Urządzenia i zasady

Rejestracja urządzeń, zgodność i dostęp warunkowy.

- Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot
- Zasady zgodności i dostęp warunkowy

Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot

Poziom: średniozaawansowany
Dotyczy: Windows 11, Microsoft Entra ID, Intune, Windows Autopilot **Czas: ~45 min**

Zanim Intune cokolwiek zrobi z komputerem, komputer musi być w Microsoft Entra ID i zarejestrowany w usłudze zarządzania. Strona porównuje cztery drogi (Entra joined, hybrid joined, Entra registered i Autopilot), mówi uczciwie, co jest możliwe dla istniejących komputerów domenowych, i pokazuje, jak sprawdzić, że rejestracja się udała.

Skróty użyte na tej stronie (15)

Skrót	Co znaczy
ANSI	American National Standards Institute: tu chodzi o kody sterujące kolorem i pozycją kursora w terminalu
CSV	w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
LAPS	Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu
LOB	Line of Business: aplikacja biznesowa dodawana do Intune jako własny plik instalacyjny, na przykład pakiet MSI
MDM	Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi
MSI	Microsoft Installer: format paczki instalacyjnej Windows
OOBE	Out-of-Box Experience: ekrany pierwszego uruchomienia Windows, na których komputer dołącza się do Entra ID i dostaje konfigurację z Autopilot
SCEP	Simple Certificate Enrollment Protocol: protokół, którym urządzenie samo prosi urząd certyfikacji o wystawienie certyfikatu

Skrót	Co znaczy
SCP	Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
TPM	Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii

Fiszka

Komendy wykonujemy w wierszu poleceń lub PowerShellu na komputerze, którego dotyczą, z uprawnieniami administratora lokalnego. Ścieżki w centrach administracyjnych podajemy po angielsku, tak jak w dokumentacji. Microsoft przenosi pozycje menu, więc w razie rozbieżności szukamy po nazwie.

TYLKO ODCZYT

Sprawdzenie stanu dołączenia: dsregcmd /status

```
dsregcmd /status
```

Pokazuje, jak komputer jest związany z Microsoft Entra ID. Interesują nas trzy wiersze w sekcji Device State: `AzureAdJoined`, `DomainJoined` i `WorkplaceJoined` (ten ostatni w sekcji User State, więc polecenie uruchamiamy w kontekście zalogowanego użytkownika).

Przykład dla komputera domenowego po udanym hybrid join:

```
+----------------------------------------------------------------------+
| Device State                                                         |
+----------------------------------------------------------------------+

             AzureAdJoined : YES
          EnterpriseJoined : NO
              DomainJoined : YES
                DomainName : AD
```

```
           Device Name : ws-ksiegowosc01.ad.zielona.example

+----------------------------------------------------------------------+
| Tenant Details                                                       |
+----------------------------------------------------------------------+

                MdmUrl :
https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc

+----------------------------------------------------------------------+
| User State                                                           |
+----------------------------------------------------------------------+

                NgcSet : NO
         WorkplaceJoined : NO
```

Samą stronę wyniku zawężamy tak:

```
dsregcmd /status | Select-String
"AzureAdJoined|DomainJoined|WorkplaceJoined|DeviceAuthStatus|MdmUrl"
```

dsregcmd = Device Registration Command: pokaż, czy komputer jest dołączony do Entra ID, domeny albo zarejestrowany, i zdiagnozuj rejestrację

TYLKO ODCZYT

Odczyt diagnostyki przed dołączeniem: dsregcmd /status jako administrator

```
dsregcmd /status
```

> (uruchamiane w podniesionym wierszu poleceń, bo tylko wtedy sekcja diagnostyczna dotyczy kontekstu systemowego; po więcej szczegółów sięgamy po `dsregcmd /debug`)

Gdy komputer jest w domenie, ale nie dołącza do Entra ID, wynik zawiera sekcję Diagnostic Data z testami: `AD Connectivity Test`, `AD Configuration Test` (sprawdza punkt połączenia usługi, czyli SCP), `DRS Discovery Test`, `DRS Connectivity Test` i `Token Acquisition Test`. Pierwszy test z wynikiem `FAIL` wskazuje, gdzie szukać przyczyny. Wiersze `Error Phase`,

`Client ErrorCode` i `Server ErrorCode` podają fazę i kod błędu.

Przykład fragmentu wyniku, gdy brakuje SCP:

```
        AD Configuration Test : FAIL
                  Error Phase : pre-check
              Client ErrorCode : 0x801c001d
```

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **SCP** = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **DRS** = Device Registration Service: usługa Entra ID, z którą komputer rejestruje się przy dołączaniu, jej testy pokazuje dsregcmd /status · **dsregcmd** = Device Registration Command: pokaż, czy komputer jest dołączony do Entra ID, domeny albo zarejestrowany, i zdiagnozuj rejestrację

TYLKO ODCZYT

Wymuszenie dołączenia do Entra ID: dsregcmd /join

```
dsregcmd /join
```

Ręcznie uruchamia to, co normalnie robi zadanie Automatic-Device-Join. Używamy po poprawieniu SCP albo dostępu do adresów Microsoftu, żeby nie czekać na następne uruchomienie zadania. Zadanie widać w Harmonogramie zadań: Task Scheduler Library, Microsoft, Windows, Workplace Join.

SCP = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **dsregcmd** = Device Registration Command: pokaż, czy komputer jest dołączony do Entra ID, domeny albo zarejestrowany, i zdiagnozuj rejestrację

TYLKO ODCZYT

Włączenie automatycznej rejestracji MDM w GPO: Group Policy Management Editor

```
Group Policy Management Editor
→ Computer Configuration → Administrative Templates → Windows Components → MDM
→ Enable automatic MDM enrollment using default Microsoft Entra credentials → Enabled
→ Credential Type: User Credential
→ powiązanie GPO z jednostką organizacyjną z komputerami pilotażu
```

Dla komputerów hybrid joined to jest sposób, w jaki istniejąca flota rejestruje się w Intune bez dotykania komputerów. Opcja Credential Type ma wartości User Credential (domyślna dla Windows 10 w wersji 1903 i nowszych) i Device Credential, ta druga obsługiwana tylko w wąskich scenariuszach (współzarządzanie z Configuration Managerem, wieloosobowe hosty Azure Virtual Desktop). Dla zwykłych stacji zostajemy przy poświadczeniach użytkownika.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: edytor GPO na `dc01`, ścieżka Computer Configuration → Administrative Templates → Windows Components → MDM, okno ustawienia „Enable automatic MDM enrollment using default Microsoft Entra credentials" ze stanem Enabled i Credential Type: User Credential.

MDM = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi · **GPO** = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

TYLKO ODCZYT

Odświeżenie polityk komputera po zmianie GPO: gpupdate /force

```
gpupdate /force
```

Po odświeżeniu polityk system tworzy zadanie rejestracji, które w Harmonogramie zadań leży w Task Scheduler Library, Microsoft, Windows, EnterpriseMgmt. Działa co 5 minut przez jeden dzień. Potem sprawdzamy w Ustawieniach: Konta, Uzyskaj dostęp do pracy lub szkoły, nasze konto, przycisk Info (Settings, Accounts, Access work or school).

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **gpupdate** = group policy update: wymuś odświeżenie GPO

KLIKAMY W INTERFEJSIE

Sprawdzenie wyniku rejestracji MDM w dzienniku zdarzeń: Event Viewer

```
Event Viewer → Applications and Services Logs → Microsoft → Windows
→ DeviceManagement-Enterprise-Diagnostics-Provider → Admin
→ zdarzenie 75: rejestracja udana
→ zdarzenie 76: rejestracja nieudana, kod błędu w treści zdarzenia
```

Dziennik dołączenia do Entra ID leży obok, w gałęzi User Device Registration. Przy błędach dołączenia szukamy w nim zdarzeń 304, 305 i 307.

MDM = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi

TYLKO ODCZYT

Zebranie logów MDM do analizy: mdmdiagnosticstool.exe

```
mdmdiagnosticstool.exe -area "DeviceEnrollment;DeviceProvisioning;Autopilot" -zip
"C:\Users\Public\Documents\MDMDiagReport.zip"
```

W archiwum jest podsumowanie ustawień w HTML (`MDMDiagHtmlReport.html`), zrzut rejestru i dzienniki zdarzeń. To samo da się zrobić z Ustawień: Konta, Uzyskaj dostęp do pracy lub szkoły, Info, Create report.

MDM = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi · **HTML** = HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce

ZMIENIA SYSTEM

Zebranie hasha sprzętu do pliku CSV: Get-WindowsAutopilotInfo

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
New-Item -Type Directory -Path "C:\HWID"
Set-Location -Path "C:\HWID"
$env:Path += ";C:\Program Files\WindowsPowerShell\Scripts"
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Install-Script -Name Get-WindowsAutopilotInfo
Get-WindowsAutopilotInfo -OutputFile AutopilotHWID.csv
```

> (gdzie `C:\HWID` to dowolny katalog roboczy, a `AutopilotHWID.csv` to plik, który potem zaimportujemy w Intune)

Komendy można wykonywać całościowo jako blok tekstu, w podniesionym PowerShellu. Przy zmianie polityki wykonywania obowiązuje ona tylko w bieżącym oknie (`-Scope Process`).

CSV = w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami

□□ ZMIENIA SYSTEM

Wysłanie hasha prosto do Intune: Get-WindowsAutopilotInfo -Online

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Install-Script -Name Get-WindowsAutopilotInfo -Force
Get-WindowsAutopilotInfo -Online
```

Skrypt loguje się kontem z rolą Intune Administrator i sam wysyła hash. Na świeżo zainstalowanym komputerze, jeszcze przed logowaniem, otwieramy wiersz poleceń skrótem Shift+F10 w ekranie logowania OOBE i wpisujemy `powershell.exe`.

□□ **OOBE** = Out-of-Box Experience: ekrany pierwszego uruchomienia Windows, na których komputer dołącza się do Entra ID i dostaje konfigurację z Autopilot

□□ KLIKAMY W INTERFEJSIE

Import pliku CSV z hashami do Intune: Windows Autopilot, Devices

```
Microsoft Intune admin center → Devices → Windows → Enrollment → Windows Autopilot →
Devices
→ Import → wskazujemy plik AutopilotHWID.csv → Import
→ po zakończeniu: Sync, potem Refresh, aż urządzenia pojawią się na liście
```

W nowszych opisach ta sama ścieżka zaczyna się od Devices → Device onboarding → Enrollment → zakładka Windows. W jednym pliku może być najwyżej 500 wierszy, a plik musi być w kodowaniu ANSI, bez cudzysłowów i dodatkowych kolumn, edytowany w Notatniku, nie w Excelu.

□□ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: lista Windows Autopilot devices w Intune admin center po imporcie, widoczny numer seryjny nowego laptopa pana Zbigniewa, kolumna Group tag z wartością `Zarzad` i Profile status Assigned.

□□ **CSV** = w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami ·**ANSI** = American National Standards Institute: tu chodzi o kody sterujące kolorem i pozycją kursora w terminalu

◫◫ ZMIENIA SYSTEM

Utworzenie profilu wdrażania Autopilot: Deployment Profiles

```
Microsoft Intune admin center → Devices → Windows → Enrollment → Windows Autopilot →
Deployment Profiles
→ Create profile → Windows PC
→ Out-of-box experience (OOBE): Deployment mode: User-driven
→ Join to Microsoft Entra ID as: Microsoft Entra joined
→ User account type: Standard
→ Apply device name template: Yes (szablon z prefiksem firmowym)
→ Assignments: Selected groups
```

Ustawienie Convert all targeted devices to Autopilot na zakładce Basics ustawiamy na Yes tylko świadomie: rejestruje w usłudze Autopilot wszystkie firmowe urządzenia w przypisanej grupie. Stan profilu na liście urządzeń przechodzi z Unassigned przez Assigning do Assigned.

◫◫ ZMIENIA SYSTEM

Ustawienie strony postępu rejestracji: Enrollment Status Page

```
Microsoft Intune admin center → Devices → Device onboarding → Enrollment → Windows
→ Windows Autopilot → Enrollment Status Page → Create
→ Show app and profile configuration progress: Yes
→ Show an error when installation takes longer than specified number of minutes: 60
→ Turn on log collection and diagnostics page for end users: Yes
→ Block device use until all apps and profiles are installed: Yes
→ Allow users to reset device if installation error occurs: Yes
```

Wartości to nasza propozycja startowa. Stronę postępu pokazuje się przy pierwszym logowaniu i pilnuje, żeby użytkownik dostał pulpit dopiero wtedy, gdy wymagane profile i aplikacje już są na komputerze.

Z życia wzięte

◫◫ Z ŻYCIA WZIĘTE

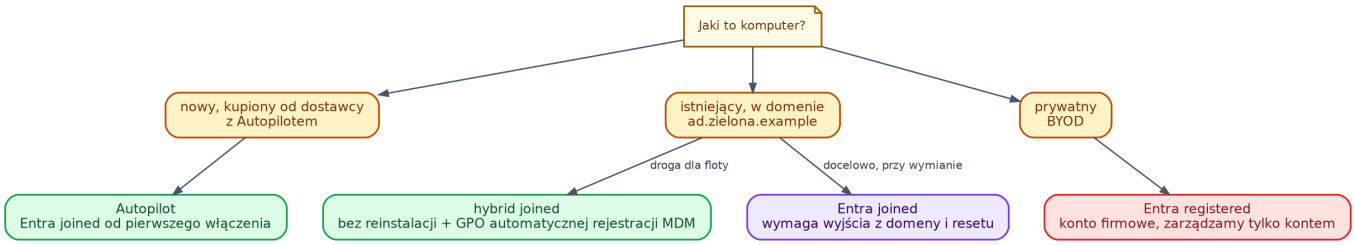
> Środa, 9:40. Pan Zbigniew wraca z urlopu z nowym laptopem kupionym w sklepie, którego nikt z dostawcą Autopilota nie zgłosił, więc jego numeru seryjnego nie ma w Intune. Tomek nie wysyła go do serwerowni: przy pierwszym ekranie konfiguracji wciska Shift+F10, wpisuje `powershell.exe` i `Get-WindowsAutopilotInfo -Online`, loguje się kontem administratora Intune i po pięciu minutach, po Sync, laptop pana Zbigniewa jest na liście. Prezes loguje się własnym kontem, patrzy na Enrollment Status Page i po kwadransie ma pulpit z Defenderem, Wi-Fi i programem do faktur.

Jak to działa

Rozwiń: jak to działa pod spodem

> **Pojęcie: dołączenie do Entra ID.** Komputer dostaje w chmurze własny obiekt, czyli tożsamość urządzenia. Dopiero z tą tożsamością Intune wie, że komputer istnieje, i może go dodać do grupy, przypisać mu profile i ocenić jego zgodność. Są trzy sposoby uzyskania tożsamości, a różnią się tym, kto jest właścicielem komputera i skąd pochodzą jego logowania.

Tryb	Dla jakiego komputera	Konto użytkownika	Zależność od domeny	Zarządzanie przez Intune
Entra joined	firmowy, Windows 10 i 11	konto firmowe z Entra ID	brak, komputer nie jest w domenie	pełne, niezależnie od tego, kto się loguje
Entra hybrid joined	firmowy, już w domenie	konto domenowe	tak, wymaga okresowej łączności z kontrolerem domeny	pełne, po automatycznej rejestracji MDM
Entra registered	prywatny (BYOD) albo mobilny	lokalne konto użytkownika, firmowe konto dodane obok	brak	ograniczone, patrz niżej



Drzewo decyzji: nowy komputer przez Autopilot jako Entra joined, istniejący domenowy jako hybrid joined albo po resecie Entra joined, prywatny jako Entra registered (kliknięcie otwiera pełny rozmiar)

Co jest realnie możliwe dla istniejących komputerów domenowych

Dla komputera, który już jest w domenie `ad.zielona.example`, mamy trzy drogi i tylko jedna z nich nie wymaga reinstalacji ani rezygnacji z domeny.

1. Hybrid join z automatyczną rejestracją MDM przez GPO. Komputer zostaje w domenie, Entra Connect Sync przenosi jego obiekt do chmury, komputer sam dołącza do Entra ID, a GPO z fiszki wyżej rejestruje go w Intune. To jest ścieżka dla naszej floty. Dokumentacja Microsoftu wprost zaleca ją dla komputerów dołączonych do lokalnego Active Directory, a hybrid join nazywa krokiem przejściowym ku Entra join.
2. Czysty Entra join po wyjściu z domeny. Taki komputer należy tylko do Entra ID, więc dla istniejącej stacji oznacza to wyjście z domeny i ponowną konfigurację (zwykle reset Windowsa, z utratą lokalnego profilu, tak jak opisuje strona o audycie GPO). Robimy to przy wymianie komputera, nie masowo.
3. Entra registered, czyli dodanie konta firmowego w Ustawieniach (Konta, Uzyskaj dostęp do pracy lub szkoły, Połącz). Ta droga jest przeznaczona dla urządzeń prywatnych. Gdy dodajemy konto firmowe do komputera domenowego, powstaje stan podwójny: komputer jest jednocześnie hybrid joined i registered. Dokumentacja podaje, że od Windows 10 1803 stan registered znika sam po hybrid join i kolejnym logowaniu tego samego użytkownika.

Wniosek dla Zielonej: dla istniejących stacji w domenie planujemy hybrid join. Rejestracja kontem firmowym („Połącz” w ustawieniach konta) nie daje pełnego zarządzania komputerem, a pełne zarządzanie bez reinstalacji daje hybrid join. Tak samo opisuje to strona Intune obok domeny: audyt GPO i plan migracji.

Ograniczenia Entra registered i BYOD

Dokumentacja Microsoftu opisuje dwie drogi dla urządzenia prywatnego. Przy wyborze opcji Email address urządzenie rejestruje się w Entra ID jako osobiste, a dokumentacja ujmuje to tak: zarządzany jest użytkownik organizacji, urządzenie nie jest zarządzane przez Intune. Przy wyborze Join this device to Azure Active Directory urządzenie dołącza do Entra ID jako firmowe i jest zarządzane niezależnie od tego, kto się loguje. Jeżeli w tenancie włączono automatyczną rejestrację MDM, dodanie konta służbowego może też zapisać komputer w MDM, ale nadal jako urządzenie osobiste, z ograniczeniami z tabeli.

Funkcja	Entra registered	Źródło ograniczenia
Windows LAPS z hasłem w Entra ID	nie działa	urządzenia registered nie są obsługiwane
Ciche szyfrowanie BitLocker przez Intune	nie	wymaga Entra joined albo hybrid joined
Polityki aktualizacji oparte na Autopatch	nie	niewspierane dla urządzeń registered
Autopilot	nie	tylko dla urządzeń firmowych
Aplikacje Win32 i ze sklepu	tak, z kontekstem System	typ instalacji User kończy się błędem Requirements not met
Dostęp warunkowy	tak, gdy urządzenie zapisano w Intune	dokumentacja Entra
Remediations	nie	wymagane Entra joined albo hybrid joined

Intune rozpoznaje urządzenia firmowe po identyfikatorach firmowych, po Autopilocie albo po rejestracji menedżera rejestracji urządzeń. Resztę uznaje za osobiste, a w ustawieniach rejestracji (Devices, Device onboarding, Enrollment, Device platform restrictions) można zablokować rejestrację urządzeń osobistych. Jeśli to zrobimy, a komputer nie jest rozpoznany jako firmowy, rejestracja kończy się błędem 80180014.

Hybrid join: czego wymaga

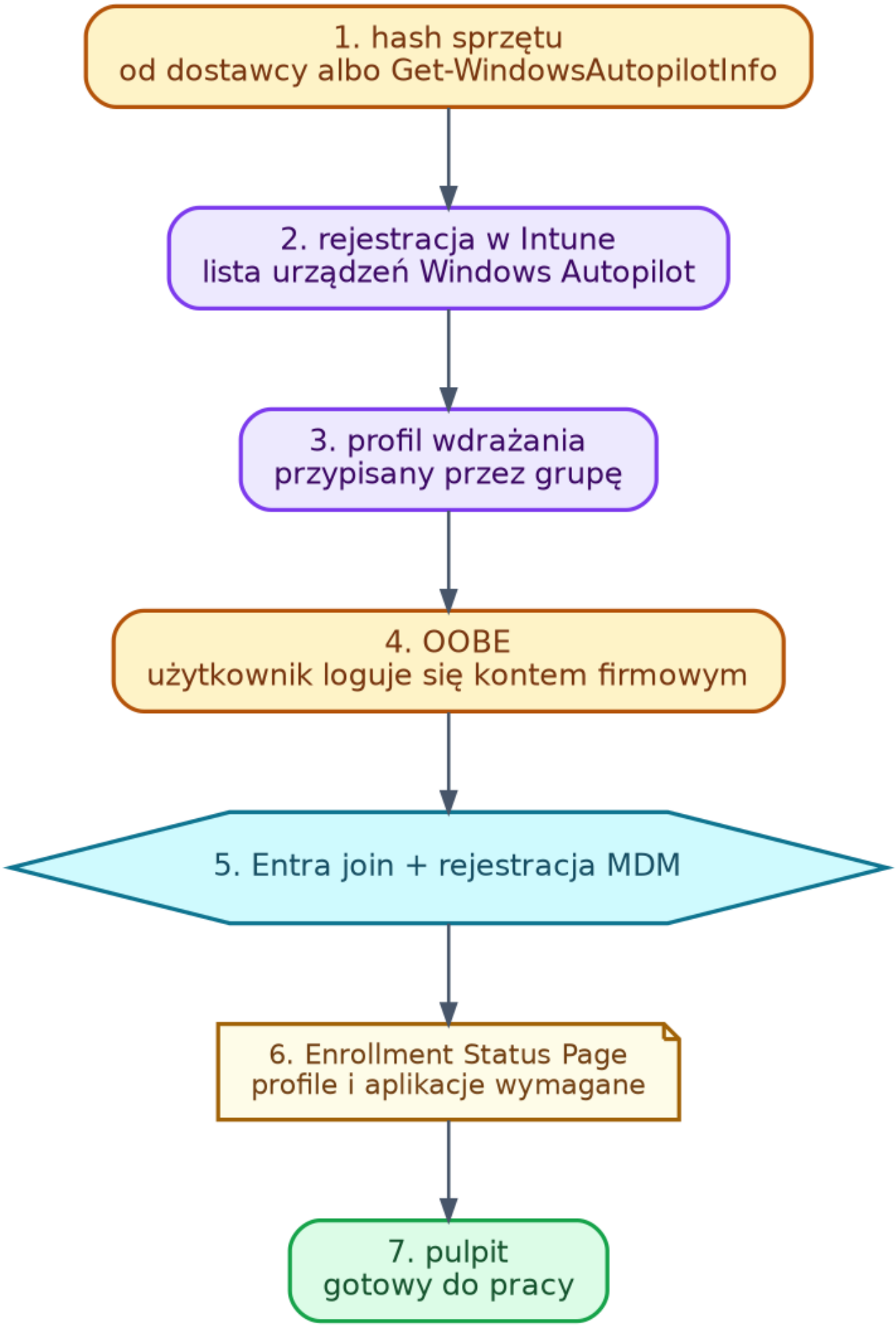
Warunki wstępne dla hybrid join na komputerach Windows 11:

- Entra Connect Sync w wersji z kreatorem opcji urządzeń (1.1.819.0 lub nowszej), z włączonym Configure Microsoft Entra hybrid join i SCP dla każdego lasu.
- Obiekty komputerów w zakresie synchronizacji (jednostki organizacyjne w filtrze).
- Dostęp komputera do `enterpriseregistration.windows.net`, `login.microsoftonline.com` i `device.login.microsoftonline.com`. Ruch do `device.login.microsoftonline.com` i `enterpriseregistration.windows.net` wyłączamy z inspekcji TLS na zaporze, bo inspekcja psuje uwierzytelnianie certyfikatem urządzenia. Na `fw01` ustawiamy wyjątek

dla tych adresów.
- Okresowa łączność z kontrolerami domeny. Według dokumentacji bez niej urządzenie staje się bezużyteczne przy zmianie hasła urządzenia, zmianie hasła użytkownika (poświadczenia w pamięci podręcznej) i resecie modułu TPM. To jest powód, dla którego przy zawodnym VPN nowe komputery kupujemy już jako Entra joined.

Autopilot

> **Pojęcie: Autopilot.** Usługa Microsoftu, która zamienia fabrycznie nowy komputer w gotowy do pracy, bez własnego obrazu systemu: komputer znamy po hashu sprzętu, usługa wie, jaki profil mu przypisaliśmy, a użytkownik tylko się loguje.


1. hash sprzętu
od dostawcy albo Get-WindowsAutopilotInfo
2. rejestracja w Intune
lista urządzeń Windows Autopilot
3. profil wdrażania
przypisany przez grupę
4. OOBE
użytkownik loguje się kontem firmowym
5. Entra join + rejestracja MDM
6. Enrollment Status Page
profile i aplikacje wymagane
7. pulpit
gotowy do pracy

Przepływ Autopilot: hash sprzętu, rejestracja w Intune, profil przypisany grupą, OOBE, Entra join i MDM, strona postępu, pulpit (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: hash sprzętu.** Długi ciąg znaków, który jednoznacznie opisuje konkretny komputer. Dostawca sprzętu może zgłosić hashe zamówionych komputerów do Intune, a komputer kupiony gdzie indziej rejestrujemy sami z komendy `Get-WindowsAutopilotInfo`. Do rejestracji ręcznej wymagane są: włączona automatyczna rejestracja Windows w Intune, licencja Microsoft Entra ID P1 lub P2 i rola Intune Administrator albo Policy and Profile Manager. W pliku CSV opcjonalna kolumna Group Tag pozwala później zbudować dynamiczną grupę, np. `device.devicePhysicalIds -any _ -eq "[OrderID]:Zarzad"` dla znacznika `Zarzad`, zamiast ręcznego dodawania.

> **Pojęcie: Enrollment Status Page (ESP).** Ekran postępu przy pierwszym logowaniu. Śledzi trzy fazy: przygotowanie urządzenia, konfigurację urządzenia (profile, certyfikaty SCEP, profile VPN i Wi-Fi, aplikacje Win32 i winget przypisane urządzeniu) oraz konfigurację konta użytkownika. Nie mieszamy w niej aplikacji LOB (MSI) z Win32, bo obie używają tego samego instalatora systemowego i nie mogą działać jednocześnie.

Dla nowych komputerów Zielonej wybieramy profil user-driven z dołączeniem Microsoft Entra joined. Hybrid joined przez Autopilot Microsoft odradza dla nowych komputerów, wymaga Intune Connector for Active Directory, widoczności kontrolera domeny i tworzy z założenia zdublowane obiekty urządzeń. Istnieje też nowsza odmiana, Autopilot device preparation, wymagająca Windows 11 w nowszej wersji (22H2 i 23H2 z aktualizacją KB5035942, 24H2 i nowszy), obsługująca tylko Entra join. Dla Zielonej opisujemy na tej stronie klasyczny Autopilot z hashem i profilem wdrażania, a przejście na nowszą odmianę oceniamy po pilotażu, czytając aktualną dokumentację.

Częste błędy

Objaw	Przyczyna	Co robimy
`dsregcmd /status` pokazuje `AzureAdJoined : NO`, `DomainJoined : YES`	komputer nie dołączył do Entra ID	uruchamiamy `dsregcmd /status` jako administrator, patrzymy na Diagnostic Data i pierwszy test z wynikiem FAIL
`AD Configuration Test: FAIL`, kod `0x801c001d`	brak punktu połączenia usługi (SCP)	w Entra Connect konfigurujemy opcje urządzeń, w razie potrzeby tworzymy SCP, potem `dsregcmd /join`

Objaw	Przyczyna	Co robimy
Kody `0x801c0021` albo `0x801c001f`	brak dostępu do adresów rejestracji urządzeń	sprawdzamy `enterpriseregistration.windows.net` na `fw01` i wyłączamy ten ruch z inspekcji TLS
Zdarzenie 76, kod `0x80180026`	włączona polityka blokująca rejestrację MDM (`Disable MDM Enrollment`)	wyłączamy politykę blokującą w GPO i odświeżamy `gpupdate /force`
Zdarzenie 76, kod `0x8018000A`	urządzenie jest już zarejestrowane, w rejestrze zostały stare wpisy	usuwamy stare wpisy w `HKLM\Software\Microsoft\Enrollments`, po zrobieniu kopii
Zdarzenie 76, kod `0x80180018`	użytkownik bez licencji Intune	przypisujemy licencję, patrz strona z planem wdrożenia
Błąd `80180014` w Ustawieniach lub OOBE	urządzenie uznane za osobiste, a rejestracja osobistych jest zablokowana	dodajemy urządzenie do identyfikatorów firmowych albo rejestrujemy je w Autopilocie
Po imporcie CSV nie widać urządzeń	brak odświeżenia albo błędny plik (Excel, cudzysłowy, dodatkowe kolumny)	Sync, Refresh, ponownie plik zapisany w Notatniku
W Entra ID są dwa obiekty tego samego komputera	hybrid joined przez Autopilot tworzy drugi obiekt z założenia	czyścimy nieaktualny obiekt po zakończeniu wdrożenia
Enrollment Status Page kończy się błędem po 60 minutach	aplikacja nie zainstalowała się w limicie czasu	patrzymy w logi IME (strona o aplikacjach), zwiększamy limit albo zdejmujemy aplikację z wymaganych w ESP

□□ Ćwiczenia

1. W `dsregcmd /status` widzimy `AzureAdJoined : YES` i `DomainJoined : YES`. Jaki to tryb i co dalej, żeby komputer pojawił się w Intune?

Odpowiedź

To komputer hybrid joined. Żeby pojawił się w Intune, użytkownik musi być w zakresie MDM, mieć licencję, a komputer musi dostać GPO „Enable automatic MDM enrollment using default Microsoft Entra credentials". Rejestrację potwierdzamy zdarzeniem 75 w dzienniku DeviceManagement-Enterprise-Diagnostics-Provider.

1. Pani Halina zapytała, czy może dodać konto firmowe na swoim prywatnym laptopie i dostać tam te same zasady co na służbowym. Co odpowiadamy?

Odpowiedź

Prywatny laptop trafi do trybu Entra registered. Zarządzamy wtedy kontem, nie całym urządzeniem: nie zadziała LAPS, ciche szyfrowanie BitLocker, polityki aktualizacji oparte na Autopatch i Autopilot, a aplikacje muszą być instalowane w kontekście System. Pełnych zasad ze służbowego komputera na prywatnym nie dostaje się z założenia.

1. Marek kupił w sklepie 10 skanerów z Windowsem i chce je podpiąć do Intune. Od czego zaczynamy?

Odpowiedź

Od zebrania hashów sprzętu (`Get-WindowsAutopilotInfo -OutputFile`) albo zgłoszenia ich do Autopilota przez dostawcę, importu pliku CSV w Intune (do 500 wierszy na plik), przypisania profilu wdrażania grupą i dopiero potem pierwszego włączenia urządzeń. Przy kilkudziesięciu urządzeniach wartościowy jest też Group Tag, żeby dynamiczna grupa sama je łapała.

Powiązane: Intune obok domeny: audyt GPO i plan migracji · Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy · Windows LAPS: hasło lokalnego administratora w Active Directory · BitLocker z kluczem odzyskiwania w Active Directory · Aplikacje w Intune: Win32, Store, winget i zależności

Źródła: Microsoft Learn, „Windows enrollment method decision guide" (learn.microsoft.com/intune/device-enrollment/windows/guide) · „MDM enrollment of Windows devices" (learn.microsoft.com/windows/client-management/mdm-enrollment-of-windows-devices) · „Enroll a Windows 10 device automatically using Group Policy" (learn.microsoft.com/windows/client-management/enroll-a-windows-10-device-automatically-using-group-policy) · „Plan your Microsoft Entra hybrid join deployment" (learn.microsoft.com/entra/identity/devices/hybrid-join-plan) · „How to configure Microsoft Entra hybrid join" (learn.microsoft.com/entra/identity/devices/how-to-hybrid-join) · „Troubleshoot devices using the dsregcmd command" (learn.microsoft.com/entra/identity/devices/troubleshoot-device-dsregcmd) · „Troubleshoot Microsoft Entra hybrid join for current Windows devices" (learn.microsoft.com/entra/identity/devices/troubleshoot-hybrid-join-windows-current) · „Diagnose MDM failures" (learn.microsoft.com/windows/client-management/mdm-diagnose-enrollment) · „Collect MDM logs" (learn.microsoft.com/windows/client-management/mdm-collect-logs) · „Manually register devices with Windows Autopilot" (learn.microsoft.com/autopilot/add-devices) · „Windows Autopilot deployment profiles" (learn.microsoft.com/autopilot/profiles) · „Enrollment Status Page" (learn.microsoft.com/intune/intune-service/enrollment/windows-enrollment-status) · „Windows Autopilot device preparation overview" (learn.microsoft.com/autopilot/device-preparation/overview) · „Windows Autopilot for Microsoft Entra hybrid join" (learn.microsoft.com/autopilot/windows-autopilot-hybrid) · „Create device platform restrictions" (learn.microsoft.com/intune/device-enrollment/create-platform-restrictions) · „Troubleshoot Set up

for work or school enrollment" (learn.microsoft.com/troubleshoot/mem/intune/device-enrollment/troubleshoot-windows-work-school) · „Microsoft Entra registered devices" (learn.microsoft.com/entra/identity/devices/concept-device-registration)

Zasady zgodności i dostęp warunkowy

Poziom: średniozaawansowany **Dotyczy: Intune, Microsoft Entra ID P1, Windows 11**

Czas: ~45 min

Zasada zgodności sprawdza, czy komputer spełnia nasze minimum: szyfrowanie, ochronę przed złośliwym oprogramowaniem, aktualny system. Dostęp warunkowy sprawia, że poczta i SharePoint wpuszczają tylko takie komputery. Strona pokazuje obie rzeczy oraz sposób włączenia ich tak, żeby nie zablokować całej firmy.

ZAŁOŻENIA SCENARIUSZA

dostęp warunkowy do poczty, opisany na tej stronie, dotyczy podejścia z pocztą w Exchange Online. Zielona ma w przykładach serii trzy równorzędne podejścia do poczty i pakietu biurowego: MailCow na `docker01`, Microsoft 365 i Google Workspace. W podejściu z MailCow poczta sprawdza hasło w Active Directory przez LDAP, z pominięciem Entra ID (MailCow: konta z Active Directory), więc dostęp warunkowy obejmuje Teams, SharePoint i OneDrive, a nie pocztę. W podejściu z Google Workspace odpowiednikiem dostępu warunkowego jest dostęp kontekstowy w konsoli administracyjnej Google; wymagane wersje licencji sprawdzamy w dokumentacji Google.

Skróty użyte na tej stronie (3)

Skrót	Co znaczy
FIDO2	standard kluczy sprzętowych do logowania odpornego na wyłudzenie, używany w Entra ID jako metoda uwierzytelniania
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
TPM	Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów

Fiszka

Ścieżki w centrach administracyjnych podajemy po angielsku, tak jak w dokumentacji. Microsoft przenosi pozycje menu, więc w razie rozbieżności szukamy po nazwie ustawienia. Komendy sprawdzające wykonujemy na komputerze w PowerShellu z uprawnieniami administratora.

ZMIENIA SYSTEM

Utworzenie zasady zgodności dla Windows: Compliance, Create policy

```
Microsoft Intune admin center → Devices → Manage devices → Compliance → Create policy
→ Platform: Windows 10 and later
→ Basics: nazwa Zgodnosc-Windows-Zielona
→ Compliance settings (zakładki poniżej)
→ Actions for noncompliance
→ Assignments: grupa pilotażowa
```

Zasada obejmuje wszystkie Windows 10 i 11. Dalej ustawiamy poszczególne grupy opcji.

KLIKAMY W INTERFEJSIE

Ustawienie zdrowia urządzenia: BitLocker, Secure Boot, integralność kodu

```
Compliance settings → Device Health
→ Require BitLocker: Require
→ Require Secure Boot to be enabled on the device: Require
→ Require code integrity: Require
```

Wszystkie trzy ustawienia korzystają z usługi atestacji zdrowia urządzenia, więc stan jest mierzony przy uruchomieniu komputera. Po zaszyfrowaniu dysku komputer musi być jeszcze raz uruchomiony, żeby został uznany za zgodny.

KLIKAMY W INTERFEJSIE

Ustawienie wersji systemu: Device Properties

```
Compliance settings → Device Properties
→ Minimum OS version: 10.0.NumerBudowy.NumerRewizji
```

> (gdzie `10.0.NumerBudowy.NumerRewizji` to najstarsza wersja systemu, którą jeszcze akceptujemy; wersję komputera odczytujemy w wierszu poleceń komendą `ver`)

Format to `major.minor.build.revision`, a dla Windows 11 24H2 budowa zaczyna się od `10.0.26100`. Gdy chcemy dopuścić kilka linii wydań naraz, używamy ustawienia Valid operating system builds, w którym każdy wiersz ma swoją wersję minimalną i maksymalną.

□□ TYLKO ODCZYT

Ustawienie zabezpieczeń systemu: szyfrowanie, zapora, TPM, Defender

```
Compliance settings → System Security
→ Encryption of data storage on a device: Require
→ Firewall: Require
→ Trusted Platform Module (TPM): Require
→ Antivirus: Require
→ Antispyware: Require

Compliance settings → Microsoft Defender Antimalware
→ Microsoft Defender Antimalware: Require
→ Microsoft Defender Antimalware minimum version: wersja, którą widzimy na pilotażu
→ Microsoft Defender Antimalware security intelligence up-to-date: Require
→ Real-time protection: Require
```

Ustawienie Encryption of data storage on a device sprawdza obecność szyfrowania na dysku systemowym, a Intune obsługuje tu tylko BitLockera. Ustawienie Require BitLocker z poprzedniej fiszki jest dokładniejsze, bo korzysta z atestacji na poziomie TPM. W obu przypadkach komputer musi pasować do zasady także po restarcie.

□□ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran tworzenia zasady zgodności w Intune admin center, zakładka Compliance settings z rozwiniętą grupą Device Health, widoczne trzy ustawienia ustawione na Require.

□□ **TPM** = Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów

🖱️ KLIKAMY W INTERFEJSIE

Ustawienie działań przy niezgodności: Actions for noncompliance

```
Actions for noncompliance
→ Mark device noncompliant: po 3 dniach (Schedule)
→ Send email to end user: natychmiast
```

Domyślnie komputer zostaje uznany za niezgodny od razu. Wydłużamy ten okres do kilku dni, a przed tym dokładamy wiadomość do użytkownika, żeby miał czas naprawić komputer, zanim straci dostęp.

👁️ TYLKO ODCZYT

Odczyt wersji systemu i stanu szyfrowania na komputerze: cmd /c ver

```
cmd /c ver
manage-bde -status C:
Confirm-SecureBootUEFI
```

Pierwsza komenda podaje wersję Windows, druga stan BitLockera na dysku `C:`, a trzecia zwraca `True`, gdy Secure Boot jest włączony. Jeżeli `Confirm-SecureBootUEFI` pokazuje błąd, komputer pracuje w trybie starego BIOS-u i zgodność w Intune z Secure Boot nie przejdzie.

Przykład:

```
Microsoft Windows [Version 10.0.26100.4000]
```

👁️ **manage-bde** = BitLocker Drive Encryption: zarządzanie szyfrowaniem dysków

👁️ TYLKO ODCZYT

Sprawdzenie ochrony przed złośliwym oprogramowaniem: Get-MpComputerStatus

```
Get-MpComputerStatus | Select-Object AMRunningMode, RealTimeProtectionEnabled,
AntivirusSignatureLastUpdated
```

Trzy pola odpowiadają ustawieniom zgodności dla Defendera: tryb pracy silnika, ochrona w czasie rzeczywistym i data ostatniej aktualizacji sygnatur.

Przykład:

```
AMRunningMode RealTimeProtectionEnabled AntivirusSignatureLastUpdated
------------ ------------------------ ----------------------------
Normal                                True 02.10.2026 07:42:11
```

◫◫ KLIKAMY W INTERFEJSIE

Zmiana traktowania urządzeń bez zasady zgodności: Compliance policy settings

```
Microsoft Intune admin center → Endpoint security → Device compliance → Compliance
policy settings
→ Mark devices with no compliance policy assigned as: Not compliant
→ Compliance status validity period (days): 30
```

Domyślnie komputer bez przypisanej zasady jest uznawany za zgodny. Dokumentacja zaleca przy korzystaniu z dostępu warunkowego przestawić to na Not compliant, bo inaczej komputer, o którym Intune nic nie wie, dostaje dostęp. Okres ważności statusu (domyślnie 30 dni, zakres od 1 do 120) mówi, jak długo komputer może milczeć, zanim zostanie uznany za niezgodny.

◫◫ ZMIENIA SYSTEM

Utworzenie konta awaryjnego: Entra ID, Users

```
Microsoft Entra admin center → Entra ID → Users → New user → Create new user
→ User principal name: awaria1@ domena początkowa .onmicrosoft.com
→ Assigned roles: Global Administrator (aktywna na stałe, nie kwalifikowana)
→ metoda logowania: klucz FIDO2 (passkey)
→ dodanie do grupy zabezpieczeń EmergencyAccess
```

Zakładamy dwa konta (`awaria1` i `awaria2`), tylko w chmurze, w domenie początkowej `.onmicrosoft.com`, niezwiązane z żadną osobą i niesynchronizowane z Active Directory. Hasła i klucze trzymamy w osobnych, zamkniętych sejfach.

◻◻ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: lista Users w Microsoft Entra admin center z dwoma kontami awaryjnymi, widoczny typ konta (cloud only) i grupa `EmergencyAccess` z ich członkostwem. Bez haseł i kluczy.

◻◻ ZMIENIA SYSTEM

Utworzenie polityki dostępu warunkowego: wymaganie zgodnego urządzenia

```
Microsoft Entra admin center → Entra ID → Conditional Access → Policies → New policy
→ Name: CA-Zgodne-Urzadzenie-Poczta-SharePoint
→ Users: Include → Select users and groups → GG_Intune_Pilot
→ Users: Exclude → grupa EmergencyAccess i konta synchronizacji katalogu (Directory Synchronization Accounts)
→ Target resources: Resources → Select resources → Office 365
→ Conditions → Device platforms → Windows
→ Grant → Grant access → Require device to be marked as compliant
→ Enable policy: Report-only
```

Dokumentacja zaleca wskazywać grupę Office 365 jako całość (zawiera Exchange Online, SharePoint Online, Teams i pokrewne usługi), zamiast wybierać usługi pojedynczo, żeby uniknąć problemów z zależnościami między nimi. Warunek Device platforms ograniczony do Windows chroni telefony: bez niego polityka objęłaby także iOS i Androida, na których nie wdrożyliśmy jeszcze zarządzania.

◻◻ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran New policy w Conditional Access z wypełnionymi sekcjami Users (Include grupa pilotażowa, Exclude `EmergencyAccess`), Target resources (Office 365), Conditions (Windows) i Grant (Require device to be marked as compliant), przełącznik Enable policy ustawiony na Report-only.

◻◻ TYLKO ODCZYT

Podgląd wyników w trybie tylko raportowania: Sign-in logs

```
Microsoft Entra admin center → Entra ID → Monitoring & health → Sign-in logs
→ wybieramy logowanie → zakładka Report-only
→ wyniki: Report-only: Success, Failure, User action required, Not applied
```

Polityka w trybie tylko raportowania jest oceniana przy każdym logowaniu, ale niczego nie blokuje. Wynik Failure oznacza, że użytkownik zostałby zablokowany po włączeniu polityki. Podsumowanie wpływu polityki z ostatnich 24 godzin, 7 dni albo miesiąca pokazuje widok Policy Impact i skoroszyt Conditional Access Insights and Reporting.

ZMIENIA SYSTEM

Utworzenie polityki wymagającej uwierzytelniania wieloskładnikowego: Conditional Access

```
Microsoft Entra admin center → Entra ID → Conditional Access → Policies → New policy
→ Name: CA-MFA-Wszyscy
→ Users: Include → All users, Exclude → EmergencyAccess
→ Target resources: All resources
→ Grant → Grant access → Require multifactor authentication
→ Enable policy: Report-only
```

Przed przełączeniem na On wszyscy muszą mieć zarejestrowaną metodę uwierzytelniania (aplikacja Microsoft Authenticator albo klucz). Zamiast Require multifactor authentication można wybrać Require authentication strength i zażądać metody odpornej na wyłudzanie.

TYLKO ODCZYT

Monitorowanie logowań kont awaryjnych: SigninLogs

```
SigninLogs
| where UserId == "IdentyfikatorKontaAwaria1" or UserId == "IdentyfikatorKontaAwaria2"
| project TimeGenerated, UserPrincipalName, UserId, IPAddress, ResultType,
ResultDescription
```

> (gdzie `IdentyfikatorKontaAwaria1` to identyfikator obiektu konta z Entra ID; zapytanie wklejamy w Log Analytics i podpinamy do alertu w Azure Monitor)

Każde logowanie na konto awaryjne ma od razu wywołać alert, bo normalnie nikt się na nie nie loguje.

□□ KLIKAMY W INTERFEJSIE

Sprawdzenie stanu zgodności komputera w Intune: Device compliance

```
Microsoft Intune admin center → Devices → All devices → wybrany komputer → Device compliance
Microsoft Intune admin center → Reports → Device compliance → Noncompliant devices
Microsoft Intune admin center → Devices → Monitor → Setting compliance
```

Pierwsza ścieżka pokazuje zasady i ich wynik dla jednego komputera, druga zbiorczy raport niezgodnych, trzecia stan każdego ustawienia na całej flocie.

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Piątek, 16:05. Tomek, zadowolony z pilotażu, włącza politykę „wymagaj zgodnego urządzenia" od razu na wszystkich użytkowników i wszystkie usługi, bez trybu raportowania. Po dziesięciu minutach dzwoni pani Halina, że Outlook pyta o logowanie w kółko, a chwilę później Kasia, że telefon nie pobiera poczty. Tomek otwiera panel kontem awaryjnym, wykluczonym z polityki, i przełącza ją na tryb tylko raportowania. W raporcie od razu widać dwa błędy: komputery księgowości jeszcze nie były w Intune, a telefony w ogóle nie podlegały zarządzaniu.

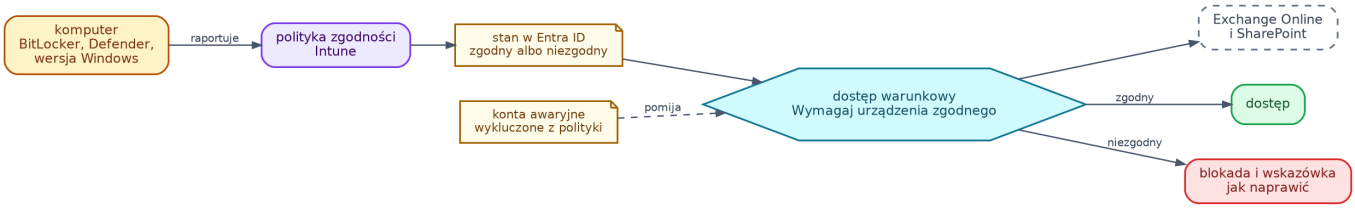
Jak to działa

□□ Rozwiń: jak to działa pod spodem

> **Pojęcie: zasada zgodności.** Lista warunków, które komputer ma spełniać. Intune porównuje z nią stan komputera i zapisuje wynik w Microsoft Entra ID: zgodny albo niezgodny.

> **Pojęcie: dostęp warunkowy.** Reguła w Microsoft Entra ID w postaci „jeśli użytkownik X próbuje wejść do usługi Y z urządzenia o cechach Z, to wymagamy W". Wymaga licencji Entra ID P1, którą mamy w pakiecie Business Premium. Warunki oparte na ryzyku logowania wymagają Entra ID P2.

Obie rzeczy są osobnymi mechanizmami. Zasada zgodności tylko oznacza komputer, a to dostęp warunkowy odmawia albo przyznaje wejście. Dlatego dostęp warunkowy bez zasady zgodności nie zadziała zgodnie z oczekiwaniami: dokumentacja ostrzega, że bez utworzonej zasady w Intune polityka dostępu warunkowego nie będzie działać tak, jak zamierzamy.



Komputer raportuje do zasady zgodności, stan trafia do Entra ID, dostęp warunkowy wpuszcza zgodne komputery do Exchange Online i SharePointa, a konta awaryjne są poza polityką (kliknięcie otwiera pełny rozmiar)

Co dokładnie sprawdzamy i gdzie są pułapki

Ustawienie	Co sprawdza	Pułapka
Require BitLocker	szyfrowanie dysku systemowego, atestacja przez TPM	stan mierzony przy starcie, po szyfrowaniu potrzebny restart
Require Secure Boot to be enabled on the device	Secure Boot włączony	wymaga TPM 2.0, UEFI i konfiguracji PCR7 w stanie Bound, inaczej Not compliant mimo włączonego Secure Boot

Ustawienie	Co sprawdza	Pułapka
Require code integrity	wykrywa niepodpisany sterownik albo zmieniony plik systemowy ładowany do jądra	jak przy pozostałych ustawieniach atestacji wynik sprawdzamy na pilotażu, zanim włączymy go całej flocie
Minimum OS version	wersja Windows	rośnie co miesiąc, dlatego ustawiamy minimum zamiast dokładnej wartości
Firewall	zapora włączona	GPO, które wyłącza zaporę albo dopuszcza cały ruch przychodzący, wygrywa z Intune i daje Not compliant
TPM	obecność modułu o wersji większej niż 0	stare komputery bez TPM nigdy nie będą zgodne
Antivirus, Antispyware, Defender	produkt zarejestrowany w Centrum zabezpieczeń Windows, aktualne sygnatury, ochrona w czasie rzeczywistym	wyłączony albo nieaktualny produkt daje Not compliant

Jak wdrażamy dostęp warunkowy bez wywrócenia firmy

1. Zasada zgodności trafia do grupy pilotażowej, bez żadnej polityki dostępu.
2. Polityka dostępu warunkowego powstaje w trybie tylko raportowania, z wykluczonym kontem awaryjnym i ograniczona do Windows.
3. Przez tydzień patrzymy w Sign-in logs, kto dostałby Failure.
4. Naprawiamy komputery z Failure albo rozszerzamy zasadę, a dopiero potem przełączamy politykę na On, najpierw dla grupy pilotażowej.
5. Dopiero z końcem wdrożenia przestawiamy Mark devices with no compliance policy assigned as na Not compliant.

> ⚠ Polityki w trybie tylko raportowania wymagające zgodnego urządzenia mogą na macOS, iOS i Androidzie wywołać prośbę o wybór certyfikatu urządzenia, mimo że niczego nie blokują. Dokumentacja radzi wykluczyć te platformy z takich polityk. Polityka ograniczona do Windows tego problemu nie ma. W przeglądarkach innych niż Microsoft Edge użytkownik może zobaczyć prośbę o wybór certyfikatu klienta przy pierwszym logowaniu.

Konta awaryjne

Konto awaryjne (break glass) to konto, którym wchodzimy, gdy zablokujemy sobie wszystkie zwykłe konta administratorów: błędna polityka dostępu warunkowego, awaria usługi uwierzytelniania wieloskładnikowego albo odejście ostatniego administratora. Zalecenia Microsoftu, które stosujemy:

- co najmniej dwa konta, tylko w chmurze, w domenie początkowej `.onmicrosoft.com`, niesynchronizowane i niefederowane,
- rola Global Administrator aktywna na stałe, nie kwalifikowana w Privileged Identity Management,
- logowanie metodą odporną na wyłudzanie (klucz FIDO2 jako podstawowy wybór), inną niż u zwykłych administratorów,
- wykluczenie z polityk dostępu warunkowego, które blokują albo ograniczają logowanie (polityki tylko raportujące nie wymagają wykluczenia),
- alert przy każdym logowaniu i test działania co najmniej raz na 90 dni,
- dane logowania w zamkniętych sejfach w osobnych miejscach.

Częste błędy

Objaw	Przyczyna	Co robimy
Komputer ma szyfrowanie, a Intune pokazuje Not compliant dla BitLockera	stan mierzony przy starcie, po szyfrowaniu nie było restartu	restartujemy komputer, sprawdzamy ponownie
Secure Boot włączony, a zgodność nadal Not compliant	brak TPM 2.0, stary BIOS zamiast UEFI albo PCR7 w stanie innym niż Bound	`Confirm-SecureBootUEFI`, `msinfo32` (BIOS Mode, PCR7 Configuration), `tpm.msc`, w razie potrzeby aktualizacja firmware
Firewall: Not compliant mimo profilu zapory w Intune	GPO wyłącza zaporę albo dopuszcza cały ruch przychodzący i nadpisuje Intune	poprawiamy GPO albo wyłączamy to GPO po przeniesieniu zapory do Intune
Po włączeniu polityki wszyscy dostają blokadę	polityka bez trybu raportowania, brak zasady zgodności dla grupy albo komputery jeszcze nie w Intune	tryb Report-only, zasada zgodności przypisana najpierw, konto awaryjne przełącza politykę
Telefony nie pobierają poczty	polityka obejmuje wszystkie platformy	warunek Device platforms ograniczony do Windows, zarządzanie telefonami wdrażamy osobno
Zgodny wczoraj komputer jest dziś niezgodny, bo nie zgłasza się do Intune	przekroczony okres ważności statusu zgodności (domyślnie 30 dni)	sprawdzamy, czy komputer ma łączność z Intune, wymuszamy Sync

Objaw	Przyczyna	Co robimy
Nowy komputer od razu dostaje dostęp mimo braku zasady	Mark devices with no compliance policy assigned as ma wartość Compliant	przestawiamy na Not compliant po zakończeniu wdrożenia
Konto awaryjne nie loguje się w czasie awarii	było objęte polityką blokującą albo nikt go nie testował	wykluczamy grupę `EmergencyAccess` z polityk blokujących, testujemy co 90 dni

Ćwiczenia

1. Dlaczego pierwsza polityka dostępu warunkowego powstaje w trybie tylko raportowania i dla grupy pilotażowej?

Odpowiedź

Tryb Report-only ocenia politykę przy każdym logowaniu, ale niczego nie blokuje. Wyniki w Sign-in logs pokazują, kto dostałby Failure, więc możemy naprawić komputery przed włączeniem blokady. Grupa pilotażowa dodatkowo ogranicza skutki pomyłki w samej polityce.

1. Kasia ma służbowy laptop zgodny z zasadą i prywatny telefon. Co się stanie z jej pocztą na telefonie po włączeniu polityki wymagającej zgodnego urządzenia dla wszystkich platform?

Odpowiedź

Telefon nie jest zarejestrowany w Intune i nie ma statusu zgodnego, więc dostęp do poczty zostanie zablokowany. Dlatego na początku ograniczamy politykę warunkiem Device platforms do Windows, a zarządzanie telefonami wprowadzamy w osobnym kroku.

1. Jak zabezpieczamy konta awaryjne i co z nimi robimy co 90 dni?

Odpowiedź

Zalecenia to: konto tylko w chmurze w domenie `.onmicrosoft.com` z rolą Global Administrator aktywną na stałe, logowanie metodą odporną na wyłudzanie (klucz FIDO2), wykluczenie z polityk blokujących wraz z alertem przy każdym logowaniu. Co 90 dni testujemy, czy konto potrafi się zalogować.

Powiązane: Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot · Profile konfiguracji: katalog ustawień zamiast GPO · BitLocker z kluczem odzyskiwania w Active Directory · Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM

Źródła: Microsoft Learn, „Windows compliance settings in Microsoft Intune" (learn.microsoft.com/intune/device-security/compliance/ref-windows-settings) · „Create a compliance policy in Microsoft Intune" (learn.microsoft.com/intune/device-security/compliance/create-policy) · „Device compliance policies overview" (learn.microsoft.com/intune/device-security/compliance/overview) · „Secure Boot enabled device shows not compliant" (learn.microsoft.com/troubleshoot/mem/intune/device-protection/secure-boot-enabled-device-shows-not-compliant) · „Require a compliant device with Conditional Access" (learn.microsoft.com/entra/identity/conditional-access/policy-all-users-device-compliance) · „Conditional Access: Report-only mode" (learn.microsoft.com/entra/identity/conditional-access/concept-conditional-access-report-only) · „Target resources in Conditional Access" (learn.microsoft.com/entra/identity/conditional-access/concept-conditional-access-cloud-apps) · „Conditional Access overview" (learn.microsoft.com/entra/identity/conditional-access/overview) · „Manage emergency access accounts in Microsoft Entra ID" (learn.microsoft.com/entra/identity/role-based-access-control/security-emergency-access) · „Microsoft Intune Reports" (learn.microsoft.com/intune/device-management/reports/overview)