# Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy

**Poziom: średniozaawansowany**

**Dotyczy: Microsoft 365 Business Premium, Microsoft Entra ID, Microsoft Entra Connect Sync, Intune**

**Czas: ~40 min**

*Zanim pierwszy komputer trafi pod Intune, ustawiamy licencje, synchronizujemy konta z Active Directory do Microsoft Entra ID i wyznaczamy grupy pilotażowe. Strona jest planem całego wdrożenia: co kupujemy, co konfigurujemy, w jakiej kolejności obejmujemy działy i jak się wycofujemy, gdy coś pójdzie źle.*

**ZAŁOŻENIA SCENARIUSZA**

komputery w Swarzędzu są w sieci centrali (VLAN 30 za `fw01`) i widzą `dc01` oraz `dc02` bez tunelu, więc hybrid join i Entra Connect Sync (`sync01` w VLAN 10) działają tak samo jak w biurze. Przy osobnej lokalizacji z routerem `rtr-mag01` komputery magazynu potrzebują tunelu do kontrolerów domeny: IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy.

**Skróty użyte na tej stronie (12)**

| Skrót | Co znaczy |
|---|---|
| **AD** | Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie |
| **EPM** | Endpoint Privilege Management: funkcja Intune, która pozwala użytkownikom uruchamiać wskazane programy z podniesionymi uprawnieniami, wymaga osobnej licencji ponad Business Premium |
| **FAQ** | Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami |
| **GPO** | Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery |
| **IT** | Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy |

| Skrót | Co znaczy |
|---|---|
| **MDM** | Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi |
| **PKI** | Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów |
| **SCP** | Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym |
| **UPN** | User Principal Name: login w formie adresu, np. jan.nowak@zielona.example |
| **URL** | Uniform Resource Locator: adres strony lub zasobu |
| **VLAN** | Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie |
| **WIP** | Windows Information Protection: starsza funkcja ochrony danych firmowych w aplikacjach, której nazwa przetrwała w niektórych menu Intune |

# Fiszka

Ścieżki w centrach administracyjnych podajemy po angielsku, tak jak w dokumentacji Microsoftu. Interfejs bywa po polsku, a Microsoft co jakiś czas przenosi pozycje menu, więc przy rozbieżności szukamy po nazwie ustawienia.

**□□ KLIKAMY W INTERFEJSIE**

## Przypisanie licencji grupie: Microsoft 365 admin center

```
Microsoft 365 admin center → Billing → Licenses → Assign licenses
→ wybieramy grupę, np. GG_Intune_Pilot
→ wybieramy subskrypcję Microsoft 365 Business Premium
→ Assign licenses
```

Licencjonowanie grupowe wymaga Microsoft Entra ID P1, które mamy w pakiecie, a każdy użytkownik musi mieć ustawioną lokalizację (kraj użycia). Grupy zagnieżdżone nie są obsługiwane, więc licencjonujemy grupy płaskie.

**□□ ZRZUT EKRANU DO UZUPEŁNIENIA**

Zrzut do uzupełnienia: ekran Microsoft 365 admin center → Billing → Licenses po przypisaniu licencji, widoczna subskrypcja Microsoft 365 Business Premium, zakładka Groups z grupą `GG_Intune_Pilot` i liczbą przypisanych licencji.

**ZMIENIA SYSTEM**

## Dodanie sufiksu UPN do lasu Active Directory: Set-ADForest

```
Get-ADForest | Set-ADForest -UPNSuffixes @{add="NazwaDomenyPublicznej"}
```

> (gdzie `NazwaDomenyPublicznej` to domena zweryfikowana w Microsoft 365, u nas `zielona.example`, taka sama jak w adresach e-mail)

Domena Active Directory `ad.zielona.example` nie jest domeną pocztową. Gdyby konta synchronizowały się z sufiksem, którego nie zweryfikowaliśmy w tenancie, Microsoft Entra ID przeliczy nazwę logowania na `NazwaPocztowa@domena-poczatkowa.onmicrosoft.com`. Dlatego sufiks dokładamy i weryfikujemy domenę przed pierwszą synchronizacją.

**UPN** = User Principal Name: login w formie adresu, np. jan.nowak@zielona.example

**ZMIENIA SYSTEM**

## Zmiana sufiksu UPN jednego użytkownika: Set-ADUser

```
Set-ADUser -Identity nazwa_usera -UserPrincipalName "nazwa_usera@NazwaDomenyPublicznej"
```

Przykład weryfikacji:

```
Get-ADUser jan.nowak -Properties UserPrincipalName | Select-Object SamAccountName,
UserPrincipalName
```

```
SamAccountName UserPrincipalName
-------------- -----------------
jan.nowak      jan.nowak@zielona.example
```

**UPN** = User Principal Name: login w formie adresu, np. jan.nowak@zielona.example

**KLIKAMY W INTERFEJSIE**

## Weryfikacja domeny w Microsoft 365: Settings, Domains

```
Microsoft 365 admin center → Settings → Domains → Add domain
→ wpisujemy zielona.example → Use this domain
```

```
→ Verify (rekord TXT w DNS domeny publicznej)
```

**□□ TYLKO ODCZYT**

## Sprawdzenie harmonogramu synchronizacji na sync01: Get-ADSyncScheduler

```
Get-ADSyncScheduler
```

Polecenie uruchamiamy na serwerze z Microsoft Entra Connect Sync. Domyślny odstęp między cyklami to 30 minut, pole `SyncCycleEnabled` musi mówić `True`.

**□□ ZMIENIA SYSTEM**

## Wymuszenie synchronizacji różnicowej na sync01: Start-ADSyncSyncCycle

```
Start-ADSyncSyncCycle -PolicyType Delta
```

Używamy po dodaniu użytkownika do grupy pilotażowej, żeby nie czekać na najbliższy cykl. Pełną synchronizację (`-PolicyType Initial`) uruchamiamy tylko po zmianie reguł synchronizacji.

**□□ KLIKAMY W INTERFEJSIE**

## Ustawienie zakresu MDM: automatyczna rejestracja

```
Microsoft Intune admin center → Devices → Device onboarding → Enrollment
→ zakładka Windows → Automatic Enrollment
→ MDM user scope: Some → Select groups → GG_Intune_Pilot
→ MDM terms of use URL, MDM discovery URL, MDM compliance URL: zostawiamy wartości domyślne
```

W starszych opisach to samo ustawienie nazywa się Mobility (MDM and WIP) → Microsoft Intune w centrum Microsoft Entra. Jeżeli ekran wygląda inaczej, szukamy opcji MDM user scope.

**◫◫ ZRZUT EKRANU DO UZUPEŁNIENIA**

Zrzut do uzupełnienia: ekran Automatic Enrollment w Intune admin center, widoczne MDM user scope ustawione na Some, wybrana grupa `GG_Intune_Pilot` i domyślne adresy URL MDM.

◫◫ **MDM** = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi · **WIP** = Windows Information Protection: starsza funkcja ochrony danych firmowych w aplikacjach, której nazwa przetrwała w niektórych menu Intune · **URL** = Uniform Resource Locator: adres strony lub zasobu

**◫◫ TYLKO ODCZYT**

### Utworzenie dynamicznej grupy urządzeń hybrid joined: Entra ID, Groups

```
Microsoft Entra admin center → Entra ID → Groups → New group
→ Group type: Security
→ Group name: Intune-Urzadzenia-Hybrid
→ Membership type: Dynamic Device
→ Add dynamic query → Edit
```

Reguła członkostwa:

```
device.deviceTrustType -eq "ServerAD"
```

Wartość `ServerAD` oznacza urządzenie hybrid joined, `AzureAD` oznacza Entra joined, a `Workplace` Entra registered. W grupach dynamicznych licencji Entra ID P1 wymaga każdy użytkownik, urządzenia licencji nie potrzebują.

# Z życia wzięte

**◫◫ Z ŻYCIA WZIĘTE**

Poniedziałek, 9:30. Pan Zbigniew pyta, ile to potrwa i kiedy jego laptop będzie „w chmurze". Tomek rysuje na tablicy cztery pudełka z datami, a pan Zbigniew zauważa, że trzecie wypada w listopadzie, w czasie zakazu zmian. Wniosek: magazyn Swarzędz dostaje swoją fazę dopiero po 6 stycznia, a księgowość musi zdążyć przed 15 listopada i omijać ostatnie trzy dni

robocze miesiąca. Plan z datami wisi od tej chwili nad biurkiem Tomka.

# Jak to działa

**Rozwiń: jak to działa pod spodem**

## Licencje: co mamy, czego nie mamy

> **Pojęcie: licencja.** Prawo konkretnego użytkownika do korzystania z usługi. Intune i Entra ID nie działają dla użytkownika bez przypisanej licencji, a komputer rejestruje się w Intune w imieniu zalogowanego użytkownika.

Według dokumentacji Microsoftu (stan na październik 2026) pakiet Microsoft 365 Business Premium, przeznaczony dla firm do 300 użytkowników, zawiera między innymi Microsoft Intune Plan 1, Microsoft Entra ID P1, Microsoft Defender for Business i Microsoft Defender for Office 365 Plan 1. Zielona ma 180 osób, więc mieści się w limicie. Skład pakietu sprawdzamy przy zakupie i przy każdym odnowieniu, bo Microsoft go zmienia.

| Funkcja | Czy wystarczy Business Premium | Uwaga |
|---|---|---|
| Rejestracja, profile, zasady zgodności, aplikacje Win32 | tak | to jest Intune Plan 1 |
| Dostęp warunkowy i uwierzytelnianie wieloskładnikowe | tak | Entra ID P1 |
| Dostęp warunkowy oparty na ryzyku logowania | nie | wymaga Entra ID P2, w Business Premium dostępne w dodatkowym pakiecie Defender Suite |
| Windows LAPS z hasłem w Entra ID | tak | dostępne od Entra ID Free |
| Remediations (skrypty wykrywania i naprawy) | do sprawdzenia | dokumentacja wymaga m.in. Windows Enterprise E3 lub E5, Business Premium nie jest tam wymieniony |
| Microsoft Cloud PKI | nie | wymaga dodatkowej subskrypcji ponad Intune Plan 1 lub 2 (Intune Suite albo osobny dodatek) |
| Endpoint Privilege Management, Remote Help, Advanced Analytics | nie | Intune Plan 2 albo Intune Suite |

| Funkcja | Czy wystarczy Business Premium | Uwaga |
|---|---|---|
| Windows Autopatch i hotpatch | tak, z warunkami | Business Premium jest na liście licencji, hotpatch wymaga Windows 11 24H2 lub nowszego z włączonym VBS |

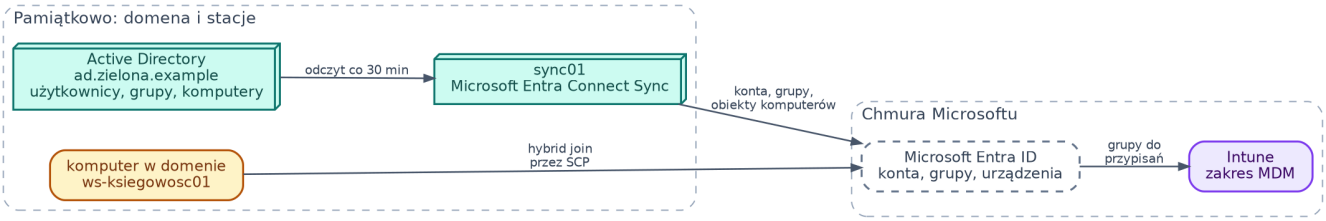
> ⚠ Licencje zmieniają się częściej niż nasza wiedza o nich. Przed zakupem dodatku (Cloud PKI, Remediations, EPM) potwierdzamy wymagania w aktualnej dokumentacji i u dostawcy licencji. Strony o profilach i certyfikatach powtarzają ostrzeżenie przy każdej funkcji spoza Plan 1.

# Synchronizacja: konta z AD do Entra ID

**Pojęcie: Microsoft Entra Connect Sync.** Program na osobnym serwerze, który co 30 minut czyta użytkowników, grupy i komputery z Active Directory i zapisuje je w Microsoft Entra ID. Dla komputerów w trybie hybrid joined jest to konieczne, bo to on przenosi do chmury obiekty komputerów.

**Pojęcie: Microsoft Entra Cloud Sync.** Lżejsza odmiana synchronizacji: w firmie stoi tylko mały agent, a konfiguracją zarządza chmura. Długo nie synchronizowała urządzeń potrzebnych do hybrid join, ale według przewodnika decyzyjnego Microsoftu zaktualizowanego 6 października 2026 robi to już, po osobnym włączeniu tej funkcji.

Szczegóły i nasza ocena są na stronie Entra Connect i Cloud Sync: synchronizacja ad.zielona.example z Entra ID.



*Active Directory na dc01 i dc02 synchronizuje konta przez sync01 do Entra ID, komputery domenowe rejestrują się w Entra ID przez SCP, Intune bierze grupy z Entra ID (kliknięcie otwiera pełny rozmiar)*

| Cecha | Entra Connect Sync | Cloud Sync |
|---|---|---|
| Gdzie stoi logika synchronizacji | na serwerze w firmie | w chmurze, w firmie tylko agent |
| Synchronizacja urządzeń dla hybrid join | tak | tak od jesieni 2026, włączana osobno (status do potwierdzenia) |
| Wymagania dla serwera | domenowy Windows Server z pulpitem, zalecany 2022 lub 2025 | agent może stać na kontrolerze domeny |
| Nasz wybór | tak, bo działa i istniejące komputery rejestrujemy jako hybrid joined | ocena przy wymianie `sync01` |

Dla Zielonej wybieramy Entra Connect Sync na nowej maszynie wirtualnej `sync01` (propozycja nazwy, na klastrze `hv01` i `hv02`). Serwer musi być w domenie, nie może być Server Core i traktujemy go jak element o największych uprawnieniach: dostęp tylko dla administratorów domeny, uwierzytelnianie wieloskładnikowe dla kont uprzywilejowanych. Microsoft ogłosił też wymóg aktualizacji do wersji 2.6.84.0 lub nowszej wraz z uwierzytelnianiem aplikacyjnym do 7 kwietnia 2027, więc numer wersji sprawdzamy przy instalacji.

Ustawienia, które pilnujemy podczas instalacji:

- Konfiguracja opcji urządzeń (Configure device options), a w niej Configure Microsoft Entra hybrid join, z wyborem systemów Windows 10 lub nowszych. To ona tworzy punkt połączenia usługi (SCP), po którym komputery znajdują tenant.
- Filtrowanie po jednostkach organizacyjnych: synchronizujemy `OU=Komputery` i jednostki z kontami użytkowników. Komputery poza zakresem synchronizacji nie zostaną hybrid joined. Filtr korzysta z pełnej nazwy jednostki, więc po zmianie nazwy jednostki z ukośnikiem (opisanej na stronie o BitLockerze) poprawiamy też filtr.
- Domeny pocztowe: UPN użytkowników musi kończyć się zweryfikowaną domeną `zielona.example`, inaczej konta trafią do chmury z sufiksem `onmicrosoft.com`.

# Zakres MDM i grupy

> **Pojęcie: MDM user scope.** Ustawienie, które mówi, kogo komputery mają rejestrować się w Intune automatycznie: nikogo (None), wybrane grupy (Some) albo wszystkich (All). Zakres liczy się po użytkowniku, który się loguje, nie po komputerze. Na czas pilotażu ustawiamy Some z grupą `GG_Intune_Pilot` i poszerzamy z fazą. Użytkownicy nie powinni być jednocześnie w zakresie MDM i w zakresie WIP, który ustawiamy na None.

Grupy trzymamy w dwóch rodzajach. Grupy użytkowników `GG_Intune_Pilot`, `GG_Intune_Ksiegowosc`, `GG_Intune_Magazyn`, `GG_Intune_Handlowcy` zakładamy w AD, jak resztę grup globalnych (`GG_`), i synchronizujemy. Grupy urządzeń (`Intune-Urzadzenia-Hybrid`, grupa pilotażowa urządzeń) zakładamy w Entra ID, najlepiej jako dynamiczne.

# Fazy


Faza 0: przygotowanie
licencje, Entra Connect, grupy, konta awaryjne
Faza 1: pilotaż IT
3 komputery zespołu IT
bramka: brak zgłoszeń
przez 2 tygodnie
Faza 2: księgowość
pani Halina i zespół, poza zamknięciem miesiąca
zakaz zmian
15 listopada do 6 stycznia
Faza 3: magazyn Swarzędz
po 6 stycznia, poza 6:00
Faza 4: handlowcy
komputery w terenie, najwięcej zysku

*Fazy wdrożenia: przygotowanie, pilotaż IT, księgowość, przerwa na zakaz zmian od 15 listopada do 6 stycznia, magazyn, handlowcy (kliknięcie otwiera pełny rozmiar)*

Terminy poniżej są propozycją do uzgodnienia, wynikają z kalendarza awarii Zielonej: zamknięcie miesiąca w ostatnich trzech dniach roboczych, szczyt w magazynie od listopada i zakaz zmian od 15 listopada do 6 stycznia.

| Faza | Kto | Co włączamy | Kryterium przejścia | Termin orientacyjny |
|---|---|---|---|---|
| 0. Przygotowanie | zespół IT | licencje, `sync01`, domena, UPN, konta awaryjne, grupy | konta widoczne w Entra ID, licencje przypisane | do połowy października |
| 1. Pilotaż IT | trzy komputery IT, w tym Tomka | hybrid join, automatyczna rejestracja, profil z jednym ustawieniem, jedna aplikacja Win32, zasady zgodności bez dostępu warunkowego | dwa tygodnie bez zgłoszeń, `dsregcmd /status` poprawny | do końca października |
| 2. Księgowość | pani Halina i zespół | te same profile i zgodność, dostęp warunkowy w trybie tylko raportowania | brak zgłoszeń przez tydzień, Optima działa | od 2 do 13 listopada, poza zamknięciem miesiąca i piątkami po 15:00 |
| 3. Magazyn Swarzędz | Marek i zmiana | profile, aplikacje, aktualizacje w pierścieniu krytycznym | skanery i WMS bez zmian | po 6 stycznia, rejestracja po zmianie, nie o 6:00 |
| 4. Handlowcy | pięciu handlowców w terenie | wszystko plus certyfikaty, Wi-Fi i VPN z Intune | laptop Kasi aktualizuje się z hotelu | styczeń i luty |

Dlaczego handlowcy na końcu, skoro zyskują najwięcej? Bo pomoc dla nich jest tylko zdalna: jeśli rejestracja się nie uda, nie podejdziemy do biurka. Wchodzimy do nich z wypracowanym procesem, a ich laptopy rejestrujemy najlepiej podczas wizyty w biurze.

# Ryzyka

| Ryzyko | Skutek | Zabezpieczenie |
|---|---|---|
| Zły UPN w synchronizacji | użytkownik nie zaloguje się, konta z końcówką `onmicrosoft.com` | sufiks UPN i weryfikacja domeny przed pierwszą synchronizacją |

| Ryzyko | Skutek | Zabezpieczenie |
|---|---|---|
| Dostęp warunkowy włączony zbyt wcześnie | blokada poczty całej firmy | najpierw tryb tylko raportowania, konta awaryjne wykluczone |
| Konflikt GPO i profilu Intune o to samo ustawienie | niespodziewane zachowanie komputera | jedna metoda na ustawienie, GPO wyłączamy po potwierdzeniu, że profil doszedł |
| Szyfrowanie wymuszone bez kopii klucza | dysk bez możliwości odzyskania | klucz w Entra ID przed szyfrowaniem, patrz strona o profilach |
| Rejestracja w złym momencie | przestój w księgowości albo magazynie | kalendarz awarii: nie w zamknięcie miesiąca, nie o 6:00, nie w piątek po 15:00 |
| Serwer `sync01` niedostępny dłużej niż 7 dni | po powrocie potrzebna pełna synchronizacja | monitorowanie usługi, plan odtworzenia maszyny |

# Plan wycofania

Wycofujemy warstwa po warstwie, od najłatwiejszej.

1. Dostęp warunkowy: przełączamy politykę na tryb tylko raportowania albo wyłączamy. Konto awaryjne daje dostęp, gdyby coś zablokowało administratorów.
2. Profil, aplikacja albo zasada zgodności: usuwamy przypisanie grupy. Komputer pobierze zmianę przy najbliższym zgłoszeniu do Intune. Nie wszystkie ustawienia wracają do poprzedniej wartości po usunięciu przypisania, dlatego odwracalność sprawdzamy w pilotażu, a GPO zostaje włączone, dopóki profil nie zostanie potwierdzony.
3. Rejestracja komputera: usuwamy użytkownika z grupy zakresu MDM, a na komputerze akcja Retire usuwa dane i ustawienia firmowe zarejestrowane przez Intune. Komputer zostaje w domenie, a klucz BitLockera zostaje w AD.
4. Cały tenant: wyłączamy w GPO automatyczną rejestrację MDM i ustawiamy zakres MDM na None. Komputery nadal działają jak przed wdrożeniem, bo domena nigdy nie przestała nimi rządzić.

Wycofanie jest tym prostsze, że w modelu hybrid joined domena zostaje na swoim miejscu. Intune dokładamy obok, nie zamiast.

# Częste błędy

| Objaw | Przyczyna | Co robimy |
|---|---|---|

| | | |
|---|---|---|
| Użytkownik w Entra ID ma nazwę `jan.nowak@...onmicrosoft.com`, a nie `@zielona.example` | w AD sufiks UPN nie jest zweryfikowany w tenancie | dodajemy sufiks, weryfikujemy domenę w Microsoft 365, zmieniamy UPN w AD i czekamy na synchronizację |
| Komputer domenowy nie pojawia się w Entra ID jako hybrid joined | jednostka z komputerem poza zakresem synchronizacji albo brak SCP | sprawdzamy filtr jednostek w Entra Connect i opcje urządzeń, potem `dsregcmd /status` na komputerze |
| Licencja nie przypisuje się grupie | użytkownik bez lokalizacji albo grupa zagnieżdżona | ustawiamy lokalizację użytkownika, przypisujemy licencję grupie płaskiej |
| Użytkownik w grupie pilotażowej, a komputer się nie rejestruje, błąd `0x80180018` | użytkownik nie ma licencji Intune | przypisujemy licencję, wymuszamy `gpupdate /force` |
| Błąd `0x80180003` przy rejestracji | użytkownik poza zakresem MDM user scope | dodajemy użytkownika do grupy w zakresie MDM |
| Zmiana w AD nie widać w chmurze | harmonogram synchronizacji wyłączony albo przerwa dłuższa niż 7 dni | `Get-ADSyncScheduler`, w razie potrzeby `Start-ADSyncSyncCycle -PolicyType Initial` |

# □□ Ćwiczenia

1. Dlaczego do hybrid join zostajemy przy Entra Connect Sync, skoro Cloud Sync też synchronizuje już urządzenia?

**Odpowiedź**

Hybrid join wymaga, żeby obiekty komputerów z Active Directory trafiały do Microsoft Entra ID. Gdy planowaliśmy wdrożenie, robił to tylko Entra Connect Sync; według przewodnika Microsoftu z 6 października 2026 Cloud Sync też to umie, ale funkcję włącza się osobno, a jej status jeszcze potwierdzamy. Entra Connect Sync na `sync01` działa i ma skonfigurowany hybrid join, a dwa narzędzia nie mogą synchronizować tych samych obiektów, więc zmianę rozważamy dopiero przy wymianie `sync01`.

1. Zakres MDM ustawiamy na Some z grupą `GG_Intune_Pilot`. Tomek loguje się na laptopie pani Haliny. Czy ten laptop zarejestruje się w Intune?

**Odpowiedź**

Tak, jeśli Tomek ma licencję i jest w grupie pilotażowej, bo zakres MDM liczy się po użytkowniku, który się loguje, nie po właścicielu komputera. Dlatego w pilotażu nie logujemy się na komputerach działów, które nie są jeszcze w fazie.

1. Chcemy zacząć od magazynu w Swarzędzu 20 listopada. Co mówi na to kalendarz Zielonej?

**Odpowiedź**

Od 15 listopada do 6 stycznia obowiązuje zakaz zmian w infrastrukturze, a magazyn pracuje wtedy na trzy zmiany. Magazyn dostaje fazę po 6 stycznia, a księgowość musimy zakończyć do 13 listopada.

**Powiązane:** Intune obok domeny: audyt GPO i plan migracji · Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot · Windows LAPS: hasło lokalnego administratora w Active Directory · BitLocker z kluczem odzyskiwania w Active Directory

**Źródła:** Microsoft Learn, „Microsoft 365 Business Premium security FAQ" (learn.microsoft.com/microsoft-365/admin/security-and-compliance/m365bp-security-faq) · „Add Microsoft Defender Suite for Business Premium" (learn.microsoft.com/microsoft-365/admin/security-and-compliance/add-defender-suite-business-premium) · „Microsoft Cloud PKI for Microsoft Intune" (learn.microsoft.com/intune/cloud-pki) · „Use Remediations to detect and fix support issues" (learn.microsoft.com/intune/device-management/tools/deploy-remediations) · „Prerequisites for Windows Autopatch" i „Hotpatch updates" (learn.microsoft.com/windows/deployment/windows-autopatch) · „Conditional Access overview" (learn.microsoft.com/entra/identity/conditional-access/overview) · „Prerequisites for Microsoft Entra Connect" (learn.microsoft.com/entra/identity/hybrid/connect/how-to-connect-install-prerequisites) · „Migrate from Microsoft Entra Connect to Cloud Sync: Decision Guide" (learn.microsoft.com/entra/identity/hybrid/cloud-sync/connect-to-cloud-sync-decision-guide) · „Microsoft Entra Connect Sync: Scheduler" (learn.microsoft.com/entra/identity/hybrid/connect/how-to-connect-sync-feature-scheduler) · „UserPrincipalName and non-routable domains" (learn.microsoft.com/entra/identity/hybrid/connect/plan-connect-userprincipalname) · „Enable MDM automatic enrollment for Windows" (learn.microsoft.com/intune/device-enrollment/windows/enable-automatic-mdm) · „Dynamic membership rules for groups" (learn.microsoft.com/entra/identity/users/groups-dynamic-membership) · „Assign or remove licenses for a group" (learn.microsoft.com/entra/identity/users/licensing-groups-assign) · „Add a domain to Microsoft 365" (learn.microsoft.com/microsoft-365/admin/setup/add-domain) · „Diagnose MDM enrollment" (learn.microsoft.com/windows/client-management/mdm-diagnose-enrollment)

---

Revision #19
Created 2026-10-03 11:22:59 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:09 UTC by Tomasz Konieczny