Machine Identity Isolation po KB5124008 — diagnoza, obejście, naprawa relacji zaufania

Typ: procedura

Dotyczy: Windows 11 24H2, 25H2 i 26H1 w domenie AD z Credential Guard; kontrolery domeny Windows Server 2019–2025

Czas: ~15 min na diagnozę floty, ~20–30 min na maszynę z zerwaną relacją zaufania

Efekt: wiemy, które maszyny mają Machine Identity Isolation w trybie Enforcement i skąd ten tryb przyszedł; w domenie z kontrolerami poniżej poziomu funkcjonalnego 2025 wartość `MachineIdentityIsolation` *jest ustawiona na 0 przed kolejnymi aktualizacjami, a maszyny, które po KB5124008 straciły relację zaufania, mają naprawiony kanał bezpieczny i logują użytkowników domenowych bez pamięci podręcznej.*

Skróty użyte na tej stronie (9)

Skrót	Co znaczy
AD	Active Directory: katalog kont, komputerów i zasad w domenie Windows
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
KB	Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008)
LAPS	Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów
LSA	Local Security Authority: podsystem Windows obsługujący logowanie i sekrety
NTLM	NT LAN Manager: starszy protokół uwierzytelniania Windows, poprzednik Kerberosa w domenie
VBS	Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows
WinRM	Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting

Fiszka

TYLKO ODCZYT

Odczyt ustawienia MachineIdentityIsolation

```
# polecenia pomocnicze; źródła podają tylko klucze, nazwę wartości i zmianę z 2 na 0
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name
MachineIdentityIsolation -ErrorAction SilentlyContinue
Get-ItemProperty HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard -Name
MachineIdentityIsolation -ErrorAction SilentlyContinue
```

Wartość `2` to tryb Enforcement — ten, który po KB5124008 zrywał relację zaufania. Pierwszy klucz to stan w LSA, drugi — polityka (z GPO albo Intune). Brak wartości w obu miejscach znaczy, że ustawienie nie było konfigurowane. Wartość w kluczu `Policies` ma pierwszeństwo i wraca przy każdym odświeżeniu zasad, więc jeśli tam stoi 2, poprawka musi pójść przez GPO albo Intune, a nie przez lokalny rejestr.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
MachineIdentityIsolation : 2
PSPath                   :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Lsa
```

GPO = Group Policy Object: obiekt zasad grupy w Active Directory · **KB** = Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008) · **LSA** = Local Security Authority: podsystem Windows obsługujący logowanie i sekrety

TYLKO ODCZYT

Czy kanał bezpieczny z domeną działa: Test-ComputerSecureChannel

```
Test-ComputerSecureChannel
```

Bez parametru `-Repair` polecenie tylko sprawdza relację zaufania i zwraca `True` albo `False`. To pierwszy test przy zgłoszeniu „nie mogę się zalogować, choć hasło jest dobre” na maszynie z Credential Guard po wrześniowej aktualizacji. Szczegóły kanału pokazuje też `nltest /sc_verify:nazwa.domeny` (polecenie pomocnicze). `Test-ComputerSecureChannel` jest

udokumentowany tylko dla Windows PowerShell 5.1 — uruchamiamy go w `powershell.exe`, nie w PowerShell 7 (`pwsh`); to samo dotyczy `Remove-Computer` i `Add-Computer` z kroku 5. W `Invoke-Command` z karty inwentaryzacji problem nie występuje, bo domyślny punkt końcowy WinRM to Windows PowerShell 5.1.

TYLKO ODCZYT

Czy Credential Guard i VBS działają: Win32_DeviceGuard

```
# polecenie pomocnicze
Get-CimInstance -Namespace root\Microsoft\Windows\DeviceGuard -ClassName
Win32_DeviceGuard |
    Select-Object VirtualizationBasedSecurityStatus, SecurityServicesRunning
```

`VirtualizationBasedSecurityStatus` = 2 oznacza, że VBS działa; liczba 1 w `SecurityServicesRunning` — że działa Credential Guard. Machine Identity Isolation przenosi sekret konta komputera właśnie do Credential Guard, więc na maszynie bez działającego Credential Guard problem z tej strony nie występuje — a na maszynie w trybie Enforcement, na której Credential Guard po restarcie nie wystartuje, uwierzytelnienie w domenie jest niemożliwe.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
VirtualizationBasedSecurityStatus SecurityServicesRunning
--------------------------------- ----------------------
                                2 {1, 2}
```

VBS = Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows

TYLKO ODCZYT

Poziom funkcjonalny domeny i wersje kontrolerów

```
# polecenia pomocnicze; moduł ActiveDirectory
(Get-ADDomain).DomainMode
Get-ADDomainController -Filter * | Select-Object Name, OperatingSystem
```

Według relacji IT-Connect Machine Identity Isolation działa poprawnie tylko z kontrolerami domeny przy **poziomie funkcjonalnym domeny Windows Server 2025**; w środowiskach z kontrolerami 2019 i 2022 kanał bezpieczny się zrywa. Tego wymogu nie ma w pobranej dokumentacji Microsoftu — traktujemy go jako górną granicę ryzyka, nie jako potwierdzony

warunek. Jeśli `DomainMode` jest niższy niż Windows Server 2025, zakładamy, że domena jest narażona.

Czym jest i co się stało

> **Pojęcie: Machine Identity Isolation.** W dokumentacji „Credential Guard protected machine accounts". Przenosi sekret **konta komputera** z rejestru i LSA do odizolowanego środowiska Credential Guard w VBS, tak żeby nie mieli do niego dostępu ani nieuprzywilejowani użytkownicy, ani administratorzy, ani sterowniki. Tryby: **Audit** — sekret w Credential Guard plus kopia w LSA, z powrotem do LSA przy błędzie; **Enforcement** — sekret przeniesiony do Credential Guard i usunięty z LSA; **Disabled** — po wcześniejszym Enforcement wymaga odłączenia i ponownego przyłączenia do domeny. W GPO ustawienie leży pod Konfiguracja komputera → Szablony administracyjne → System → Device Guard → Turn On Virtualization Based Security.

Microsoft ostrzega w dokumentacji, że jeśli w trybie Enforcement Credential Guard nie wystartuje po restarcie, „skutkuje to niemożnością uwierzytelnienia w domenie, potencjalnie wymagając interwencji z lokalnego konta administratora". Dokumentacja wspomina też, że funkcja była „tymczasowo wyłączona w Windows Server 2025 i Windows 11 24H2" z powodu problemu z rotacją hasła maszyny w Kerberosie.

Potwierdzone przez Microsoft: w sekcji znanych problemów noty **KB5124008** (8 września 2026) urządzenia „z kontami maszyn chronionymi przez Credential Guard mogą utracić bezpieczną relację zaufania z domeną po zainstalowaniu tej aktualizacji lub późniejszych". Objawy według BleepingComputer: błędy relacji zaufania mimo poprawnych poświadczeń, logowanie działające tylko z pamięci podręcznej, awarie Kerberosa z przejściem na NTLM i Netlogon. Microsoft potwierdził problem i podał obejście **18 września 2026**.

Tylko z prasy (IT-Connect): aktualizacja nie włącza funkcji sama, lecz „wymusza respektowanie istniejących ustawień, które włączały ten tryb" — na przykład wartości 2 wpisanej wcześniej przez bazę bezpieczeństwa albo szablon; problem dotyczy 24H2, 25H2 i 26H1, a warunkiem poprawnego działania jest poziom funkcjonalny domeny Windows Server 2025.

Zanim zaczniemy

Mamy **dostęp do lokalnego konta administratora** na maszynach, które będziemy naprawiać — maszyna bez relacji zaufania nie zaloguje domenowego administratora spoza pamięci podręcznej. Hasła lokalnych administratorów trzymamy w Windows LAPS; odczyt hasła z AD albo Entra ID opisuje strona Windows LAPS. Do maszyn wirtualnych mamy dostęp przez konsolę hypervisora, do

fizycznych — przez kogoś na miejscu albo zdalną konsolę sprzętową.

Ustalamy, **skąd przyszła wartość 2**: najczęściej z bazy bezpieczeństwa Microsoftu dla 24H2 lub 25H2 wdrożonej jako GPO, z szablonu Intune „Account protection” albo z bazy bezpieczeństwa w Intune. Dopóki źródło ustawienia jest aktywne, lokalna zmiana wróci przy najbliższym odświeżeniu zasad.

Wydzielamy grupę testową kilku maszyn, na których zmianę zrobimy pierwszą, i robimy kopię zapasową obu kluczy (polecenie pomocnicze):

```
reg export HKLM\SYSTEM\CurrentControlSet\Control\Lsa C:\Temp\lsa-przed.reg /y
reg export HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard C:\Temp\deviceguard-przed.reg
/y
```

Przebieg

1. Inwentaryzacja floty

TYLKO ODCZYT

MachineIdentityIsolation, Credential Guard i kanał bezpieczny na wielu maszynach

```
# polecenie pomocnicze; klucze i nazwa wartości z BleepingComputer i IT-Connect
$komputery = Get-Content .\komputery.txt
Invoke-Command -ComputerName $komputery -ScriptBlock {
    $lsa = (Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -ErrorAction
SilentlyContinue).MachineIdentityIsolation
    $pol = (Get-ItemProperty HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard -
ErrorAction SilentlyContinue).MachineIdentityIsolation
    $dg  = Get-CimInstance -Namespace root\Microsoft\Windows\DeviceGuard -ClassName
Win32_DeviceGuard
    [pscustomobject]@{
        MII_Lsa         = $lsa
        MII_Polityka    = $pol
        CredentialGuard = ($dg.SecurityServicesRunning -contains 1)
        KanalOK         = Test-ComputerSecureChannel
```

```
        Wydanie         = (Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion').DisplayVersion
    }
} -Credential (Get-Credential) |
    Select-Object PSComputerName, MII_Lsa, MII_Polityka, CredentialGuard, KanalOK,
Wydanie |
    Export-Csv .\mii-inwentaryzacja.csv -NoTypeInformation -Encoding UTF8
```

Na maszynach, które już straciły relację zaufania, połączenie przez WinRM kontem domenowym zwykle się nie uda — te maszyny wypadną z wyniku z błędem połączenia i to też jest informacja. Interesują nas wiersze z wartością 2 w którejkolwiek kolumnie `MII_` i z `CredentialGuard` = `True`: to maszyny narażone przy kolejnej aktualizacji. Konfigurację WinRM opisuje WinRM — zarządzanie zdalne.

WinRM = Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting

2. Ustalenie źródła ustawienia

```
# polecenie pomocnicze
gpresult /scope computer /h C:\Temp\gpresult.html
```

W raporcie szukamy GPO, które konfiguruje Device Guard → Turn On Virtualization Based Security. W Intune przeglądamy profile „Account protection” i przypisane bazy bezpieczeństwa dla 24H2 i 25H2. Zapisujemy nazwę GPO albo profilu — to w nim zrobimy zmianę w kroku 3.

3. Wyłączenie Machine Identity Isolation

Na flocie zmieniamy ustawienie **w źródle**: w GPO z kroku 2 albo w profilu Intune przestawiamy Machine Identity Isolation z Enforcement na wyłączone. Na maszynach z grupy testowej, żeby nie czekać na odświeżenie zasad, możemy zmienić wartość lokalnie:

ZMIENIA SYSTEM

Zmiana MachineIdentityIsolation z 2 na 0 i restart

```
# polecenie pomocnicze; klucze, nazwa wartości i zmiana z 2 na 0 — z BleepingComputer i
IT-Connect
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name
```

```
MachineIdentityIsolation -Value 0 -Type DWord
Set-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard -Name
MachineIdentityIsolation -Value 0 -Type DWord
Restart-Computer
```

Obejście podane przez BleepingComputer i IT-Connect: wyłączyć Machine Identity Isolation (Intune, GPO albo rejestr), zrestartować i naprawić kanał. Jeśli po restarcie w kluczu `Policies` znów stoi 2, to GPO albo Intune nadal wymusza Enforcement — wracamy do kroku 2. Przy kontrolerach domeny poniżej poziomu funkcjonalnego 2025 ustawiamy 0 na wszystkich maszynach z Credential Guard **przed** kolejnymi aktualizacjami, zanim zrobi to za nas awaria.

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

4. Naprawa kanału bezpiecznego

ZMIENIA SYSTEM

Naprawa relacji zaufania: Test-ComputerSecureChannel -Repair

```
Test-ComputerSecureChannel -Repair -Credential (Get-Credential)
```

Polecenie z BleepingComputer i IT-Connect. Uruchamiamy w PowerShellu jako administrator — na maszynie bez relacji zaufania logujemy się w tym celu lokalnym kontem administratora. W oknie poświadczeń podajemy konto domenowe z prawem resetowania konta komputera. Wynik `True` znaczy, że kanał jest naprawiony; wylogowujemy się i logujemy kontem domenowym. O pracy z poświadczeniami w skryptach — Poświadczenia i bezpieczne hasła w skryptach.

5. Gdy naprawa kanału nie wystarcza

OSTROŻNIE · NIEODWRACALNE

Odłączenie od domeny i ponowne przyłączenie

```
# polecenia pomocnicze; wymóg odłączenia i ponownego przyłączenia — z dokumentacji
Microsoftu
# krok A: odłączenie (po restarcie maszyna zna już tylko konta lokalne)
```

```
Remove-Computer -UnjoinDomainCredential (Get-Credential) -WorkgroupName TYMCZASOWA -
Restart


# krok B: po restarcie, zalogowani lokalnym kontem administratora
Add-Computer -DomainName nazwa.domeny -Credential (Get-Credential) -Restart
```

Dokumentacja Microsoftu mówi wprost, że przejście do trybu Disabled po wcześniejszym Enforcement wymaga odłączenia i ponownego przyłączenia do domeny — więc jeśli po krokach 3 i 4 `Test-ComputerSecureChannel` nadal zwraca `False`, to jest właściwa droga, a nie kolejne próby naprawy. `Remove-Computer` domyślnie pyta o potwierdzenie i przy odłączeniu wyłącza konto komputera w AD (dokumentacja cmdletu) — nie dodajemy `-Force`, żeby to pytanie zostało. Karta jest czerwona, bo po kroku A maszyna nie zaloguje już żadnego konta domenowego: **bez działającego hasła lokalnego administratora zostaje tylko reinstalacja**. Przed krokiem A sprawdzamy więc hasło z LAPS, logując się nim lokalnie, a nie tylko odczytując je z katalogu.

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

Weryfikacja

`Test-ComputerSecureChannel` zwraca `True`, a `nltest /sc_verify:nazwa.domeny` pokazuje poprawny kanał. Użytkownik domenowy, który **nigdy wcześniej** nie logował się na tej maszynie, loguje się bez błędu — to jedyny test, który wyklucza logowanie z pamięci podręcznej. `klist` (polecenie pomocnicze) pokazuje bilety Kerberos wydane przez kontroler domeny, a nie pustą listę. W wyniku skryptu z kroku 1, uruchomionego ponownie po kilku dniach, nie ma już wartości 2 w kolumnach `MII_`.

Wycofanie zmian

Przywrócenie trybu Enforcement ma sens dopiero wtedy, gdy kontrolery domeny i poziom funkcjonalny domeny są na Windows Server 2025 i gdy grupa testowa przejdzie z nim co najmniej jeden cykl aktualizacji bez utraty relacji zaufania. Wracamy wtedy do wartości 2 w GPO albo w Intune; kopie `.reg` sprzed zmiany służą do porównania, a nie do bezmyślnego importu. Pamiętamy o asymetrii: włączenie Enforcement jest proste, a ponowne wyłączenie po nim — według dokumentacji — wymaga odłączenia i ponownego przyłączenia do domeny. Poziomy funkcjonalne i kontrolery opisują strony serii o Active Directory i o Windows Server 2008–2025.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
Po wrześniowej aktualizacji błąd relacji zaufania mimo poprawnego hasła	Machine Identity Isolation w trybie Enforcement, respektowana od KB5124008	kroki 3 i 4
Użytkownicy logują się tylko ci, którzy logowali się wcześniej	logowanie z pamięci podręcznej; kanał z domeną zerwany	`Test-ComputerSecureChannel`, potem kroki 3 i 4
Awarie Kerberosa, w dziennikach przejście na NTLM i Netlogon	ten sam problem widziany od strony uwierzytelniania	kroki 3 i 4; po domyślnym wyłączeniu sieciowego NTLM ta ścieżka awaryjna zniknie — patrz Bezpieczeństwo domyślne
Po restarcie wartość w kluczu `Policies` znów wynosi 2	GPO albo profil Intune nadal wymusza Enforcement	zmiana w źródle ustawienia (krok 2)
`Test-ComputerSecureChannel -Repair` zwraca `False`	konto bez prawa resetu konta komputera, brak łączności z kontrolerem albo stan po Enforcement wymagający ponownego przyłączenia	konto z właściwymi uprawnieniami, sprawdzenie DNS i łączności; jeśli nadal `False` — krok 5
Po restarcie w trybie Enforcement nikt z domeny nie może się zalogować	Credential Guard nie wystartował — ostrzeżenie z dokumentacji Microsoftu	lokalne konto administratora (hasło z LAPS), wyłączenie Enforcement, restart, naprawa kanału
Brak hasła lokalnego administratora na maszynie bez relacji zaufania	LAPS nie był wdrożony albo hasło w nieznanym katalogu	konsola i procedura odzyskiwania konta albo reinstalacja; na przyszłość — Windows LAPS

Powiązane: Windows 11 w firmie 2026 — przegląd zmian · Windows LAPS · Bezpieczeństwo domyślne 24H2/25H2 · WinRM — zarządzanie zdalne · Skrypty audytowe Active Directory · Poświadczenia i bezpieczne hasła w skryptach

Źródła: KB5124008 — znane problemy · Credential Guard protected machine accounts · BleepingComputer — zerwana relacja zaufania · IT-Connect — mechanizm

---

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