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.

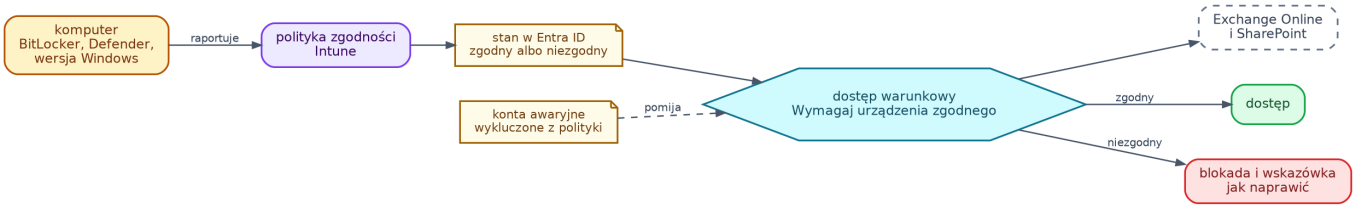
Jak to działa

□□ 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)

Revision #16
Created 2026-10-03 11:23:03 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:13 UTC by Tomasz Konieczny