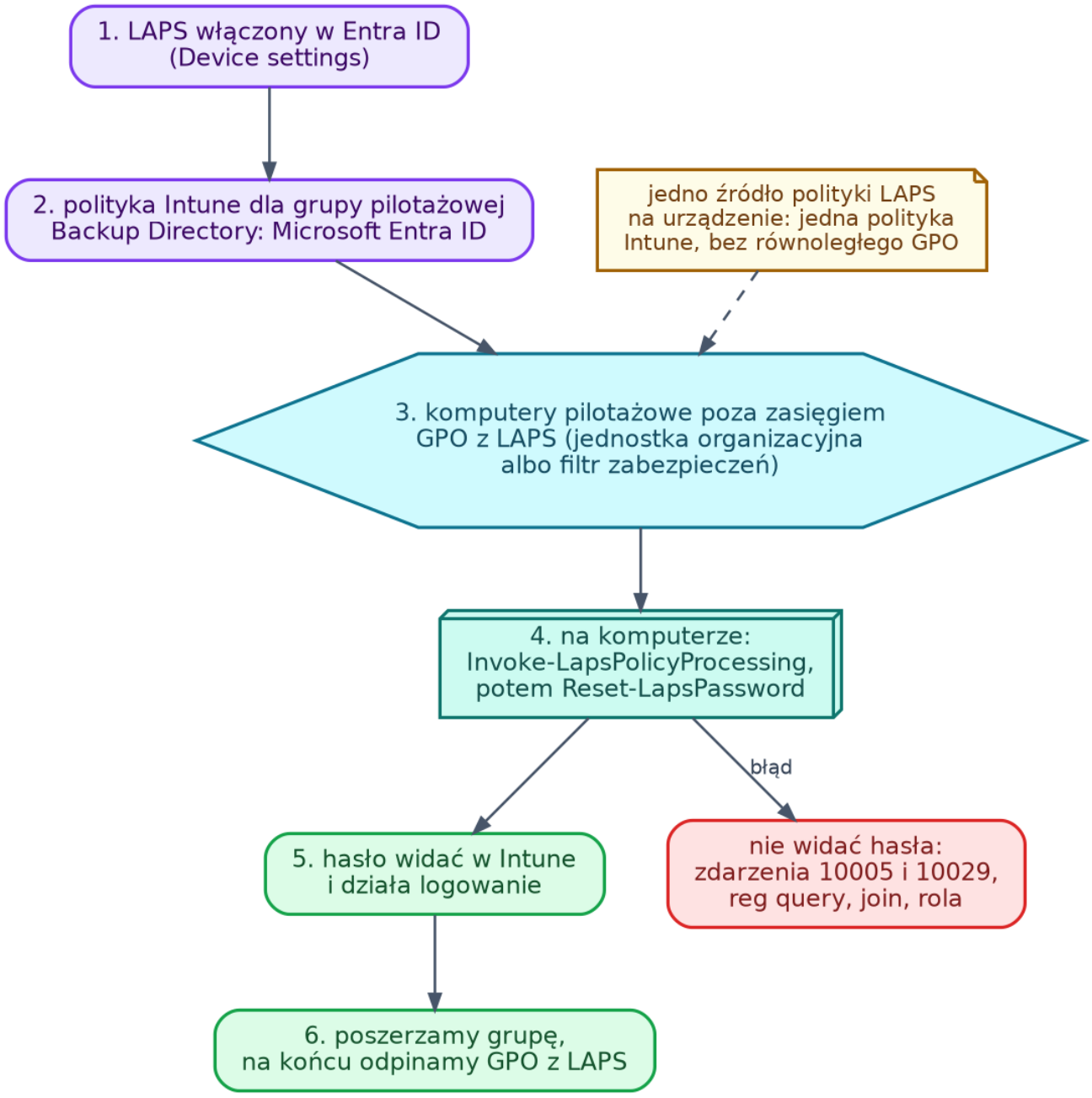
Role wbudowane są szerokie: Cloud Device Administrator zarządza urządzeniami, więc dawanie jej całemu helpdeskowi tylko po to, by czytał hasła, łamie zasadę najmniejszych uprawnień. Zamiast tego tworzymy rolę niestandardową z jednym uprawnieniem `microsoft.directory/deviceLocalCredentials/password/read` (wymaga Entra ID P1, które mamy w Business Premium) i przypisujemy ją grupie pomocy technicznej. Czy do przypisania roli grupa musi być grupą chmurową z włączonym przypisywaniem ról, a nie grupą zsynchronizowaną z AD, sprawdzamy w dokumentacji Entra, zanim zaplanujemy `ZIELONA\Helpdesk`.

Do ręcznej rotacji w Intune potrzebna jest osobna rola Intune, bo uprawnienie Rotate Local Admin Password nie jest w żadnej roli wbudowanej. Politykę LAPS w Intune tworzy rola z

prawami do Security baselines, a w Endpoint Security Manager ma je domyślnie.

Przejście z GPO bez konfliktu

Na komputerach hybrid LAPS już działa z GPO i zapisuje hasło w AD. Przejście do Entra robimy grupami, zaczynając od pilotażu IT, i trzymamy jedną zasadę: jedno źródło polityki na komputer.



Sześć kroków przejścia z GPO na Intune: włączenie w Entra, polityka pilotażowa, wyłączenie GPO dla komputerów pilotażu, wymuszenie przetwarzania i rotacji, kontrola hasła, poszerzanie grupy (kliknięcie otwiera pełny rozmiar)

1. Włączamy LAPS w Entra (fiszka wyżej) i tworzymy rolę z prawem odczytu haseł dla pomocy technicznej.
2. Tworzymy politykę Intune z katalogiem Microsoft Entra ID i przypisujemy ją tylko grupie pilotażowej urządzeń.
3. Wyłączamy GPO z LAPS dla komputerów pilotażowych (inna jednostka organizacyjna albo filtr zabezpieczeń). Polityka z Intune i tak wygrywa, bo CSP jest pierwszym źródłem czytanym przez Windows LAPS, ale ustawień z GPO i z CSP nie łączy, więc zostawianie obu to proszenie się o niespodzianki.
4. Na komputerze pilotażowym uruchamiamy `Invoke-LapsPolicyProcessing`, a potem `Reset-LapsPassword`. Dokumentacja nie opisuje, czy zmiana katalogu sama przenosi bieżące hasło, więc wymuszamy nowe i sprawdzamy, że trafiło do Entra.
5. W Intune odczytujemy hasło i próbujemy zalogować się kontem lokalnym. Dopiero po sukcesie przesuwamy kolejną grupę, a na końcu odpinamy GPO z LAPS od całej jednostki.

Hasło, które zostało w AD, jest po rotacji już nieważne. Atrybut zostaje w katalogu jako ślad, więc w dokumentacji audytowej zapisujemy, od kiedy źródłem prawdy jest Entra, a pomocy technicznej mówimy, żeby nie szukała w AD.

Druga część zasady to jedna polityka Intune na urządzenie. Gdy komputer dostanie dwie polityki LAPS z różnymi ustawieniami, obie zgłaszają konflikt, a komputer zostaje przy ostatniej wartości albo w ogóle nic nie dostaje. Dlatego grupy `Intune-Urzadzenia-Hybrid` i `Intune-Urzadzenia-EntraJoined` nie mogą się pokrywać, a polityki nigdy nie przypisujemy grupom użytkowników.

Audyt

Pan Wojtek zapyta o trzy rzeczy: czy hasła są różne, kto je odczytał i kiedy zostały zmienione. Pierwsze potwierdza sam mechanizm (każdy komputer ma własne, losowe hasło), drugie dziennik audytu Entra z wpisami Recover device local administrator password, trzecie raport w Intune z datami ostatniej i następnej rotacji. Czas przechowywania dziennika audytu Entra zależy od licencji, więc przy wymaganiu dłuższego okresu sprawdzamy go w dokumentacji i ewentualnie eksportujemy wpisy do Log Analytics.

Częste błędy

Objaw	Przyczyna	Co robimy
W Intune brak zakładki Local admin password albo hasło puste	LAPS wyłączony w Entra, komputer jest tylko Entra registered, polityka nie dotarła albo komputer nie wysłał jeszcze hasła	sprawdzamy Device settings w Entra, `dsregcmd /status`, `reg query` i zdarzenia 10005 oraz 10029
Intune nie pokazuje hasła komputera, który ma LAPS	hasło jest w AD, a Intune czyta tylko Entra	używamy `Get-LapsADPassword` albo przenosimy komputer do polityki z Entra
Zdarzenie 10005 po zmianie katalogu	katalog niezgodny z typem dołączenia, na przykład AD dla komputera Entra joined	zmieniamy Backup Directory na zgodny z typem dołączenia
Hasło istnieje, ale nie logujemy się kontem Administrator	wbudowane konto jest wyłączone	`Get-LocalUser`, w razie potrzeby tryb automatycznego zarządzania kontem na 24H2
Ustawienia Automatic Account Management nic nie zmieniają	komputer ma Windows starszy niż 11 24H2	tryb działa tylko na istniejącym koncie, aktualizujemy system albo zostajemy przy Administratorze
Obie polityki LAPS pokazują konflikt	komputer należy do dwóch grup z różnymi politykami LAPS	rozdzielamy grupy tak, żeby każdy komputer miał jedną politykę
Ręczna rotacja w Intune kończy się błędem	brak roli Intune z Remote tasks: Rotate Local Admin Password albo komputer Entra joined jest offline	dokładamy rolę, ponawiamy po włączeniu komputera
`Get-LapsAADPassword` zwraca błąd uprawnień	brak zakresu `DeviceLocalCredential.Read.All` albo roli z prawem odczytu hasła	łączymy się z właściwym zakresem, sprawdzamy rolę
Zdarzenie 10031 w dzienniku LAPS	ktoś albo coś (skrypt, narzędzie) próbuje zmienić hasło zarządzanego konta	szukamy źródła, usuwamy skrypt zmieniający hasło konta
Hasło komputera zniknęło po porządkach w Entra	usunięto obiekt urządzenia w Entra, a hasło jest przy obiekcie i przepada razem z nim	przed usunięciem duplikatów (strona o rejestracji, błędy hybrid join) sprawdzamy, który obiekt ma aktualne hasło, a po usunięciu wymuszamy rotację
Komputer wyłączony w Entra nie zapisuje nowego hasła	zmiana i zapis haseł nie działają dla wyłączonych urządzeń	włączamy obiekt urządzenia

□□ Ćwiczenia

1. Komputer hybrid joined ma GPO z LAPS ze strony o Active Directory i nową politykę Intune z katalogiem Entra. Gdzie trafi hasło i dlaczego mimo to wyłączamy GPO?

Odpowiedź

Windows LAPS czyta źródła polityki po kolei (CSP z Intune, potem GPO) i używa pierwszego, w którym jest choć jedno ustawienie, więc hasło trafi do Entra. Ustawienia z GPO nie uzupełnią polityki z Intune, więc to, czego Intune nie ustawia, wraca do wartości domyślnych, a nie do wartości z GPO. Dlatego GPO wyłączamy, żeby zachowanie komputera było przewidywalne.

1. Pan Zbigniew ma komputer Entra joined z Windows 11 24H2. Jakie trzy ustawienia zmieniają konto, którego hasłem zarządza LAPS, i co się stanie na komputerze z Windows 11 23H2?

Odpowiedź

Włączenie automatycznego zarządzania kontem, wybór konta własnego zamiast wbudowanego oraz losowanie nazwy (przedrostek `ZielonaAdm` z sześcioma cyframi). Na 23H2 te ustawienia nie działają, a LAPS zarządza tylko kontem, które już istnieje, na przykład wbudowanym Administratorem.

1. Tomek chce, żeby cały helpdesk czytał hasła LAPS z Entra. Jaką rolę przypisujemy i czego unikamy?

Odpowiedź

Rolę niestandardową z uprawnieniem `microsoft.directory/deviceLocalCredentials/password/read`, bo Helpdesk Administrator widzi tylko metadane, a Cloud Device Administrator i Intune Administrator mają za szerokie uprawnienia do samego czytania haseł. Unikamy też przypisywania roli pojedynczym osobom na stałe, jeśli da się ją przypisać grupie.

1. Sprzątamy duplikaty obiektów komputerów w Entra po hybrid join przez Autopilot. Co sprawdzamy, zanim usuniemy obiekt, i dlaczego?

Odpowiedź

Czy to jest obiekt, przy którym leży aktualne hasło LAPS. Hasło jest zapisane przy obiekcie urządzenia, a po jego usunięciu przepada i nie ma sposobu odzyskania, więc najpierw ustalamy, który obiekt jest używany, a po sprzątaniu wymuszamy rotację hasła.

Powiązane: Windows LAPS: hasło lokalnego administratora w Active Directory · Profile konfiguracji: katalog ustawień zamiast GPO · Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot · Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy · Intune obok domeny: audyt GPO i plan migracji · BitLocker z Intune: ciche szyfrowanie i klucze odzyskiwania w Entra ID

Źródła: Microsoft Learn, „Windows LAPS overview" (learn.microsoft.com/windows-server/identity/laps/laps-overview) · „Windows LAPS policy settings" (learn.microsoft.com/windows-server/identity/laps/laps-management-policy-settings) · „Windows LAPS account management modes" (learn.microsoft.com/windows-server/identity/laps/laps-concepts-account-management-modes) · „Key concepts in Windows LAPS" (learn.microsoft.com/windows-server/identity/laps/laps-concepts-overview) · „Use Windows LAPS event logs" (learn.microsoft.com/windows-server/identity/laps/laps-management-event-log) · „Get started with Windows LAPS and Microsoft Entra ID" (learn.microsoft.com/windows-server/identity/laps/laps-scenarios-azure-active-directory) · „Migrate from legacy Microsoft LAPS" (learn.microsoft.com/windows-server/identity/laps/laps-scenarios-migration) · „Use Windows LAPS with Microsoft Entra ID" (learn.microsoft.com/entra/identity/devices/howto-manage-local-admin-passwords) · „Windows LAPS in Microsoft Intune" (learn.microsoft.com/intune/device-security/laps/overview oraz .../deploy-policy) · „Get-LapsAADPassword" i „Get-LapsADPassword" (learn.microsoft.com/powershell/module/laps) · „Get deviceLocalCredentialInfo" (learn.microsoft.com/graph/api/devicelocalcredentialinfo-get)

Revision #15
Created 2026-10-03 15:34:00 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:21 UTC by Tomasz Konieczny