Odporność i AI w firmie — Quick Machine Recovery, Recall i Click to Do

Typ: fiszka **Poziom: średniozaawansowany**

Dotyczy: Windows 11 24H2+ (QMR: kompilacja 26100.4700+), Copilot+ PC, urządzenia zarządzane przez Intune albo GPO

Czas: ~25 min

Efekt: wiemy, dlaczego po awarii z 19 lipca 2024 roku maszyny w domenie nadal nie naprawią się same, dopóki nie włączymy Quick Machine Recovery, jak sprawdzić, że środowisko odzyskiwania w ogóle działa, i jakie decyzje trzeba świadomie podjąć wobec Recall (domyślnie usunięty) i Click to Do (domyślnie włączony) na urządzeniach firmowych.

Skróty użyte na tej stronie (16)

Skrót	Co znaczy
AI	Artificial Intelligence: sztuczna inteligencja
CSP	Configuration Service Provider: interfejs ustawień Windows sterowany przez MDM, np. Intune
EDR	Endpoint Detection and Response: agent wykrywający i blokujący ataki na stacji
EOG	Europejski Obszar Gospodarczy: UE oraz Islandia, Liechtenstein i Norwegia
ESS	Enhanced Sign-in Security: izolacja biometrii Windows Hello w VBS
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
KB	Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008)
MVI	Microsoft Virus Initiative: program współpracy Microsoftu z producentami antywirusów
NPU	Neural Processing Unit: układ do obliczeń sieci neuronowych
PC	Personal Computer: komputer osobisty
QMR	Quick Machine Recovery: automatyczne naprawianie niestartującego Windows z chmury
TOPS	Tera Operations Per Second: bilion operacji na sekundę, miara mocy NPU

Skrót	Co znaczy
UTC	Coordinated Universal Time: uniwersalny czas koordynowany
WinRE	Windows Recovery Environment: środowisko odzyskiwania Windows
WPA	Wi-Fi Protected Access: zabezpieczenie sieci Wi-Fi hasłem
XML	Extensible Markup Language: tekstowy format danych ze znacznikami

Fiszka

□□ TYLKO ODCZYT

Czy środowisko odzyskiwania działa: reagentc /info

```
reagentc /info
```

Quick Machine Recovery uruchamia maszynę do WinRE, więc bez sprawnego WinRE nie zadziała wcale. Sprawdzamy, że status jest `Enabled` i że wskazana jest lokalizacja obrazu. Po latach aktualizacji partycja odzyskiwania bywa za mała — notatka, na której opiera się ta strona, łączy to ze znanym problemem KB5034441 z 2024 roku, ale tego nie weryfikowała.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
Windows RE status:         Enabled
Windows RE location:       \\?\GLOBALROOT\device\harddisk0\partition4\Recovery\WindowsRE
```

□□ **KB** = Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008) · **WinRE** = Windows Recovery Environment: środowisko odzyskiwania Windows

□□ TYLKO ODCZYT

Ustawienia Quick Machine Recovery: reagentc /getrecoverysettings

```
reagentc.exe /getrecoverysettings
```

Zwraca XML z bieżącą konfiguracją: `CloudRemediation` (czy maszyna ma szukać poprawki w Windows Update), `AutoRemediation` z atrybutami `totalwaittime` i `waitinterval` (skan jednorazowy albo w pętli z interwałem) oraz opcjonalnie poświadczenia Wi-Fi. Po wdrożeniu polityki z Intune tu sprawdzamy, że dotarła.

□□ **XML** = Extensible Markup Language: tekstowy format danych ze znacznikami

□□ TYLKO ODCZYT

Czy kompilacja obsługuje QMR

```
# polecenie pomocnicze; próg kompilacji z dokumentacji Microsoftu
$cv = Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion'
[pscustomobject]@{
    Kompilacja = "$($cv.CurrentBuild).$($cv.UBR)"
    QMRMozliwy = ([int]$cv.CurrentBuild -gt 26100) -or ([int]$cv.CurrentBuild -eq 26100
-and [int]$cv.UBR -ge 4700)
}
```

Quick Machine Recovery wymaga Windows 11 24H2 w kompilacji **26100.4700** lub nowszej. Maszyna z 23H2 albo z nieaktualnym 24H2 nie skorzysta z polityki, nawet jeśli ją dostanie.

□□ **QMR** = Quick Machine Recovery: automatyczne naprawianie niestartującego Windows z chmury

□□ ZMIENIA SYSTEM

Tryb testowy QMR (tylko kompilacje Insider)

```
# wiersz polecenia jako administrator; kolejność i pisownia jak w dokumentacji
Microsoftu
reagentc.exe /SetRecoveryTestmode
reagentc.exe /BootToRe
# potem ręczny restart
```

Tryb testowy dokumentacja przewiduje wyłącznie dla urządzeń w kanale Experimental programu Windows Insider: pierwsze polecenie włącza symulację, drugie każe przy następnym rozruchu wejść do WinRE, gdzie po ręcznym restarcie maszyna przechodzi ścieżkę naprawy tak, jakby nie mogła się uruchomić, i sama restartuje się z powrotem do Windows. Osobnego polecenia wyłączającego tryb testowy dokumentacja nie podaje — symulacja jest jednorazowa. Robimy to wyłącznie na maszynie testowej z kanału Insider, z kablem sieciowym — i z kluczem BitLockera pod ręką, bo WinRE może o niego poprosić.

□□ **QMR** = Quick Machine Recovery: automatyczne naprawianie niestartującego Windows z chmury · **WinRE** = Windows Recovery Environment: środowisko odzyskiwania Windows

□□ TYLKO ODCZYT

Czy na urządzeniu jest składnik Recall

```
# polecenie pomocnicze
Get-WindowsOptionalFeature -Online | Where-Object FeatureName -like '*Recall*' |
    Select-Object FeatureName, State
```

Na urządzeniach zarządzanych Recall jest domyślnie **wyłączony i usunięty**; na komputerze, który nie jest Copilot+ PC, składnika zwykle w ogóle nie ma. Wynik pokazuje, czy polityka zadziałała tak, jak zakładamy, i czy ktoś go nie dopuścił.

PC = Personal Computer: komputer osobisty

OSTROŻNIE · NIEODWRACALNE

Zakaz Recall: Allow Recall to be enabled

```
./Device/Vendor/MSFT/Policy/Config/WindowsAI/AllowRecallEnablement
```

Polityka „Allow Recall to be enabled” — CSP jak wyżej, w GPO pod Składniki systemu Windows → Windows AI. Ustawienie jej na „nie zezwalaj” (w CSP wartość `0` — Recall niedostępny; domyślnie `1`) **usuwa komponent i kasuje istniejące migawki** — migawek nie da się potem odzyskać. Na urządzeniu, na którym użytkownik świadomie korzystał z Recall, uprzedzamy go przed zmianą. Druga polityka, „Turn off saving snapshots for Recall” (CSP `…/WindowsAI/DisableAIDataAnalysis`), wyłącza tylko zapisywanie nowych migawek.

AI = Artificial Intelligence: sztuczna inteligencja · **CSP** = Configuration Service Provider: interfejs ustawień Windows sterowany przez MDM, np. Intune · **GPO** = Group Policy Object: obiekt zasad grupy w Active Directory

ZMIENIA SYSTEM

Wyłączenie Click to Do: DisableClickToDo

```
./Device/Vendor/MSFT/Policy/Config/WindowsAI/DisableClickToDo
./User/Vendor/MSFT/Policy/Config/WindowsAI/DisableClickToDo
```

Click to Do jest na urządzeniach komercyjnych **domyślnie włączony**. Wyłącza się go przez CSP `DisableClickToDo` — dla urządzenia i dla użytkownika (obie ścieżki według dokumentacji Policy CSP WindowsAI; `1` — wyłączony, `0` — domyślnie włączony) — albo w GPO ustawieniem „Disable Click to Do” (Składniki systemu Windows → Windows AI, w konfiguracji komputera i użytkownika). Zmianę wdrażamy najpierw na grupie pilotażowej; wycofanie to przywrócenie wartości `0` albo usunięcie przypisania polityki. Polityka nie dotyczy Click to Do

wewnątrz Recall.

CSP = Configuration Service Provider: interfejs ustawień Windows sterowany przez MDM, np. Intune · **GPO** = Group Policy Object: obiekt zasad grupy w Active Directory

Po co to istnieje

Wadliwa aktualizacja CrowdStrike Falcon z 19 lipca 2024 roku dotknęła według Microsoftu 8,5 mln urządzeń z Windows, „mniej niż 1% wszystkich maszyn z Windows”; wysłano ją o 04:09 UTC i wycofano o 05:27 UTC (godziny według centrum pomocy CrowdStrike) — tyle że ten procent to były maszyny krytyczne, a firmowe komputery w domenie wymagały ręcznej wizyty z kluczem BitLockera. Odpowiedzią Microsoftu jest Windows Resiliency Initiative — nazwę ogłoszono prawdopodobnie na Ignite w listopadzie 2024, wpisu nie udało się pobrać — a jej konkretny program 26 czerwca 2025: nowy, czarny ekran nieoczekiwanego restartu z kodem zatrzymania, dostępny od późnego lata 2025 na wszystkich urządzeniach 24H2 (koniec niebieskiego ekranu po mniej więcej czterdziestu latach), **Quick Machine Recovery** i antywirusy działające poza jądrem, w trybie użytkownika (prywatny podgląd platformy w ramach MVI 3.0 od lipca 2025; komunikatu o wyjściu z podglądu do września 2026 nie znalazłem; partnerzy to Bitdefender, CrowdStrike, ESET, SentinelOne, Sophos, Trellix, Trend Micro i WithSecure). Pojawia się też argument, że Microsoft nie może jednostronnie wyrzucić producentów EDR z jądra z powodu zobowiązania wobec Komisji Europejskiej z 2009 roku — źródła nie pobrano, więc tylko go odnotowuję. Partnerzy MVI muszą od tamtej pory wdrażać aktualizacje „stopniowo, korzystając z pierścieni wdrożeniowych i monitorowania”.

Recall i Click to Do to druga strona tej samej strony: funkcje AI z lokalną analizą ekranu, które na urządzeniu firmowym trzeba świadomie dopuścić albo wyłączyć. Historię publicznego odwrotu Microsoftu od pierwszej wersji Recall opowiada strona serii o Windows 11.

Jak to działa

Quick Machine Recovery

Przy awarii uniemożliwiającej rozruch maszyna startuje do **WinRE**, łączy się z siecią i szuka poprawki w Windows Update; zastosowane poprawki widać potem w Historii aktualizacji jako aktualizacje jakościowe. Dwa ustawienia: **Cloud remediation** — bez niego zostaje tylko lokalna Naprawa uruchamiania — i **Auto remediation**, czyli skan jednorazowy albo w pętli z interwałem. Konfiguracja przez **Recovery CSP** (`QuickMachineRecovery`), na przykład z Intune; weryfikacja — `reagentc.exe /getrecoverysettings`.

Edycja i sposób zarządzania	QMR domyślnie
Home	włączony (skan jednorazowy)
Pro niezarządzany	włączony (skan jednorazowy)
Pro w domenie	**wyłączony**
Enterprise, Education	**wyłączony**

> Dwa ograniczenia, oba udokumentowane. QMR jest domyślnie wyłączony dokładnie tam, gdzie 19 lipca 2024 roku był najbardziej potrzebny — na Pro w domenie i w Enterprise. I łączy się z siecią **tylko przez kabel albo Wi-Fi WPA/WPA2 z hasłem — bez 802.1X**, co wyklucza typową sieć firmową. Laptop w biurze z samym Wi-Fi 802.1X nie naprawi się sam, nawet z włączoną polityką.

Recall na urządzeniach firmowych

Dokumentacja zarządzania mówi: „Domyślnie Recall jest wyłączony i usunięty na urządzeniach zarządzanych”; użytkownik nie może go sam włączyć, jeśli polityka na to nie pozwala. Administrator **nie może wymusić** zapisywania migawek — potrzebna jest zgoda użytkownika. Wymagania są twarde: Copilot+ PC w standardzie Secured-core, NPU 40 TOPS, 16 GB pamięci, 8 procesorów logicznych, 256 GB dysku (50 GB wolnego, żeby włączyć; wstrzymanie poniżej 25 GB), **Windows Hello Enhanced Sign-in Security z biometrią** oraz szyfrowanie urządzenia albo BitLocker. Eksport migawek jest dostępny tylko w EOG — a więc także w Polsce.

Zależność od Enhanced Sign-in Security ma skutek praktyczny: przy włączonym ESS nie działają zewnętrzne kamery i czytniki Hello, więc laptop Copilot+ podłączony do stacji dokującej z zewnętrzną kamerą to konflikt — albo Recall, albo zewnętrzna kamera. Szczegóły ESS są na stronie Bezpieczeństwo domyślne 24H2/25H2.

Click to Do

Click to Do (Win+Q albo Win+kliknięcie) to lokalna analiza zawartości ekranu modelem **Phi Silica** na NPU: akcje na tekście — podsumuj, przepisz, zrób listę, szkic w Wordzie — i na obrazach — wyszukiwanie wizualne, rozmycie albo usunięcie obiektu w Zdjęciach — plus przekazanie do Teams i poczty. **W odróżnieniu od Recall jest domyślnie włączony na urządzeniach komercyjnych.** Języki: angielski w pełni, francuski i hiszpański częściowo; polskiego nie ma.

> Decyzja do podjęcia, a nie do odziedziczenia. Microsoft wyznacza granicę ryzyka według **trwałości danych**: Recall, który zapisuje historię ekranu, jest w firmie domyślnie usunięty,

> a Click to Do, który analizuje ekran tym samym rodzajem lokalnego modelu, ale nie zapisuje historii — domyślnie włączony. Jeśli polityka firmy mówi o analizie treści ekranu, a nie o jej przechowywaniu, Click to Do trzeba wyłączyć jawnie.

Analogia

Quick Machine Recovery w firmowej flocie przypomina gaśnicę, która w budynkach mieszkalnych wisi na korytarzu, a w biurowcu — domyślnie w szafce zamkniętej na klucz, bo zarządca budynku ma podobno własne procedury. Klucz do szafki to polityka Recovery CSP: dopóki jej nie wdrożymy, gaśnica jest, ale nikt po nią nie sięgnie. Ograniczenie analogii: nawet otwarta szafka nie pomoże, jeśli do gaśnicy prowadzą tylko drzwi na kartę 802.1X — QMR nie obsługuje takiej sieci, więc część maszyn i tak trzeba będzie odwiedzić.

Częste błędy

Założenie, że QMR „jest w 24H2, więc działa”. Na Pro w domenie i w Enterprise jest domyślnie wyłączony; bez polityki maszyna po awarii rozruchu czeka na człowieka.

Włączenie QMR bez sprawdzenia WinRE. Jeśli `reagentc /info` pokazuje `Disabled` albo partycja odzyskiwania jest za mała, polityka niczego nie zmieni.

Testowanie QMR na laptopie w sieci 802.1X. QMR łączy się tylko przez kabel albo Wi-Fi WPA/WPA2 z hasłem; brak połączenia w teście nie oznacza błędu polityki.

Wyłączenie Recall na urządzeniu, na którym użytkownik go używał, bez uprzedzenia. Wyłączenie polityki „Allow Recall to be enabled” usuwa komponent i kasuje istniejące migawki.

Pominięcie Click to Do w polityce AI. Recall jest domyślnie usunięty, więc wydaje się, że „AI na ekranie” jest załatwione — a Click to Do jest domyślnie włączony.

□□ Ćwiczenia

> Ćwiczenia wymagają maszyny testowej z Windows 11 24H2 lub 25H2 w domenie, z uprawnieniami administratora.

Ćwiczenie 1 — stan odzyskiwania przed polityką i po niej

```
reagentc /info
reagentc.exe /getrecoverysettings
```

Uruchamiamy oba polecenia na maszynie w domenie przed przypisaniem polityki Recovery CSP i po nim. Czego oczekujemy w pierwszym odczycie?

Odpowiedź

Na Pro w domenie i na Enterprise QMR jest domyślnie wyłączony, więc przed polityką XML nie pokazuje włączonej naprawy z chmury. Po wdrożeniu polityki `CloudRemediation` i `AutoRemediation` mają wartości z polityki. Jeśli `reagentc /info` pokazuje WinRE jako wyłączone, polityka nie ma na czym działać — najpierw trzeba naprawić WinRE.

Pytania kontrolne

1. Czy administrator może polityką wymusić, żeby Recall zapisywał migawki na laptopie pracownika?

Odpowiedź

Nie może. Dokumentacja mówi wprost, że administrator nie może wymusić zapisywania migawek — potrzebna jest zgoda użytkownika. Polityką administrator może Recall dopuścić, zakazać (co usuwa komponent i kasuje migawki) albo wyłączyć zapisywanie nowych migawek.

2. Dlaczego na tym samym urządzeniu firmowym Recall jest domyślnie usunięty, a Click to Do domyślnie włączony?

Odpowiedź

Bo Microsoft traktuje jako ryzyko przede wszystkim trwałą historię ekranu, którą zapisuje Recall; Click to Do analizuje ekran lokalnie, ale nie zapisuje historii, więc jest domyślnie włączony. Firma, która nie chce żadnej analizy treści ekranu, musi go wyłączyć jawnie przez `DisableClickToDo` albo GPO „Disable Click to Do”.

Powiązane: Windows 11 w firmie 2026 — przegląd zmian · Bezpieczeństwo domyślne 24H2/25H2 · Secure Boot: wymiana certyfikatów 2011 → 2023 · Skrypty audytowe Active Directory

Źródła: Quick Machine Recovery · The Windows Resiliency Initiative, 26 VI 2025 · Microsoft o awarii CrowdStrike · Manage Recall · Manage Click to Do · Windows Hello ESS

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