

# **Renowacja za pomocą usługi Microsoft Intune**

**w DB Workplace Mobile**

**Smartfon/tablet Samsung  
(system operacyjny Android 15 i nowsze)**

15 kwietnia 2026

## Spis treści

<b>1 Konieczne kroki przed renowacją</b>	<b>4</b>
1.1 Utwórz kopię zapasową danych	4
1.2 Aplikacja Authenticator – opcjonalnie	4
1.3 Tworzenie tymczasowej legitymacji pracownika DB – tryb zaawansowany	4
<b>2 Rozpocznij przywracanie: zresetuj smartfon/tablet</b>	<b>7</b>
2.1 Samodzielne zresetowanie smartfona/tabletu	7
2.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk	8
<b>3 Ponowna konfiguracja w Microsoft Intune</b>	<b>9</b>
3.1 Wybierz język	9
3.2 Zaakceptuj umowę licencyjną użytkownika końcowego	10
3.3 Skonfiguruj Wi-Fi	11
3.4 Konfiguracja Wi-Fi w budynkach DB	12
<b>4 Rejestracja urządzenia Samsung w systemie DB</b>	<b>13</b>
4.1 Skonfiguruj profil służbowy	14
4.2 Ustawianie blokady ekranu	15
4.3 Instalowanie aplikacji DB	16
4.4 Konto Google – nie jest konieczne	17
4.5 Aktywacja usług Google	18
4.6 Automatyczna instalacja aplikacji bazodanowych	19
<b>5 Aktywacja urządzenia – utworzenie tymczasowej legitymacji pracownika DB (TAP)</b>	<b>20</b>
5.1 Utwórz tymczasową legitymację pracownika DB (TAP)	20
5.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika	23
<b>6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)</b>	<b>25</b>
6.1 Konfiguracja dostępu do wszystkich aplikacji DB i stron internetowych	27
6.2 Aplikacje DB	28
<b>7 Wymagane ustawienia</b>	<b>29</b>
7.1 Sprawdź dostępność aktualizacji systemu operacyjnego	29
7.2 Outlook	30
7.2.1 Konfiguracja programu Outlook / Utworzenie konta e-mail / Konfiguracja szyfrowania wiadomości e-mail	30
7.2.2 Konfiguracja podpisu w wiadomościach e-mail	33
7.2.3 Synchronizacja poczty e-mail – wszystkie wiadomości zawsze aktualne	35

7.3 Aplikacja MS Defender	35
7.3.1 Konfiguracja aplikacji MS Defender	35
7.3.2 Przyznaj uprawnienia	38
7.4 DB M 365	41
7.5 Wyłącz przycisk Bixby	42
7.6 Ponowne włączenie aplikacji Microsoft Authenticator do uwierzytelniania	43
Gratulacje!	43

## 1 Kroki niezbędne przed renowacją

Jeśli smartfon/tablet ma problemy, takie jak spowolnienie działania, zawieszanie się lub częste awarie, pomocne może być przywrócenie ustawień fabrycznych.

Konieczne są następujące kroki:

---

### 1.1 Utwórz kopię zapasową danych

> **Uwaga:** Instrukcje wideo znajdziesz na stronie [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

- **Utwórz kopię zapasową danych**, gdy tylko otrzymasz e-mail z potwierdzeniem terminu migracji

Aby to zrobić, wykonaj następujące czynności:

- a) Utwórz kopię zapasową danych służbowych i ustawień
- b) Utwórz kopię zapasową danych osobistych i ustawień

Jeśli to możliwe:

- c) Usuń konto Samsung lub Google ze smartfona/tabletu
- d) Wyjmij wszystkie karty pamięci ze smartfona/tabletu

> Instrukcje dotyczące tworzenia kopii zapasowej danych można znaleźć na stronie [Tworzenie kopii zapasowej danych](#)

---

### 1.2 Aplikacja Authenticator – opcjonalnie

**Uwaga:** Te informacje dotyczą wyłącznie użytkowników, którzy aktywnie korzystają z aplikacji Authenticator, np. w celu uzyskania dostępu administracyjnego za pomocą tzw. konta dwuskładnikowego lub w celu uwierzytelniania dwuetapowego, np. w przypadku VPN na komputerze MAC w ramach Basic Workplace.

- Należy pamiętać, że aplikacja Authenticator nie może być używana podczas przywracania systemu.
- Nie są wymagane żadne dalsze kroki.
- Po przywróceniu urządzenia aplikację należy ponownie aktywować. Jest to opisane w [rozdziale 7.5 Ponowna aktywacja aplikacji Microsoft Authenticator](#).
- Jeśli musisz korzystać z aplikacji Authenticator podczas odzyskiwania, użyj innego smartfona/tabletu, aby połączyć się z aplikacją Authenticator. W tym celu postępuj zgodnie z instrukcjami krok po kroku dotyczącymi [konfiguracji uwierzytelniania wieloskładnikowego \(MFA\)](#).

---

### 1.3 Tworzenie tymczasowej legitymacji pracownika DB (TAP) – tryb ekspercki

Po utworzeniu kopii zapasowej danych masz dwie możliwości:

1. Twój smartfon/tablet nadal częściowo działa, przejdź do następnej strony
2. Twój smartfon/tablet w ogóle nie działa, przejdź do

> [Rozdział 2.2 Resetowanie smartfona/tabletu za pomocą aplikacji IT ServiceDesk](#)

Smartfon/tablet nadal działa częściowo:

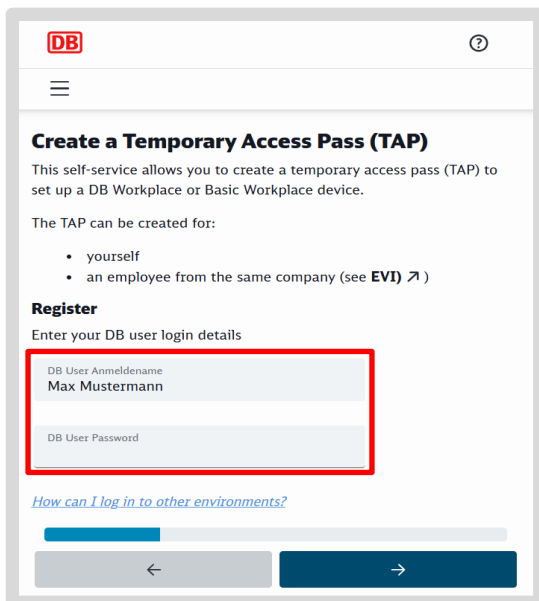
> **Uwaga:** Film instruktażowy znajdziesz na stronie [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

### Jeśli nadal masz zainstalowaną aplikację Welcome:

- otwórz aplikację *Welcome* i kliknij „Pomoc”
- Następnie kliknij „Temporary Access Pass (TAP)”, aby ją utworzyć

### Jeśli nie masz zainstalowanej aplikacji Welcome:

- Wejdź na [stronę db.de/tap](https://db.de/tap) i wprowadź swoją nazwę użytkownika DB oraz hasło użytkownika DB
- Wybierz „Dla siebie” i kliknij niebieski przycisk
- Teraz wybierz „DB Workplace Mobile”
- Wyświetli się tymczasowa legitymacja pracownika DB
- Jest on **ważny przez 60 minut** i można go używać **na wielu smartfonach/tabletach**



**Create a Temporary Access Pass (TAP)**

This self-service allows you to create a temporary access pass (TAP) to set up a DB Workplace or Basic Workplace device.

The TAP can be created for:

- yourself
- an employee from the same company (see [EVI](#)) ↗ )

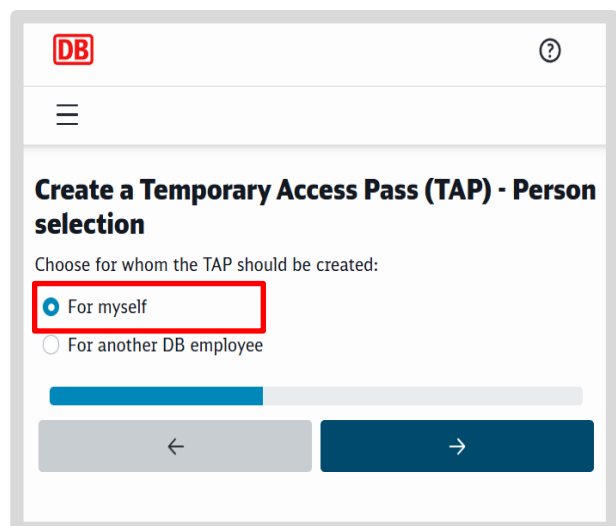
**Register**

Enter your DB user login details

DB User Anmeldenname  
Max Mustermann

DB User Password

[How can I log in to other environments?](#)

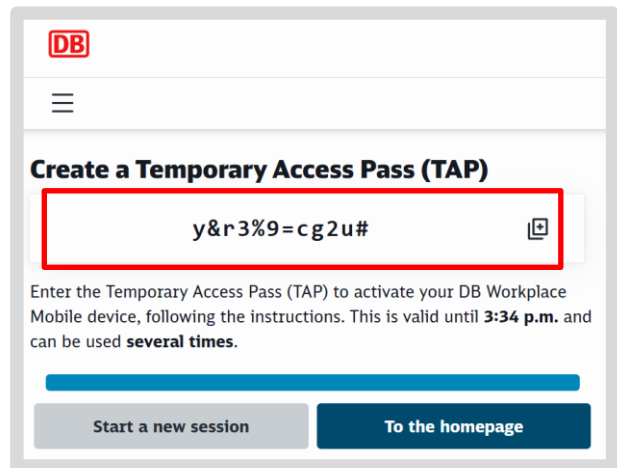
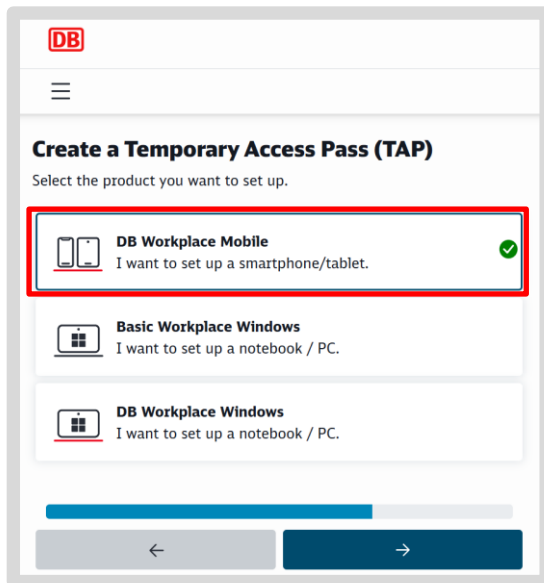


**Create a Temporary Access Pass (TAP) - Person selection**

Choose for whom the TAP should be created:

For myself

For another DB employee



**Ważne!**  
Kod **TAP** można wprowadzić wyłącznie w **aplikacji Intune**, nawet jeśli zostanie on wymagany w innej aplikacji DB lub na innym urządzeniu.

- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku
- Będzie on potrzebny później podczas logowania po zresetowaniu smartfona/tabletu
- Masz **teraz 60 minut** na zresetowanie smartfona/tabletu
- > Przejdź bezpośrednio do [rozdziału 2.1 Samodzielne resetowanie smartfona/tabletu](#)

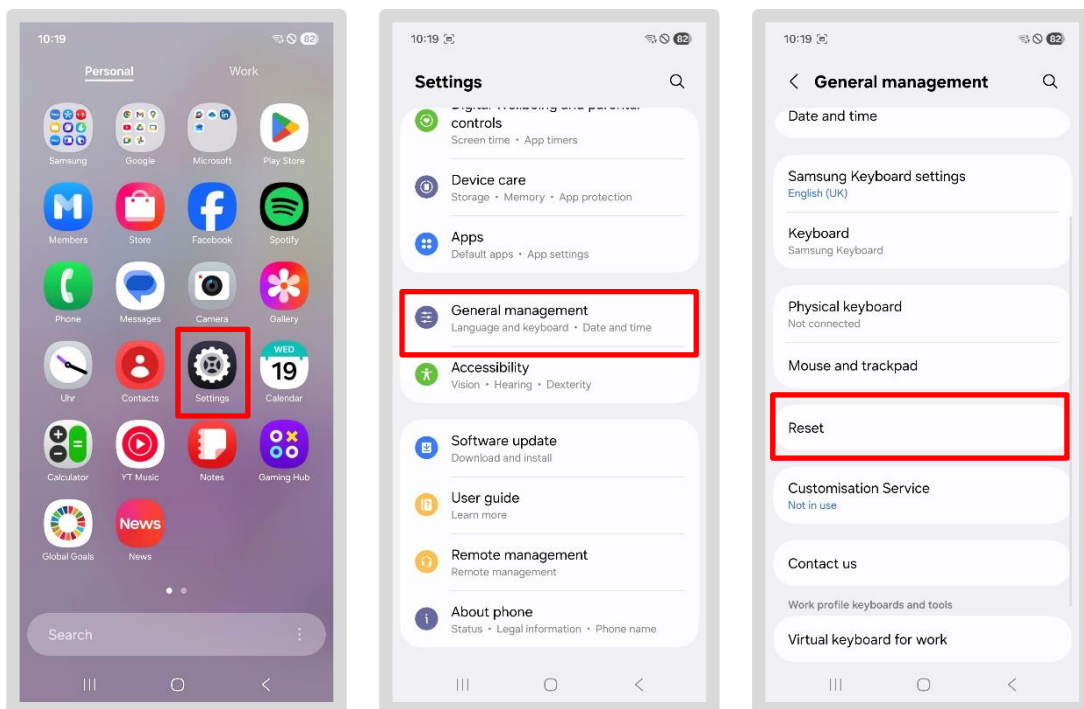
## 2 Rozpocznij odzyskiwanie: zresetuj smartfon/tablet

**Uwaga:** Poniższe ekrany mogą wyglądać inaczej w zależności od modelu smartfona/tabletu.

### 2.1 Samodzielne zresetowanie smartfona/tabletu

> **Uwaga:** Instrukcje wideo znajdziesz na stronie [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

- Przejdź do sekcji „Osobiste” na smartfonie/tablecie
- Naciśnij aplikację „Ustawienia”
- Kliknij „Zarząd”
- Przewiń w dół i dotknij „Resetuj”



- Następnie wybierz „Przywróć ustawienia fabryczne”
- Pojawi się komunikat wyjaśniający, co zostanie usunięte w wyniku resetowania
- Sprawdź, czy wykonałeś kopię zapasową danych służbowych (instrukcje: [Tworzenie kopii zapasowej danych](#))
- Następnie naciśnij przycisk „Resetuj”, wprowadź hasło blokady ekranu, a potem naciśnij „Usuń wszystko”
- Poczekaj kilka minut, a urządzenie zostanie automatycznie zresetowane

> Następnie przejdź do [rozdziału 3 „Ponowna konfiguracja w Microsoft Intune”](#)

---

## 2.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk

Jeśli smartfon/tablet przestał działać, wybierz ten krok:

- Otwórz aplikację IT ServiceDesk i wprowadź zgłoszenie dotyczące zresetowania smartfona/tabletu w sekcji „*Nowe zgłoszenie serwisowe*”.
- Jeśli nie możesz otworzyć aplikacji, zadzwoń pod ten numer:
- Infolinia IT ServiceDesk ds. migracji (poniedziałek–piątek, godz. 7:00–18:00)
  - Wewnętrzny: tel. 9833-8699
  - Zewnętrzny: Tel. 0361 430 8699
- IT ServiceDesk
  - Wewnętrzny: tel. 91-5555
  - Zewnętrzny: Tel. 0361 430 8200
  - Wybierz opcję menu zero
- Centrum Obsługi IT DB Cargo
  - Tel. 91 7777 (wewnętrzny)
  - Tel. 00800 327 978 35 (zewnętrzny)
  - Wybierz opcję menu zero
- Jeśli pojawiają się inne problemy, proszę wcześniej rozważyć następujące kwestie:
  - **Gdzie** wystąpiły **problemy**?
  - **Określ miejsce wystąpienia błędu**, abyśmy mogli szybciej udzielić Ci pomocy
  - **W przypadku problemów z certyfikatami**: Po rejestracji poczekaj **od 5 minut do 24 godzin**, aż wszystkie informacje i certyfikaty zostaną przesłane na Twój smartfon/tablet.

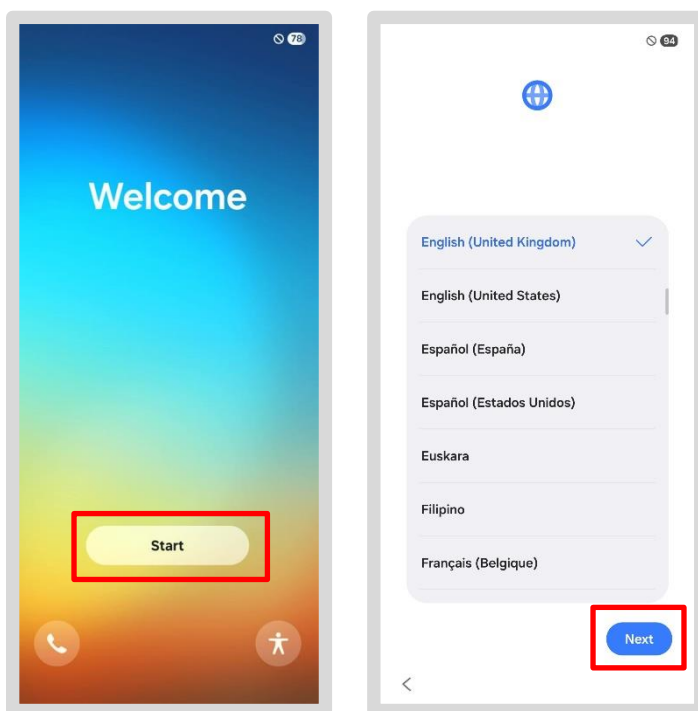
> Następnie przejdź do rozdziału 3 Skonfiguruj ponownie w Microsoft Intune

## 3 Ponowna konfiguracja w Microsoft Intune

### 3.1 Wybierz język

> **Uwaga:** Film instruktażowy można znaleźć na stronie [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

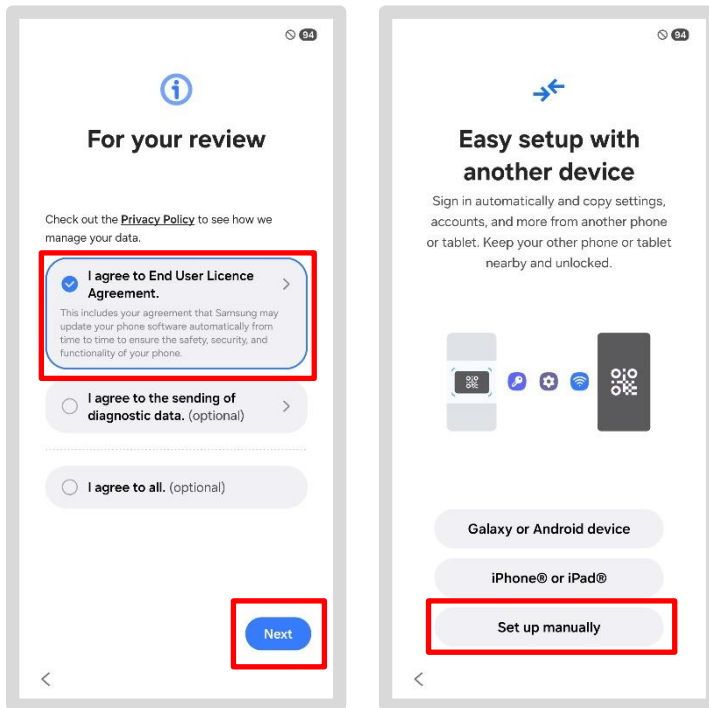
- Trzymaj tablet w **orientacji pionowej**, aby wyświetlić ekrany w takim samym układzie, jak pokazano w instrukcji
- Włącz smartfon/tablet
- Upewnij się, że smartfon/tablet jest podłączony do źródła zasilania lub ma wysoki poziom naładowania baterii podczas procesu przywracania
- Naciśnij „Start”
- Na następnym ekranie wybierz preferowany język z listy i dotknij „Dalej”



> Przejdź do rozdziału 3.2. Zaakceptuj umowę licencyjną użytkownika końcowego

### 3.2 Zaakceptuj umowę licencyjną użytkownika końcowego

- **Wystarczy** dotknąć opcji „Zgadzam się z umową licencyjną użytkownika końcowego”, a następnie „Dalej”
- W sekcji „Konfiguruj za pomocą innego urządzenia” dotknij „Konfiguruj ręcznie”



> Przejdź do [rozdziału 3.3 Konfiguracja Wi-Fi](#)

### 3.3 Konfiguracja sieci Wi-Fi w urządzeniu

Aby skonfigurować Wi-Fi, wybierz jedną z poniższych opcji:

- Korzystaj z **mobilnego transferu danych**, jeśli Twój smartfon/tablet ma kartę SIM (może to wiązać się z opłatami!).

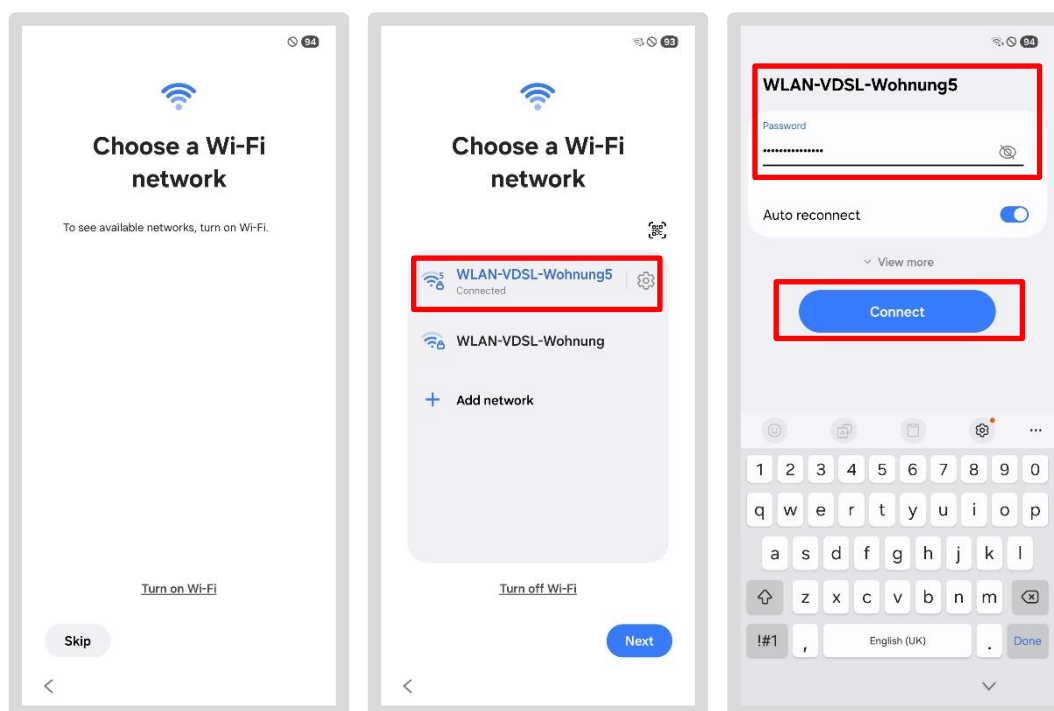
- Skonfiguruj hotspot na swoim prywatnym smartfonie/tablecie

lub

- Skorzystaj z hotspotu na smartfonie DB swojego kolegi
- Skorzystaj z Wi-Fi dbs4mobile, jeśli wykupiłeś ten produkt (zobacz: <https://dbquestions.extranet.deutschebahn.com/question/27780>)
- Skorzystaj z prywatnej sieci Wi-Fi, jeśli pracujesz z domu

Aby wybrać inną sieć Wi-Fi, postępuj w następujący sposób:

- Dotknij sieci Wi-Fi, którą chcesz wybrać
- Wprowadź swoje dane logowania i dotknij „Połącz”
- Jeśli pojawi się drugi monit, dotknij „Dalej”



Gdy urządzenie połączy się z siecią Wi-Fi, rozpocznie się połączenie z siecią DB.

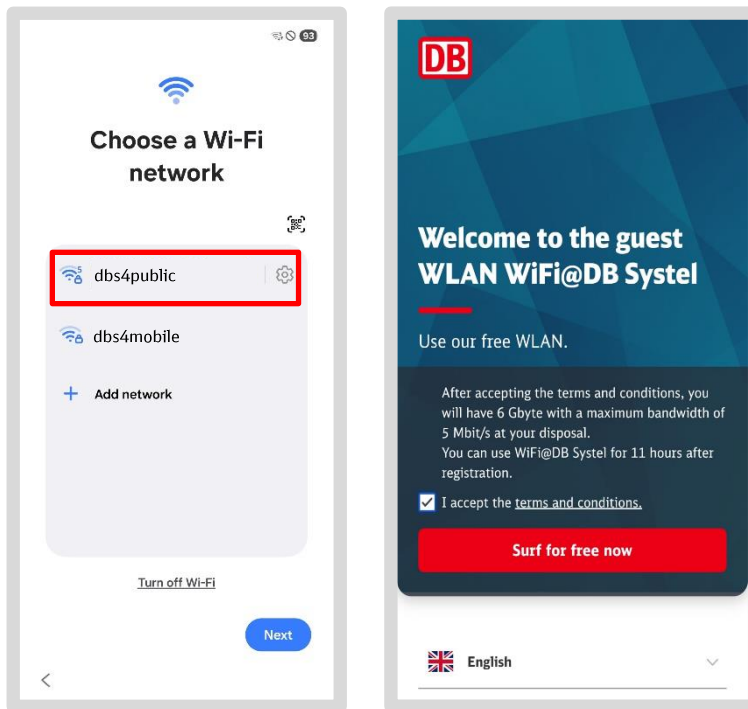
> Przejdź do [rozdziału 4 Rejestracja urządzenia Samsung w DB](#)

### 3.4 Konfiguracja Wi-Fi w budynkach DB

Ponieważ sieć Wi-Fi „dbs4public” nie zawsze działa zadowalająco w budynkach DB, zalecamy wybranie jednej z opcji opisanych w [rozdziale 3.3 Konfiguracja Wi-Fi](#).

Jeśli znajdujesz się w **budynku DB** i chcesz korzystać z sieci Wi-Fi „dbs4public”, postępuj w następujący sposób:

- Kliknij sieć Wi-Fi „dbs4public”
- Otworzy się okno dialogowe; zaakceptuj warunki
- Kliknij „Surfuj teraz za darmo”



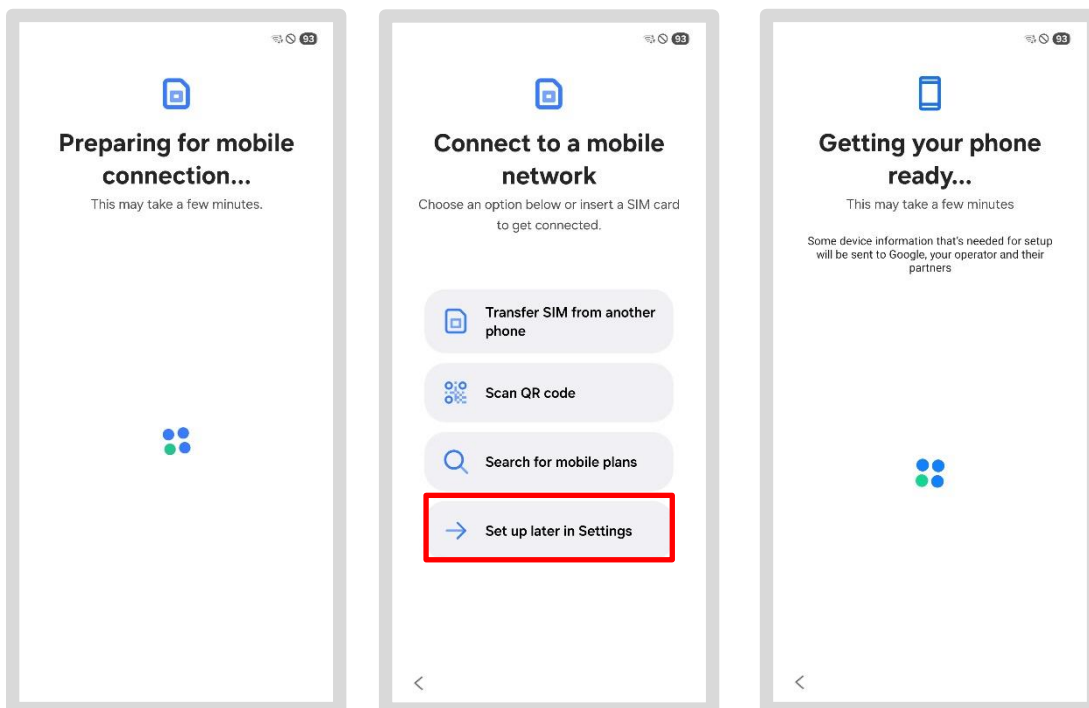
Gdy urządzenie połączy się z siecią Wi-Fi, rozpocznie się proces łączenia z siecią DB.

> Przejdź do [rozdziału 4 Rejestracja Samsunga w DB](#)

## 4 Rejestracja urządzenia Samsung w DB

W następnym kroku smartfon/tablet DB musi zostać ponownie podłączony do sieci DB (a dokładniej do Enterprise Mobility Management, czyli EMM). Poczekaj na zmieniające się informacje, aż pojawi się instrukcja. W zależności od połączenia sieciowego ekrany mogą migotać lub się zmieniać.

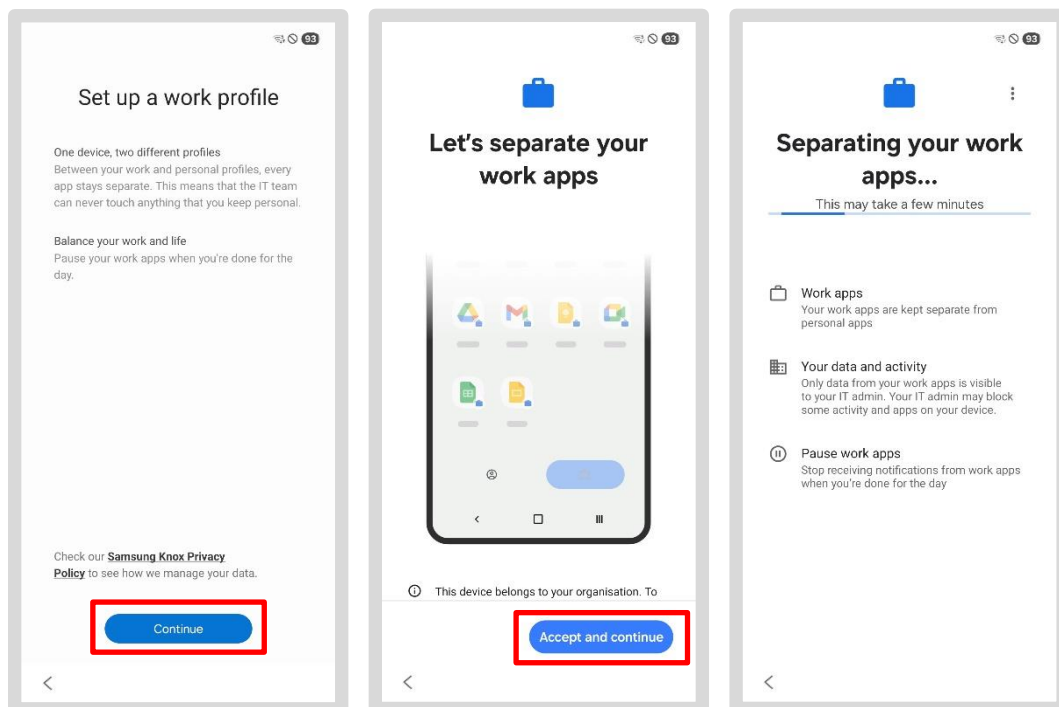
- Trzymaj tablet w **trybie pionowym**, jeśli do tej pory trzymałeś go w trybie poziomym
- Poszczególne ekrany będą teraz migać
- Naciśnij „*Skonfiguruj później*”, a kilka ekranów wyświetli się ponownie bez konieczności wykonywania jakichkolwiek czynności



## 4.1 Skonfiguruj profil służbowy

Aby przypisać aplikacje służbowe do smartfona/tabletu, konieczne jest utworzenie profilu służbowego. Należy go skonfigurować tutaj:

- Trwa konfiguracja smartfona/tabletu
- Potwierdź poniższe zapytanie, wybierając opcję „Kontynuuj”
- Gdy pojawi się komunikat „Skonfiguruj profil służbowy”, dotknij „Kontynuuj” lub „Zgadzam się”
- Gdy pojawi się komunikat „Administrator IT może kontrolować to urządzenie i blokować aplikacje” (tekst może być skrócony), naciśnij „Kontynuuj”

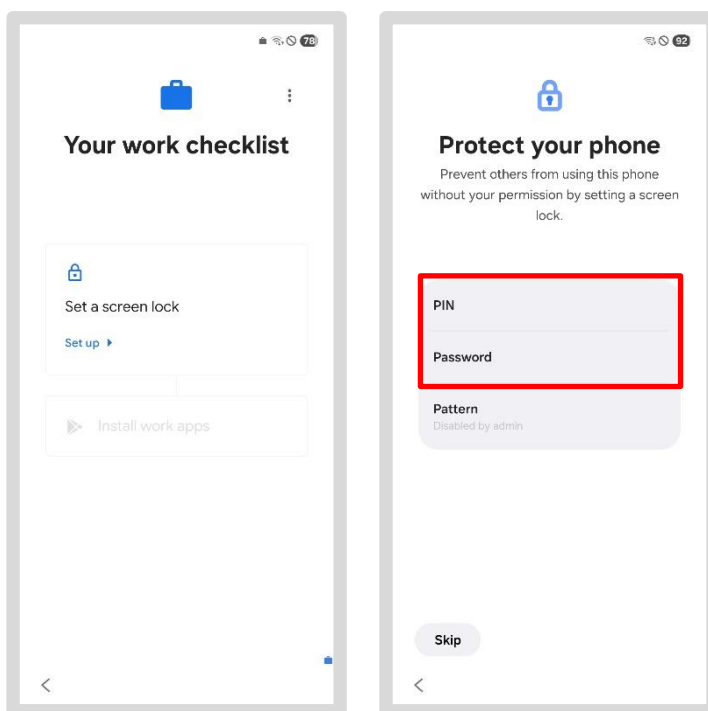


- Aktualizacja urządzenia może chwilę potrwać, a w niektórych przypadkach nawet bardzo długo, więc prosimy o cierpliwość!
- Trwa instalacja niezbędnych aplikacji
- Może pojawić się prośba o podanie konta prywatnego
  - > W takim przypadku przejdź do sekcji 4.4 Konto Google – nie jest konieczne
- Jeśli ten komunikat się nie pojawi, postępuj zgodnie z instrukcjami jak zwykle.
  - > Przejdź do sekcji 4.2 Ustaw blokadę ekranu

## 4.2 Ustaw blokadę ekranu

Kolejnym krokiem jest skonfigurowanie blokady ekranu dla urządzenia. Jest to wymagane przez DB ze względów ochrony danych i zapewnia niezawodną ochronę danych.

- Naciśnij „Skonfiguruj”
- Wybierz opcję, która najbardziej Ci odpowiada
- Wybierz jedną z dwóch opcji (PIN lub hasło), a następnie ustaw własną blokadę ekranu
- Upewnij się, że nowe hasło lub kombinacja cyfr składa się z sześciu cyfr
- Gdy pojawi się komunikat „Skonfiguruj dane biometryczne”, dotknij „Pomiń”

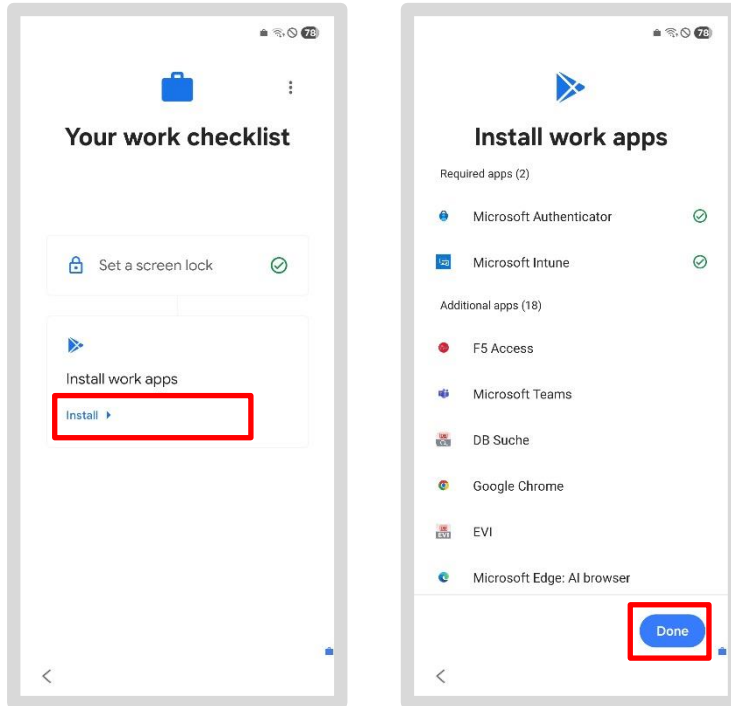


- Zwróć uwagę na informacje dotyczące prywatności i użytkowania zawarte w instrukcjach dotyczących wstępnej konfiguracji
- Potwierdź, wybierając „Kontynuuj”, a następnie „OK” po dwukrotnym wprowadzeniu danych
- Jeśli pojawi się ekran „Konta prywatne”, dotknij „Później” po wyświetleniu monitu
- W tym miejscu może pojawić się pytanie dotyczące usług Google
  - > W takim przypadku przejdź do sekcji 4.4 Konto Google – nie jest konieczne.
- Jeśli ten monit się nie pojawi, postępuj zgodnie z instrukcjami jak zwykle.
  - > Przejdź do sekcji 4.3 Instalowanie aplikacji bazodanowych

### 4.3 Instalowanie aplikacji DB

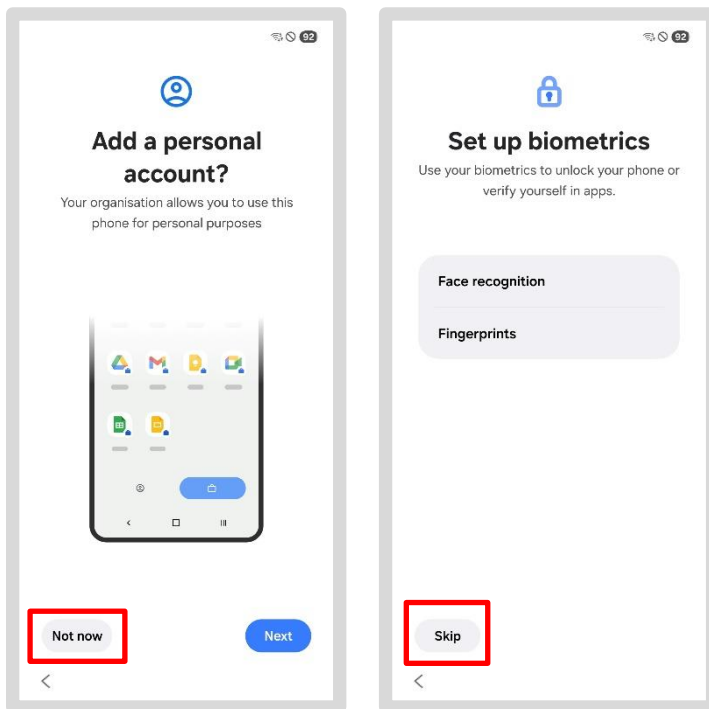
W następnym kroku wszystkie aplikacje DB zostaną ponownie zainstalowane na smartfonie/tablecie DB. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

- Naciśnij „Zainstaluj”
- Przewiń w dół i dotknij „Gotowe”



#### 4.4 Konto Google – nie jest konieczne

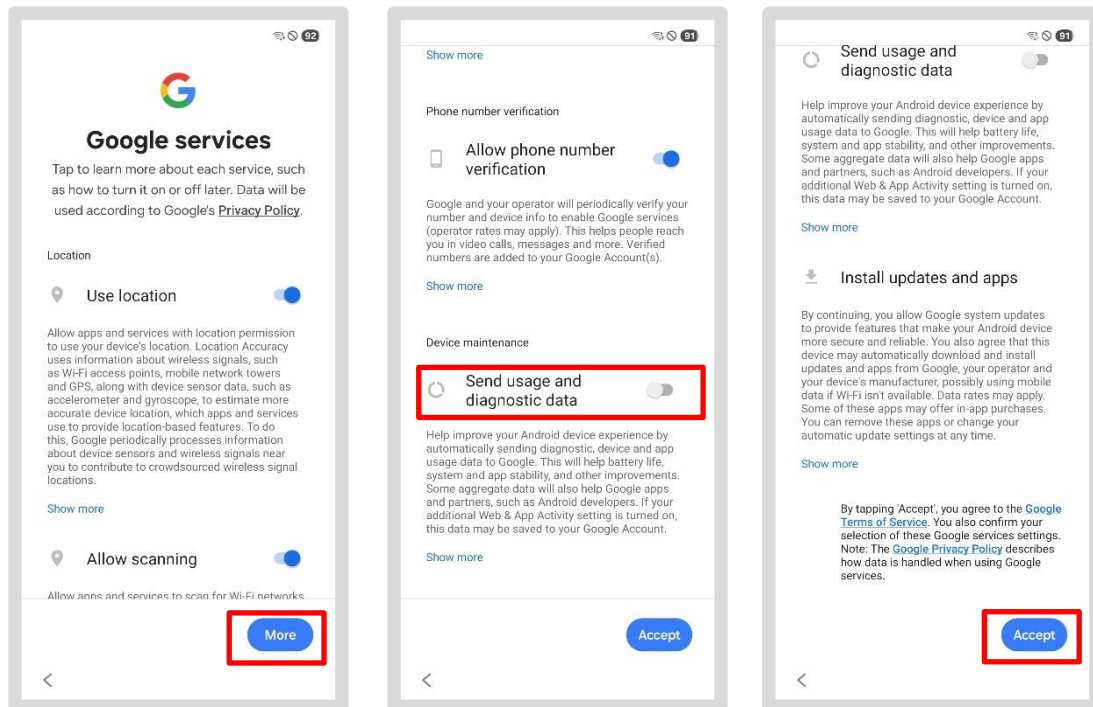
- Na smartfonie/tablecie DB **nie** jest wymagane **prywatne** konto Google!
- W razie potrzeby możesz to zrobić później
- Dlatego dotknij „*Nie teraz*”
- Gdy pojawi się komunikat „*Skonfiguruj dane biometryczne*”, dotknij „*Pomiń*”



- Konto Google jest potrzebne np. do odbierania prywatnych wiadomości e-mail przez Gmaila. Prywatne konto Google można również utworzyć później

## 4.5 Włącz usługę Google

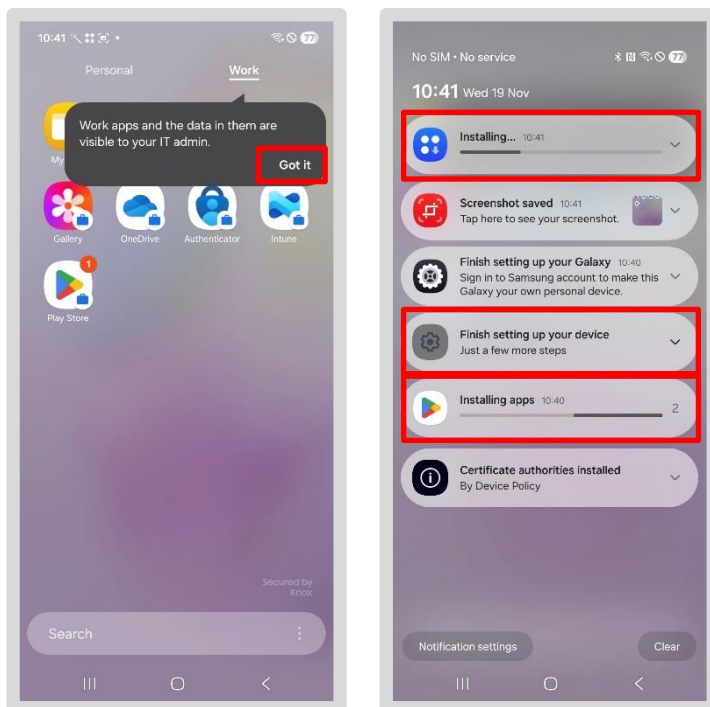
- Naciśnij „Więcej” w sekcji usług Google
- Aby **wysłać dane dotyczące użytkowania i diagnostyki**: dotknij suwaka, aby wyłączyć tę funkcję
- Przewiń dalej, a następnie dotknij „Akceptuj”



> Przejdź do [sekcji 4.6 Automatyczna instalacja aplikacji z DB](#)

## 4.6 Automatyczna instalacja aplikacji bazodanowych

- Pojawią się następujące ekrany... poczekaj, aż pojawi się ekran startowy
- Przesuń palcem od dołu do góry, aby zobaczyć podział na *Osobiste/Służbowe*
- Naciśnij „W porządku”
- Przesuń palcem od góry do dołu. Powiadomienia w tym miejscu pokazują, czy jakieś aplikacje są nadal pobierane lub instalowane
- Dotknij powiadomienia, aby sprawdzić, ile aplikacji pozostało do zainstalowania



- **Uwaga:** opcja „Dokończ konfigurację urządzenia” nie jest konieczna do skonfigurowania smartfona/tabletu z systemem DB. Zignoruj ją!
- Poczekaj chwilę, aż wszystkie aplikacje zostaną zainstalowane
- **Uwaga:** Jeśli urządzenie nie działa zgodnie z opisem lub nie wyświetla ekranów pokazanych w niniejszej instrukcji, zresetuj je ponownie. Aby to zrobić, przejdź do rozdziału 2 Rozpocznij odzyskiwanie: Zresetuj smartfon/tablet

### Ważne!

Twój smartfon/tablet nie jest jeszcze podłączony do sieci DB!

Uzyskaj **tymczasową legitymację pracownika DB** i wprowadź go w aplikacji *Intune*.

Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku zawartymi w > Rozdział 5 Aktywacja urządzenia – Utwórz tymczasową legitymację pra-

## 5 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)

Aby skonfigurować smartfon/tablet w sieci DB, potrzebne będą:

- Ważna tymczasowa legitymacja pracownika DB – [db.de/tap](https://db.de/tap)
- nazwa użytkownika DB i hasło użytkownika DB
- Aplikacja Intune

### Jeśli utworzyłeś już legitymację pracownika DB:

> Przejdź do [rozdziału 6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB](#)

> W przeciwnym razie przejdź do [rozdziału 5.1 Utwórz tymczasową legitymację pracownika DB \(TAP\)](#)

### Dla Twojej informacji:

Konto użytkownika DB to konto przeznaczone dla wszystkich pracowników Grupy DB. Składa się ono z wybranego przez Ciebie hasła oraz automatycznie wygenerowanej nazwy użytkownika.

- Hasło użytkownika DB można zresetować na stronie [db.de/password](https://db.de/password)
- **Instrukcje dotyczące zmiany hasła** można znaleźć w sekcji [Zmiana hasła użytkownika DB](#)
- Informacje o tym, **jak uzyskać dostęp do konta DB User**, można znaleźć w sekcji [Wymagania wstępne: DB User](#)
- **Nazwę użytkownika DB** można znaleźć w DeBi w sekcji [db.de/debi](https://db.de/debi)

Możesz utworzyć tymczasową legitymację pracownika DB poprzez link: [db.de/tap](https://db.de/tap) !

---

### 5.1 Utwórz tymczasową legitymację pracownika DB (TAP)

> **Uwaga:** Instrukcje wideo można znaleźć na stronie [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

Istnieje kilka sposobów utworzenia tymczasowej legitymacji pracownika DB (TAP):

#### Opcja 1:

Masz **drugi smartfon/tablet** lub komputer BKU/Basic Workplace, który jest już zalogowany do sieci DB. W takim przypadku pozostań w bieżącym rozdziale i przejdź do następnej strony.

#### Opcja 2:

**Kolega** z tej samej firmy (np. DB Sales lub DB Long-Distance) może Ci pomóc, jeśli posiada smartfon/tablet DB (lub iPhone/iPad) lub komputer BKU/Basic Workplace. Przejdź do:

> [Rozdział 5.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika](#)

#### Opcja 3 – Tryb ekspercki:

Masz **tylko smartfon/tablet** i udało Ci się użyć go do utworzenia tymczasowej legitymacji pracownika DB przed zresetowaniem urządzenia. Zanotuj swoją legitymację pracownika DB i przejdź do:

> [Rozdział 2 Rozpocznij odzyskiwanie: Zresetuj smartfon/tablet](#)

**Uwaga:** Twój Tap jest ważny tylko przez 60 minut i na wielu smartfonach/tabletach!

### Jeśli nadal masz zainstalowaną aplikację Welcome:

- otwórz „aplikację Welcome” i kliknij „Pomoc”
- Następnie kliknij „Tymczasowa legitymacja pracownika DB”, aby ją utworzyć

### Jeśli nie masz zainstalowanej aplikacji Welcome:

- Wejdź na [stronę db.de/tap](https://db.de/tap) i wprowadź swoją nazwę użytkownika DB oraz hasło użytkownika DB
- Wybierz „Dla siebie” i naciśnij niebieski przycisk
- Teraz wybierz „DB Workplace Mobile”
- Wyświetli się tymczasowa legitymacja pracownika DB
- Jest on **ważny przez 60 minut** i można go używać **na wielu smartfonach/tabletach**.

**Create a Temporary Access Pass (TAP)**

This self-service allows you to create a temporary access pass (TAP) to set up a DB Workplace or Basic Workplace device.

The TAP can be created for:

- yourself
- an employee from the same company (see [EVI](#))

**Register**

Enter your DB user login details

DB User Anmeldenname  
Max Mustermann

DB User Password

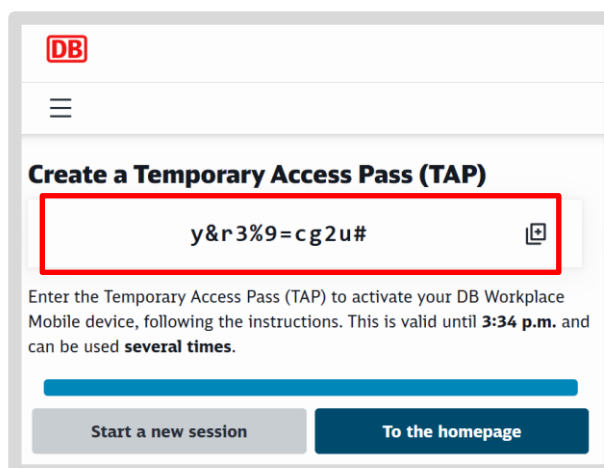
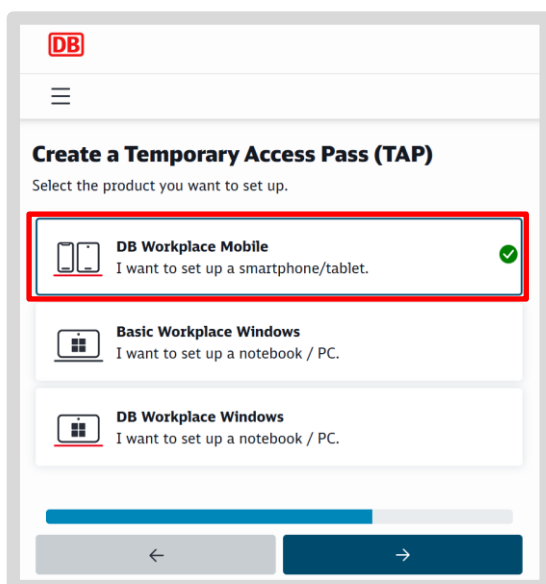
[How can I log in to other environments?](#)

**Create a Temporary Access Pass (TAP) - Person selection**

Choose for whom the TAP should be created:

For myself

For another DB employee



**Ważne!**  
Kod **TAP** można wprowadzić wyłącznie w **aplikacji Intune**, nawet jeśli zostanie on wymagany w innej aplikacji DB lub na innym urządzeniu.

- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku
- Będzie on potrzebny później podczas konfiguracji i aktywacji aplikacji Intune
- Teraz możesz aktywować swój smartfon/tablet w aplikacji Intune

> Przejdź bezpośrednio do rozdziału 6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)

**Ważne!**

Twój smartfon/tablet nie jest jeszcze podłączony do sieci DB!  
Wprowadź **tymczasową legitymację pracownika DB (TAP)** w aplikacji Intune.

> Przejdź teraz do rozdziału 6 Aktywuj urządzenie za pomocą tymczasowej legitymacji pracownika DB

## 5.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika

Aby utworzyć TAP dla współpracownika, postępuj zgodnie z poniższymi instrukcjami:

### Jeśli nadal masz zainstalowaną aplikację powitalną:

- otwórz „aplikację Welcome” i dotknij „Pomoc”
- Następnie kliknij „Tymczasowa legitymacja pracownika DB”, aby ją utworzyć

### Jeśli nie masz zainstalowanej aplikacji Welcome:

- Wejdź na [stronę db.de/tap](https://db.de/tap) i wprowadź swoją nazwę użytkownika DB oraz hasło użytkownika DB
- Wprowadź swoją nazwę użytkownika DB i hasło użytkownika DB
- Wybierz opcję „Dla innego pracownika DB” i naciśnij niebieski przycisk

**Create a Temporary Access Pass (TAP)**

This self-service allows you to create a temporary access pass (TAP) to set up a DB Workplace or Basic Workplace device.

The TAP can be created for:

- yourself
- an employee from the same company (see [EVI](#))

**Register**

Enter your DB user login details

DB User Anmeldenname  
Max Mustermann

DB User Password

[How can I log in to other environments?](#)

**Create a Temporary Access Pass (TAP) - Person selection**

Choose for whom the TAP should be created:

For myself

For another DB employee

Q Max Mustermann

DB User: [blurred]

Name: [blurred]

E-mail: [blurred]

Department: [blurred]

Company: DB Systel GmbH

I confirm that I have established the employee's identity.

- Wybierz właściwą osobę, potwierdź jej tożsamość i naciśnij przycisk
- Podczas pracy zdalnej przez Teams przełącz kontrolę swoim współpracownikom lub
- Pozwól współpracownikowi korzystać z komputera
- Pracownik DB wprowadza hasło użytkownika DB
- Następnie wyświetla się legitymacja pracownika DB. **Jest ona ważna przez 60 minut i na wielu smartfonach/tabletach**
- Odzyskaj kontrolę nad ekranem, jeśli korzystałeś z aplikacji Teams
- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku

**Create a Temporary Access Passport (TAP) for Max Mustermann**

The selected employee must personally enter their DB User access data here.

**Register**

DB User Anmeldename  
Max Mustermann

DB User Password

**Note for DB employees:** Never share your DB user login details with others.

**Create a Temporary Access Pass (TAP)**

y&r3%9=cg2u#

Enter the Temporary Access Pass (TAP) to activate your DB Workplace Mobile device, following the instructions. This is valid until 3:34 p.m. and can be used **several times**.

Start a new session To the homepage

- Będzie on potrzebny później do konfiguracji i aktywacji w aplikacji Intune
- Pracownik może teraz aktywować swój smartfon/tablet w aplikacji Intune

> Przejdź bezpośrednio do rozdziału 6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)

**Ważne!**


Twój smartfon/tablet nie jest jeszcze podłączony do sieci DB!  
Wprowadź **tymczasową legitymację pracownika DB (TAP)** w aplikacji Intune.

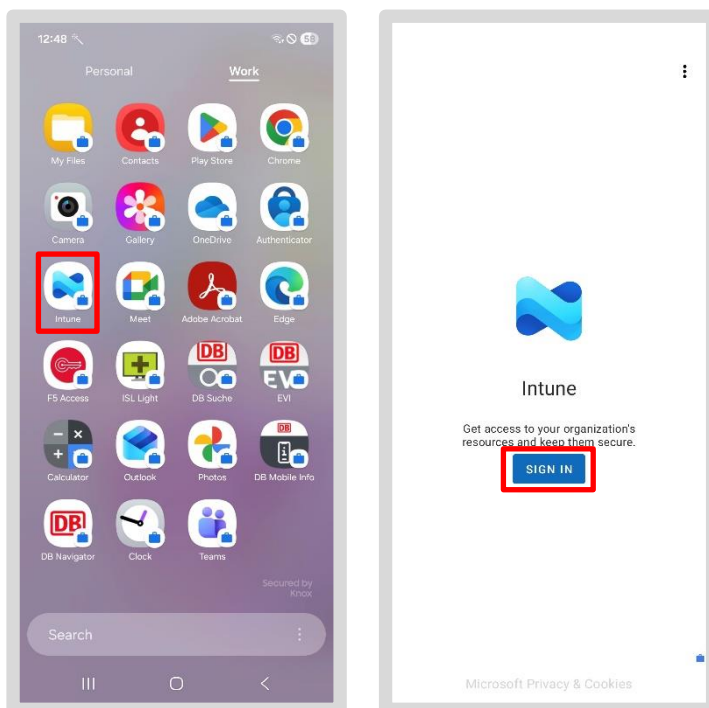
> Przejdź teraz do rozdziału 6 Aktywuj urządzenie za pomocą tymczasowej legitymacji pracownika DB

## 6 Aktywuj urządzenie za pomocą tymczasowej legitymacji pracownika DB (TAP)

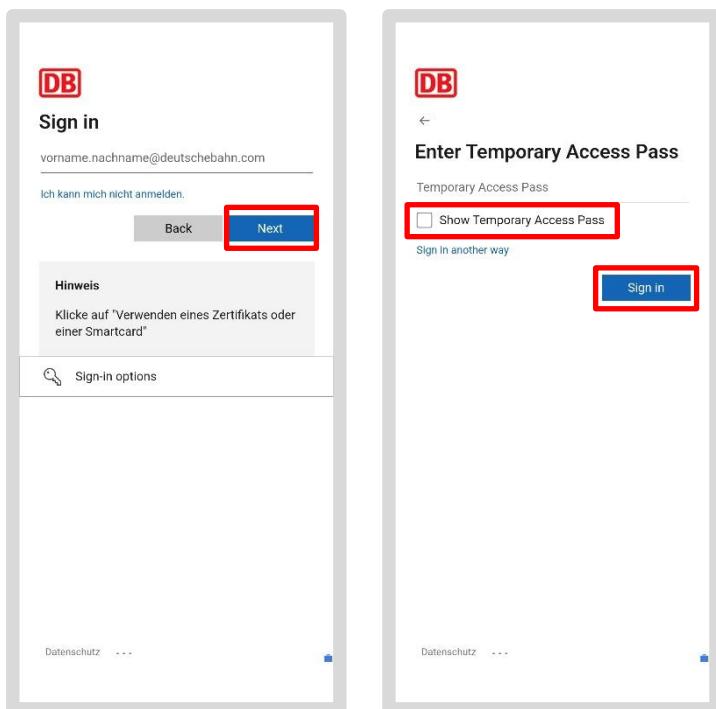
> **Uwaga:** Sprawdź, czy utworzyłeś i otrzymałeś tymczasową legitymację pracownika DB (TAP) zgodnie z opisem w rozdziale 5 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)!

> **Uwaga:** Instrukcje wideo znajdziesz na stronie [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

- Aplikacja Welcome nie jest już wymagana do aktywacji; w tym celu dostępna jest teraz aplikacja Intune
- Przejdź do sekcji „Praca”/„Biznes”
- Otwórz aplikację  „Intune”
- Następnie naciśnij przycisk „Zaloguj się”



- Wprowadź swój **adres e-mail użytkownika DB** (nie: użytkownik DB) i dotknij „Dalej”
- **Wskazówka:** Zaznacz pole obok opcji „Pokaż tymczasową legitymację pracownika DB”
- Wprowadź tymczasową legitymację pracownika DB i dotknij „Zaloguj się”



**Uwaga:** Wprowadź tymczasową legitymację pracownika DB wyłącznie w aplikacji Intune!

### Jeśli pojawi się komunikat o błędzie:

- utwórz nowe tymczasowe hasło dostępu i powtórz proces logowania zgodnie z opisem w rozdziale 5 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)

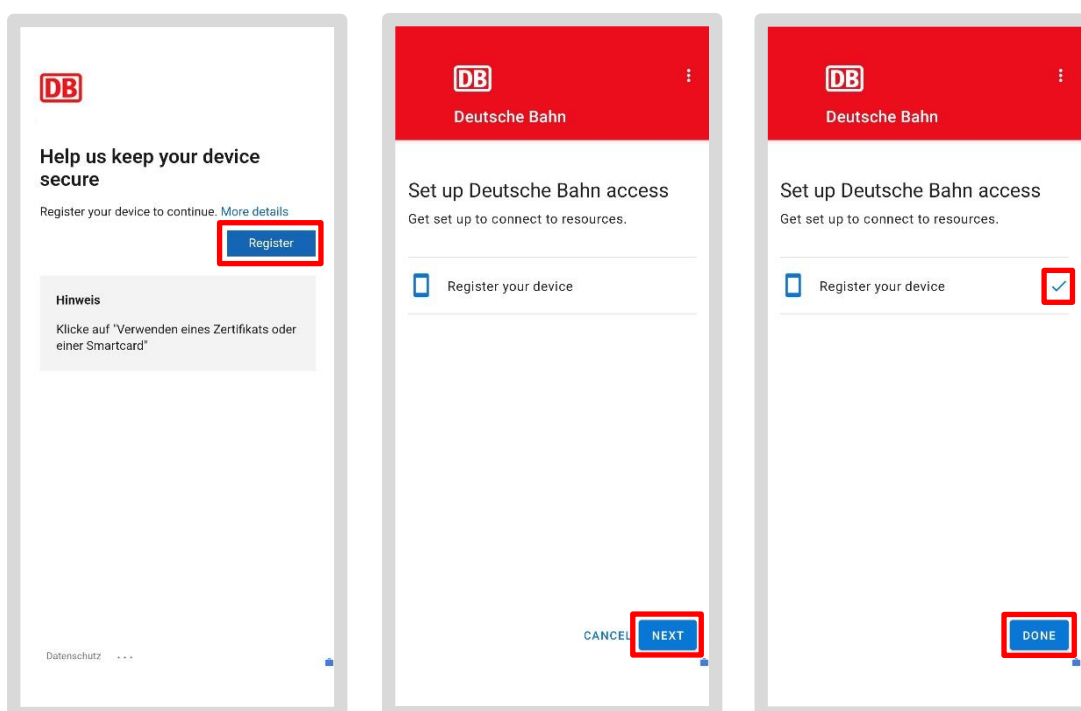
> Przejdź do rozdziału 6.1 Konfigurowanie dostępu do wszystkich aplikacji i stron internetowych DB

**Uwaga:** Jeśli tymczasowa legitymacja pracownika DB (TAP) jest ważna (w ciągu 60 minut) i otworzysz na przykład aplikację Outlook, Teams lub IT ServiceDesk, zostaniesz poproszony o podanie tymczasowej legitymacji pracownika DB. Wpisz tutaj również zapisaną tymczasową legitymację pracownika DB.

## 6.1 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB

Teraz konfigurujemy dostęp do sieci DB:

- Naciśnij „Zarejestruj”, a następnie „Dalej”
- Gdy obok opcji „Zarejestruj urządzenie” pojawi się znacznik wyboru, naciśnij przycisk „Gotowe”
- **Uwaga:** jeśli przycisk „Gotowe” nie pojawi się, aktywacja nie została zakończona
- Otwórz ponownie aplikację Intune i wykonaj krok po kroku czynności opisane w rozdziale 6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)



> **Uwaga: Po rejestracji poczekaj od 5 minut do 24 godzin!**

Wszystkie informacje i certyfikaty zostaną wówczas przeniesione na smartfon/tablet i będzie można korzystać z aplikacji, takich jak Outlook, Teams itp.

---

## 6.2 Aplikacje DB

**Uwaga:** Dostarczenie certyfikatów może potrwać **od 5 minut do 24 godzin**. Dopiero wtedy będzie można korzystać z aplikacji, takich jak Outlook, Teams itp.

Po zakończeniu konfiguracji aplikacje DB, takie jak aplikacja Outlook lub aplikacja Teams, zostaną pobrane automatycznie.

Następnie zostaną załadowane aplikacje specyficzne dla Twojej firmy lub działalności.

Dodatkowe aplikacje DB można pobrać ze sklepu Google Play dla pracy (aplikacja z ikoną walizki) w sekcji „Praca”.

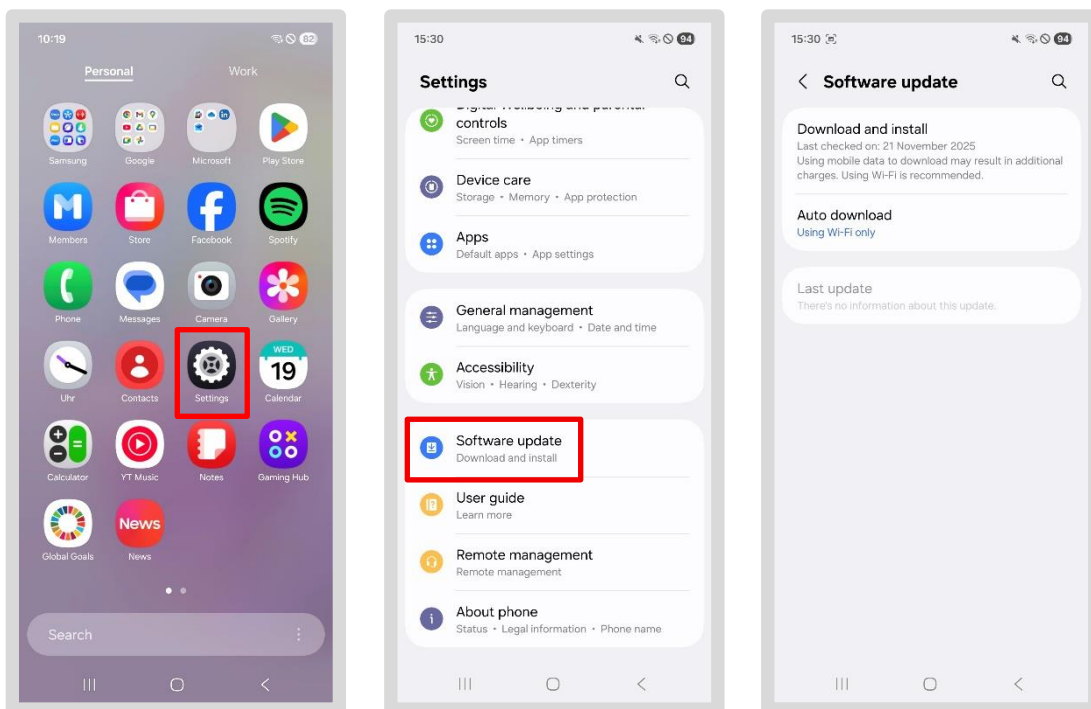
**Aplikacja „Welcome” nie jest już dostępna** na smartfonach i tabletach DB, ale **aplikacja „DB MOBIL”** zawiera wszystkie potrzebne informacje, przydatne linki i dane dotyczące smartfonów i tabletów DB.

## 7 Wymagane ustawienia

**Uwaga:** dostarczenie certyfikatów może potrwać **od 5 minut do 24 godzin**. Dopiero wtedy będzie można korzystać z aplikacji, takich jak Outlook, Teams itp.

### 7.1 Sprawdź dostępność aktualizacji systemu operacyjnego

- Przejdź do sekcji „Osobiste” na smartfonie/tablecie
- Naciśnij aplikację „Ustawienia”
- Naciśnij „Aktualizacja oprogramowania”
- W ten sposób dowiesz się, czy dostępna jest aktualizacja
- Wykonaj wszystkie oczekujące aktualizacje, dotykając opcji „Zainstaluj aktualizację”



## 7.2 Outlook

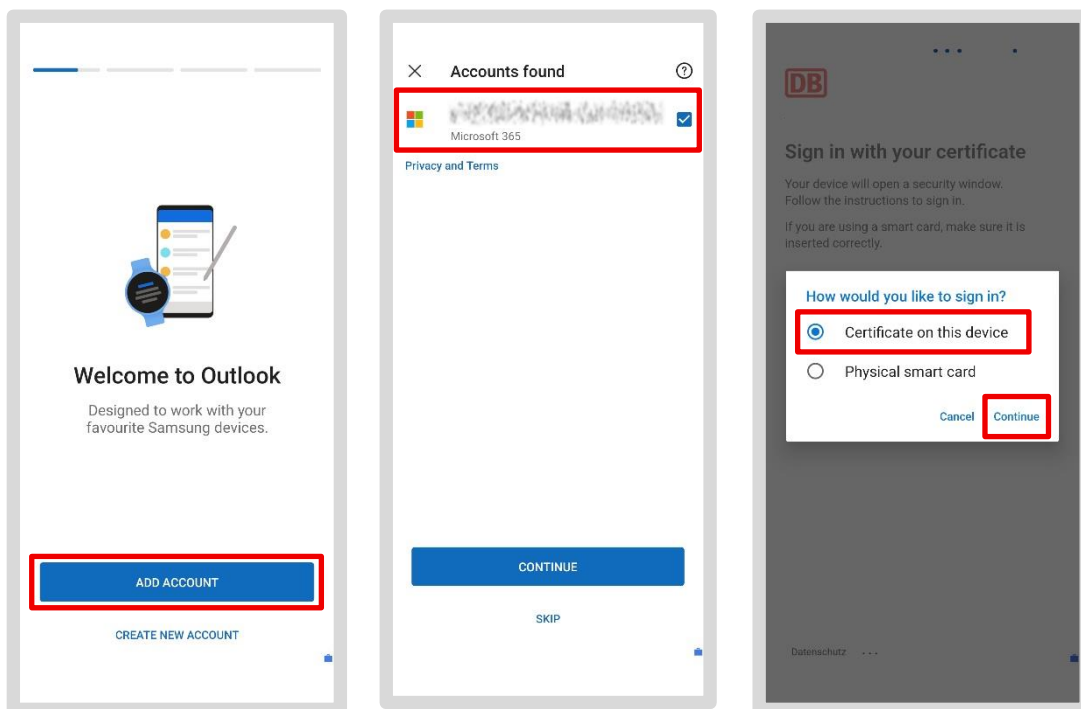
### 7.2.1 Skonfiguruj Outlook /Utwórz konto e-mail/Skonfiguruj szyfrowanie wiadomości e-mail

> **Uwaga:** Film instruktażowy znajdziesz pod adresem [db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung) (tylko w języku niemieckim)

- Przejdź do sekcji „Praca/Biznes” i dotknij aplikacji „Outlook”
- Twoje konto e-mail powinno być już zapisane automatycznie – następnie dotknij „Dodaj konto”
- W następnym kroku wybierz swój adres e-mail i dotknij „Kontynuuj”

Po wyświetleniu monitu o zalogowanie się może pojawić się prośba o podanie tymczasowej legitymacji pracownika DB (TAP):

- Możesz ją utworzyć zgodnie z opisem w [rozdziale 5.1 Tworzenie tymczasowej legitymacji pracownika DB \(TAP\)](#)
- Alternatywnie wybierz opcję „Certyfikat na tym urządzeniu” w sekcji „Wybierz inną opcję logowania”
- Naciśnij „Wybierz”, gdy pojawi się prośba o certyfikat



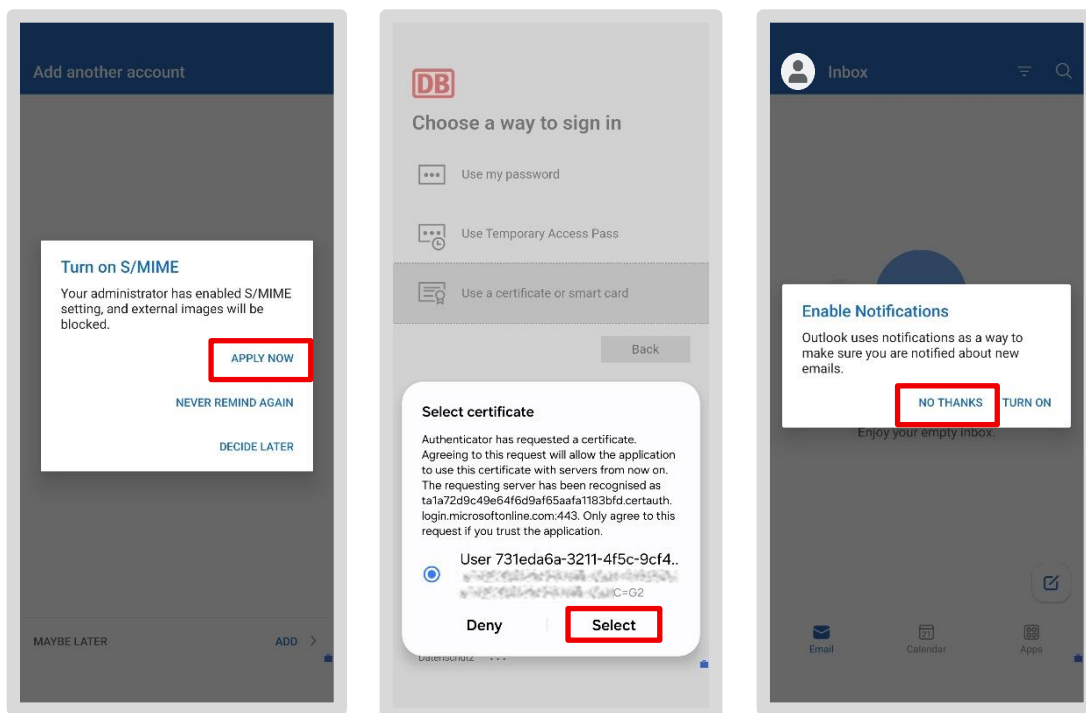
- Jeśli chcesz wysłać szczególnie wrażliwe dane (np. informacje osobowe) pocztą elektroniczną, musisz również zastosować szyfrowanie treści wiadomości e-mail
- DB zapewnia w tym celu szyfrowanie S/MIME
- Naciśnij „Zastosuj teraz”, gdy pojawi się pytanie, czy chcesz aktywować S/MIME

Pojawi się wtedy zapytanie o certyfikat. Certyfikat, który jest dla Ciebie ważny, rozpoznasz w następujący sposób:

- Pierwsza linia: „**User ds2232...** (następnie cyfry i litery)
- Drugi wiersz: „CN- Nazwa **użytkownika DB**”, np. LisaMustermann 89sd7es0ßwd (a następnie cyfry i litery)
- Zaznacz fragment tekstu i kliknij „Wybierz”

Twoje konto e-mail zostanie teraz skonfigurowane:

- Gdy pojawi się pytanie, czy chcesz dodać kolejne konto, wybierz opcję „Może później”
- I włącz opcję „Nie, dziękuję” dla powiadomień



- Twoje wiadomości e-mail zostaną teraz załadowane (może to potrwać kilka minut)
- Możesz ponownie czytać i tworzyć wiadomości e-mail

**Android 16:** Na urządzeniach z systemem Android 16 krok aktywacji S/MIME może zostać pominięty. W takim przypadku musisz zakończyć konfigurację Outlooka i ponownie uruchomić aplikację! Pojawi się wtedy monit o aktywację.



## 7.2.2 Skonfiguruj podpis e-mail

Podpisy e-mailowe są obowiązkowym elementem komunikacji biznesowej. Pojawiają się one na końcu wiadomości e-mail i zgodnie z prawem muszą zawierać określone informacje, takie jak nazwa firmy i oficjalna siedziba firmy zarejestrowanej w DB. Tekst podpisu e-mailowego można znaleźć w centralnej książce telefonicznej DB, znanej jako „EVI”.

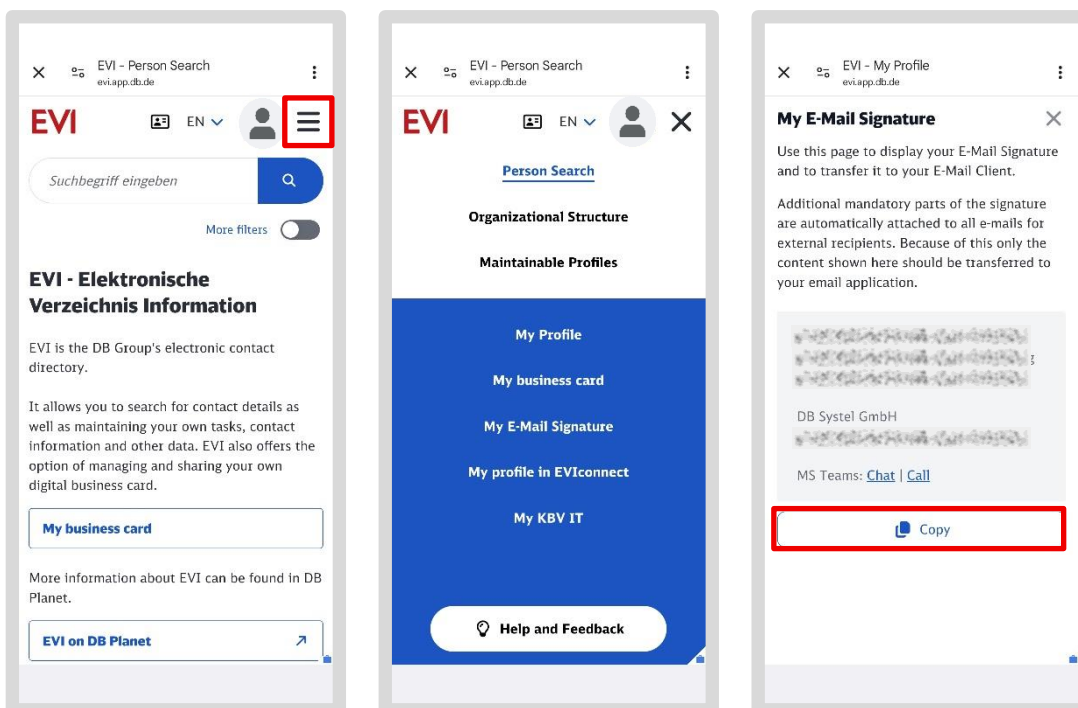
### Jak uzyskać podpis e-mailowy z EVI:




- Otwórz aplikację EVI w obszarze „Praca/Biznes”
- Zobaczysz teraz mobilny widok EVI
- Naciśnij menu w lewym górnym rogu, a następnie „Nowe EVI”

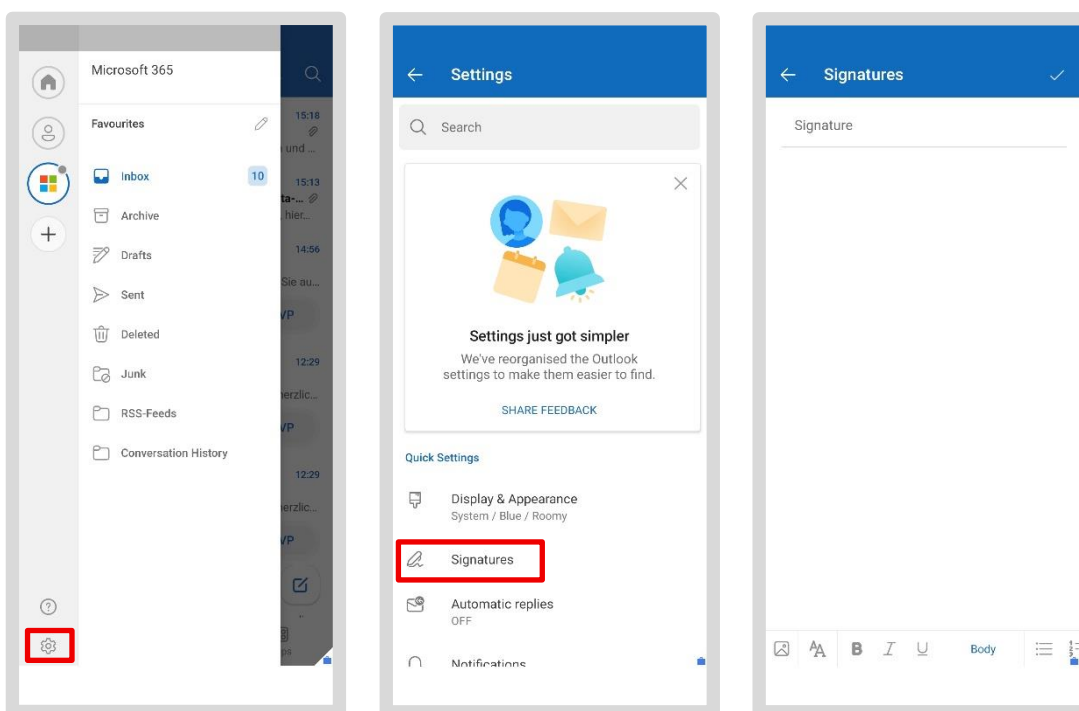
### Otworzy się widok nowego EVI:

- Naciśnij trzy linie obok swojego zdjęcia profilowego w prawym górnym rogu
- Następnie dotknij „Mój podpis e-mailowy”
- Otworzy się strona „Mój podpis e-mailowy”
- Twój osobisty podpis jest wyświetlony w szarym polu. Skopiuj go, dotykając pola „Kopiuj” na dole
- Następnie zamknij EVI



## Wklej podpis do Outlooka:

- Otwórz aplikację Outlook w sekcji „Praca/Biznes”.
- Dotknij swojego zdjęcia profilowego w lewym górnym rogu
- Po lewej stronie otworzy się przegląd folderów poczty e-mail
- Kliknij na koło zębate w lewym dolnym rogu 
- Teraz dotknij „Podpisy”
- Otworzy się pole na podpis. Jeśli jest tam już wpis, usuń go przyciskiem „✕”



- Teraz dotknij i przytrzymaj puste pole, aż pojawi się opcja „Wklej”, a następnie ją wybierz
- Twoja skopiowana sygnatura z EVI zostanie wstawiona.
- Zamknij okno – Twój podpis będzie teraz automatycznie wstawiany do wszystkich pisanych przez Ciebie wiadomości e-mail

**Uwaga:** Jeśli skonfigurowałeś wiele kont e-mail, możesz użyć suwaka „Podpis dla każdego konta”, aby ustawić oddzielny podpis dla każdego konta. W przeciwnym razie zapisany podpis będzie używany dla wszystkich Twoich kont e-mail.

### 7.2.3 Synchronizacja wiadomości e-mail – wszystkie wiadomości zawsze aktualne

Wszystkie Twoje wiadomości e-mail są automatycznie archiwizowane w aplikacji Outlook i synchronizowane z podłączonym kontem Office. Oznacza to, że bez względu na to, z jakiego urządzenia się logujesz, czy to smartfon/tablet, czy komputer BKU/Basic Workplace, zawsze jesteś na bieżąco.

## 7.3 Aplikacja MS Defender

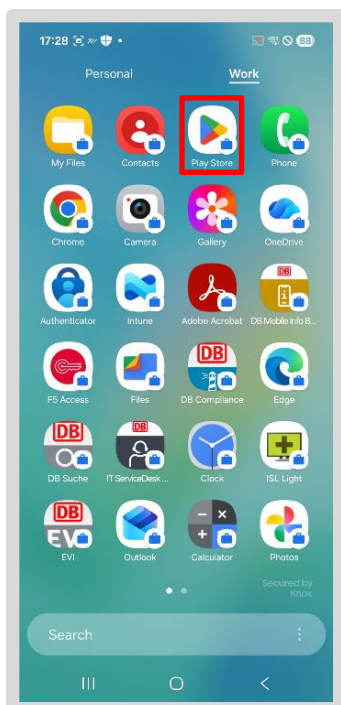
Po aktywowaniu aplikacji Outlook i Teams należy aktywować aplikację „Microsoft Defender for Endpoint Mobile” (w skrócie aplikacja MS Defender) na smartfonie/tablecie. Aplikacja chroni przed cyberatakami i skanuje istniejące aplikacje w poszukiwaniu złośliwego oprogramowania. Aby aktywować ochronę, należy raz otworzyć aplikację.

Ze względu na dużą liczbę różnych smartfonów/tabletów DB mogą wystąpić niewielkie różnice w opisie poszczególnych kroków.

### 7.3.1 Konfiguracja aplikacji MS Defender

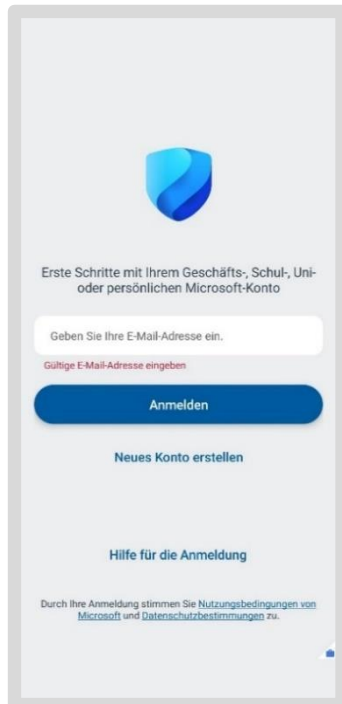
Aby skonfigurować aplikację MS Defender na smartfonie/tablecie, należy wykonać następujące czynności:

- Przejdź do sekcji Praca/Biznes i otwórz „DB Google Play Store”

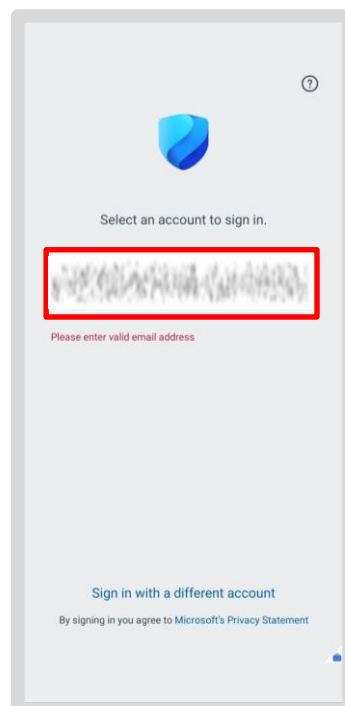
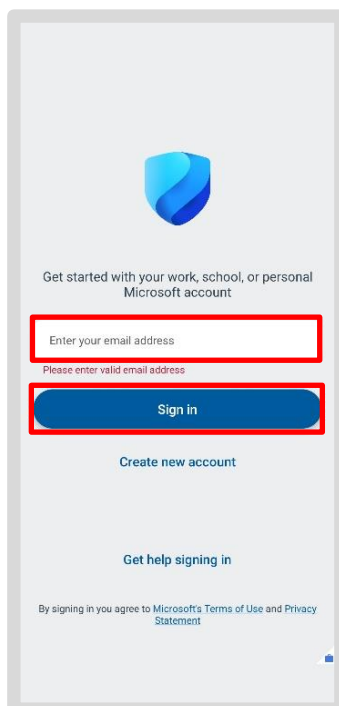


- Wyszukaj aplikację „Microsoft Defender: Antivirus” i kliknij „Zainstaluj”

- Dotknij ikony aplikacji MS Defender, aby ją otworzyć



- Zostaniesz poproszony o podanie służbowego adresu e-mail
- Naciśnij przycisk „Zaloguj się” lub aplikacja automatycznie przeniesie Cię do następnego ekranu, na którym wyświetli się Twój adres e-mail
- Dotknij swojego służbowego adresu e-mail

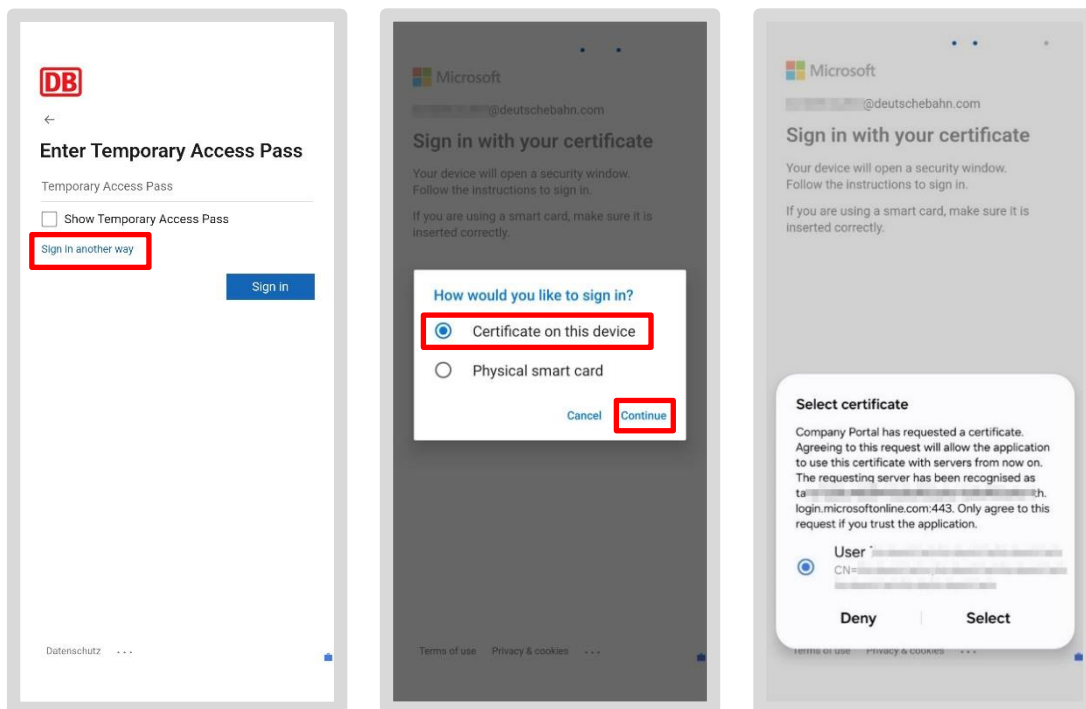


Jeśli w ciągu godziny aktywowałeś smartfon/tablet za pomocą aplikacji Intune, możesz zostać poproszony o ponowne wprowadzenie tymczasowej legitymacji pracownika DB.

- Wybierz opcję „Zaloguj się w inny sposób”

Następnie przejdź dalej:

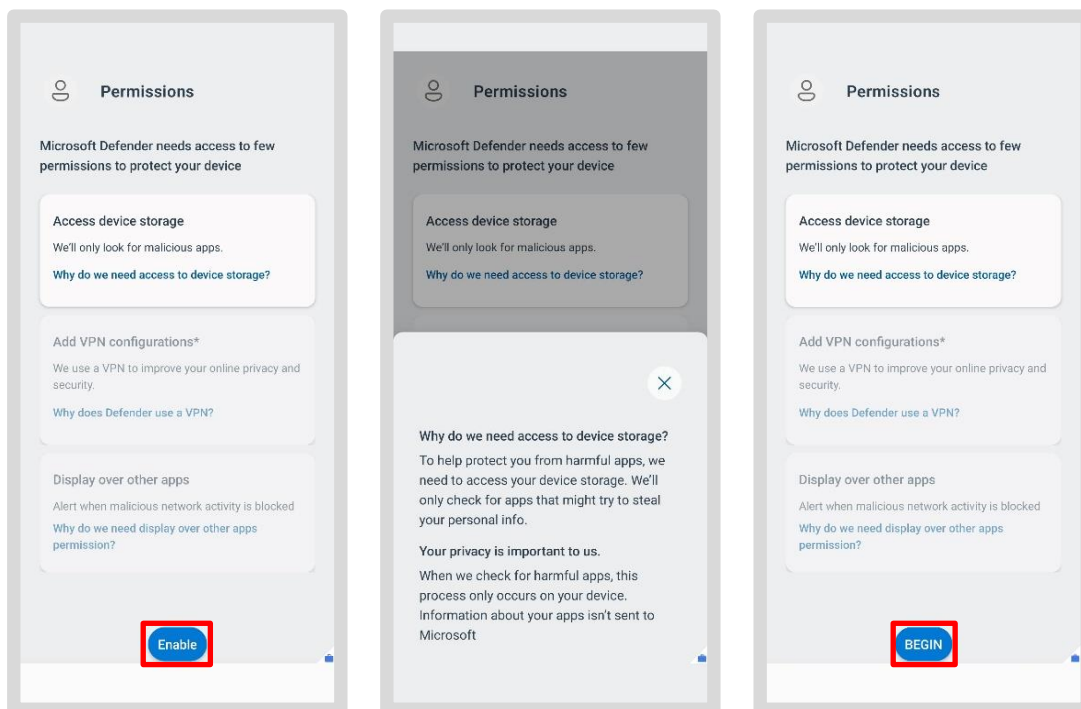
- Po wyświetleniu monitu dotknij opcji „Certyfikat na tym urządzeniu”, a następnie dotknij „Dalej”
- Wybierz certyfikat



### 7.3.2 Przyznaj uprawnienia

Aplikacja poprosi Cię teraz o niezbędne uprawnienia. W tym momencie kolejność ekranów może różnić się od podanej w instrukcji. Jeśli pierwszy ekran wygląda tak jak na obrazku:

- Naciśnij „Włącz”
- Następnie dotknij „Rozpocznij”
- Otworzy się aplikacja „Ustawienia” na Twoim smartfonie/tablecie

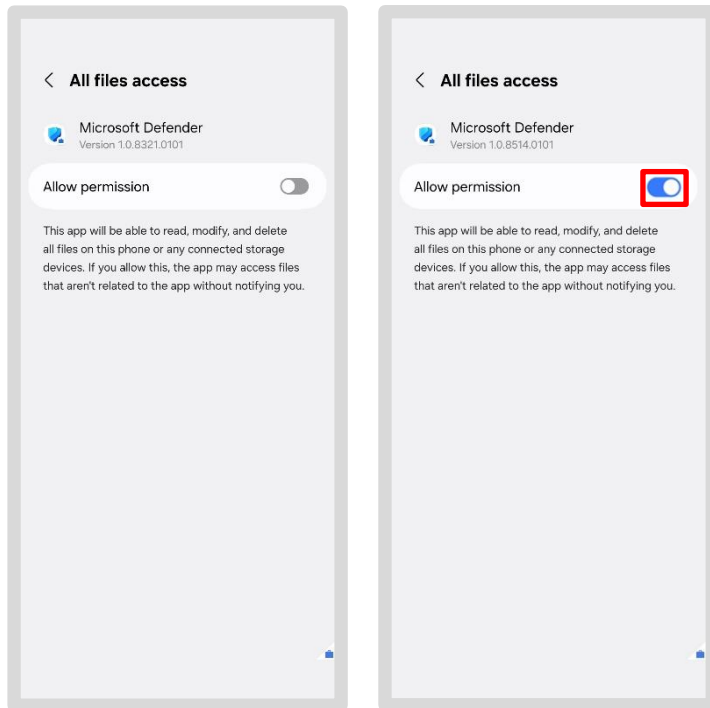


#### Informacje ogólne dotyczące uprawnień:

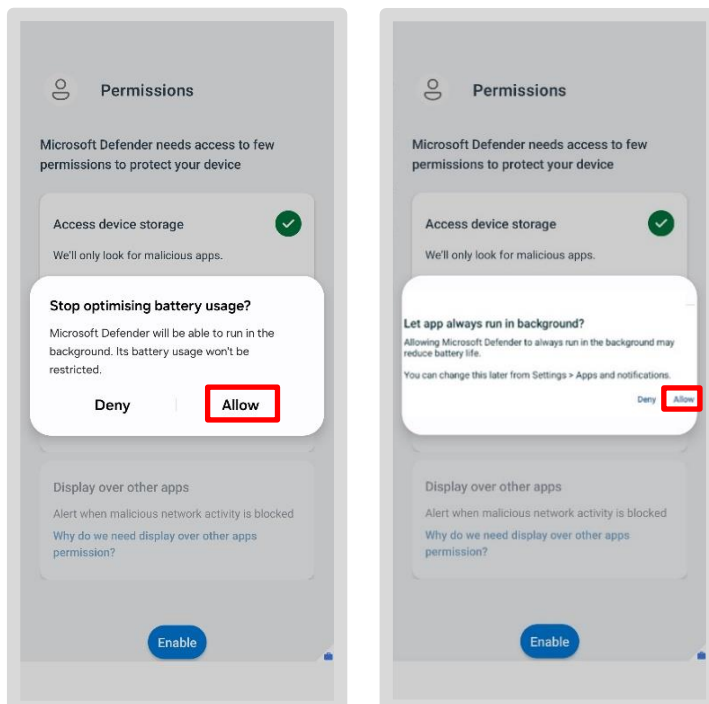
Uprawnienia te są wymagane do prawidłowego działania aplikacji i zapewnienia bezpieczeństwa urządzenia.

Możesz wyświetlić okno informacyjne dla każdego z uprawnień (np. klikając „Dlaczego potrzebujemy dostępu do pamięci urządzenia?”). Niektóre elementy nie mogą jednak zostać wybrane (są wyszarzone, np. „Dodaj konfigurację VPN”) lub są już aktywne (zielony haczyk, np. „Uruchom w tle”), ponieważ są one predefiniowane przez system.

- Przesuń suwak w prawo, aby udzielić uprawnienia
- W następnym oknie dialogowym naciśnij „Zezwól”



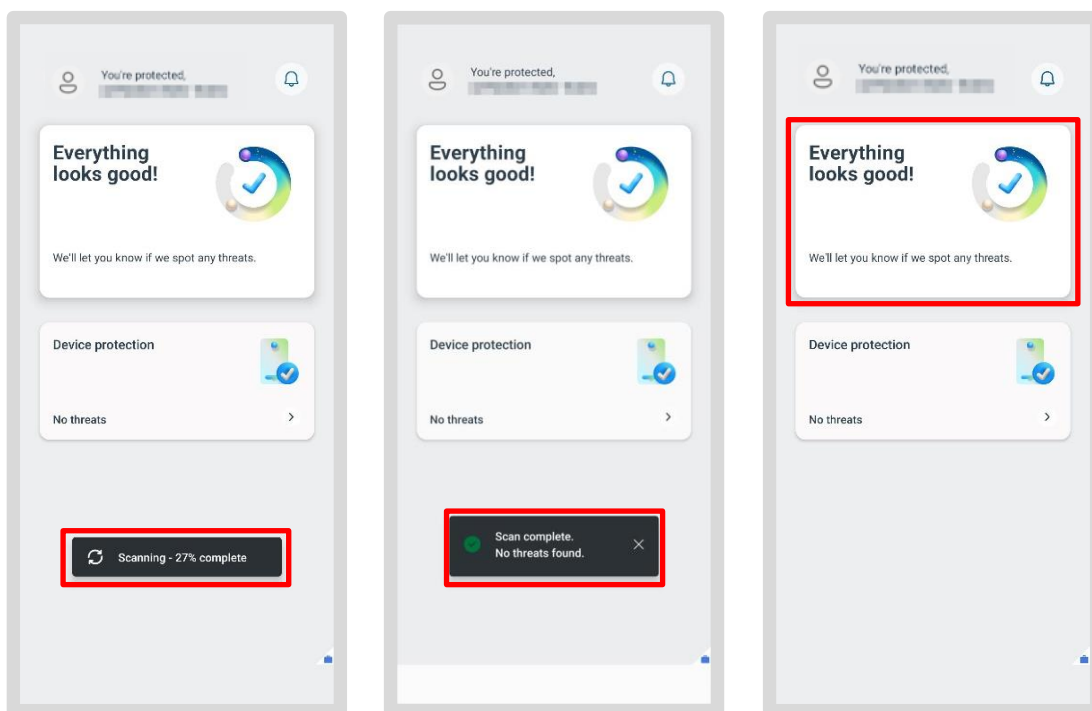
- Naciśnij „Zezwól” dla wszystkich kolejnych zapytań



**Uwaga:** W zależności od typu urządzenia wymagane są różne uprawnienia! Może to spowodować, że widoczne będzie tylko jedno z zapytań.

Następnie zostaniesz przeniesiony na stronę główną aplikacji MS Defender. Skanowanie smartfona/tabletu w poszukiwaniu złośliwego oprogramowania rozpocznie się automatycznie. Podczas skanowania wyświetlane są etapy pośrednie.

Wynik zostanie wyświetlony na stronie głównej. Jeśli widoczny jest zielony haczyk, oznacza to, że nie wykryto złośliwego oprogramowania.



## Gratulacje!

Pomyślnie zakończyłeś pierwszą konfigurację! Urządzenie jest teraz chronione przed złośliwym oprogramowaniem.

## 7.4 DB M 365

Na smartfonie/tablecie możesz również otwierać i przeglądać pliki Word, Excel, PowerPoint lub PDF. W tym celu pobierz odpowiednie aplikacje:

- Otwarcie sklepu DB Google Play
- Wyszukaj odpowiednią aplikację za pomocą paska wyszukiwania, na przykład Word, Excel, PowerPoint lub PDF Reader

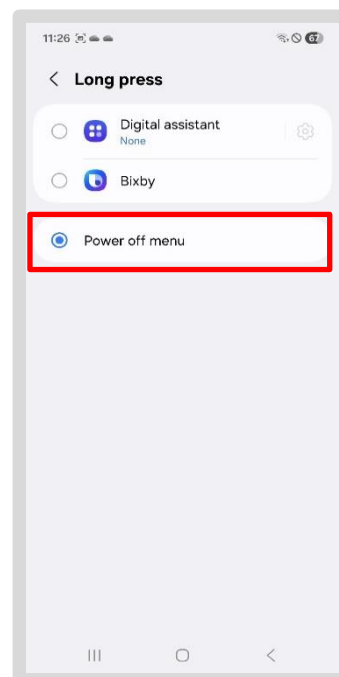
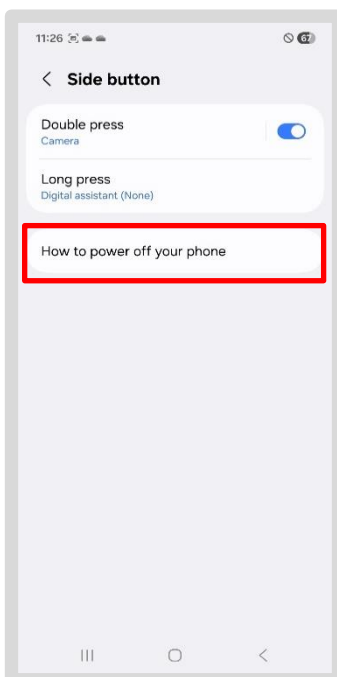
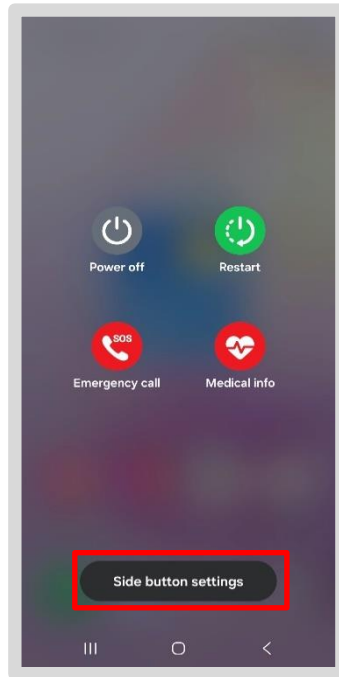


- Następnie kliknij „Zainstaluj”
- Po otwarciu pliku aplikacja uruchomi się automatycznie

**Uwaga:** Można otworzyć tylko jeden plik na raz. Nie ma możliwości otwarcia np. kilku plików Word jednocześnie.

## 7.5 Wyłącz przycisk Bixby

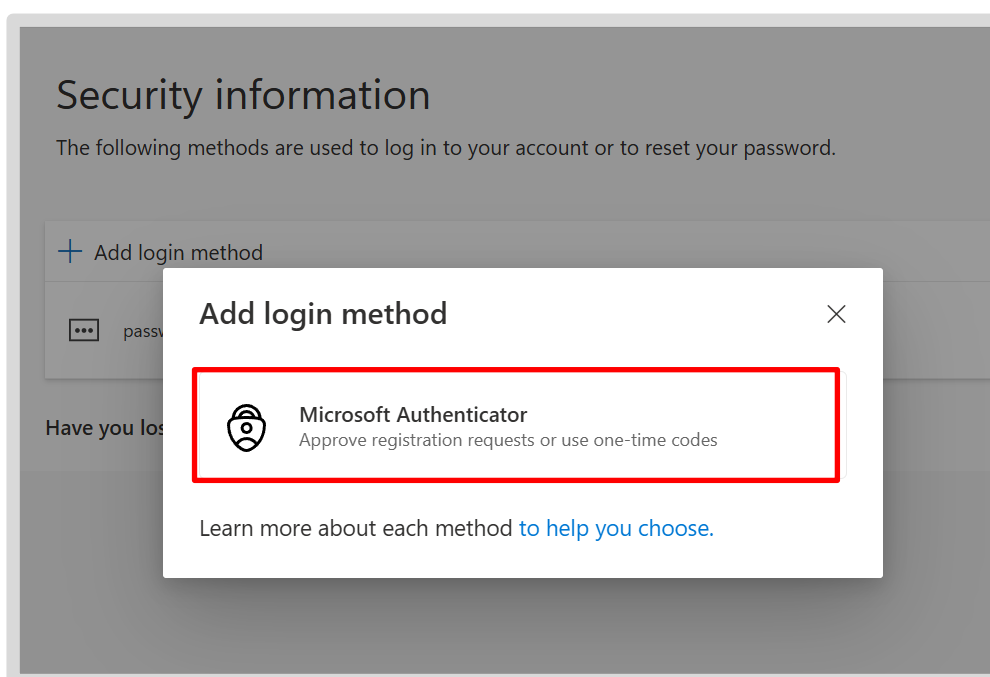
- Domyślnie przycisk zasilania uruchamia asystenta głosowego Bixby. Ze względów bezpieczeństwa należy to wyłączyć:
- Przesuń palcem w dół od góry ekranu
- Dotknij ikony zasilania w prawym górnym rogu, obok ikony ustawień
- Wybierz „Ustawienia klawiszy funkcyjnych”
- Zmień funkcję „Długie naciśnięcie” na „Menu wyłączenia”



## 7.6 Ponownie aktywuj aplikację Microsoft Authenticator do uwierzytelniania

Jeśli korzystałeś z aplikacji do uwierzytelniania, wykonaj następujące czynności:

- Kliknij na [db.de/authenticator](https://db.de/authenticator) na komputerze BKU lub Basic Workplace
- Kliknij ikonę „Plus” i przycisk „Dodaj metodę logowania”
- Otworzy się okno dialogowe; wybierz „Microsoft Authenticator”



- Przejdź na smartfon/tablet i otwórz aplikację Microsoft Authenticator do uwierzytelniania
- Otwórz tę stronę, aby uzyskać [instrukcje krok po kroku](#), kliknij przycisk „Instrukcje dotyczące konfiguracji MFA” i postępuj zgodnie z instrukcjami
- Następnie możesz używać aplikacji Microsoft Authenticator do uwierzytelniania na swoim smartfonie/tablecie
- Jeśli korzystałeś z **aplikacji Authenticator do uwierzytelniania na stronach internetowych lub w narzędziach**, reaktywuj aplikację na tych stronach

**Wskazówka:** Jeśli po migracji masz trudności z ponownym aktywowaniem połączeń w aplikacji Authenticator w procesie uwierzytelniania, skorzystaj z opcji samoobsługi: „Zresetuj aplikację Microsoft Authenticator (MFA)”: [db.de/resetmfa](https://db.de/resetmfa), a następnie postępuj zgodnie z instrukcjami.

## Gratulacje!

Pomyślnie przeprowadziłeś renowację swojego służbowego smartfona/tabletu!

Więcej informacji na temat smartfona/tabletu znajdziesz w aplikacji: DB MOBIL Info.

> Informacje o tym, jak zapisać kontakty w OneDrive i zaimportować je ponownie, znajdziesz w instrukcji konfiguracji w sekcji [Tworzenie kopii zapasowej kontaktów w OneDrive](#)

> Szczegółowe instrukcje konfiguracji znajdziesz na stronie [db.de/mobile-setup](https://db.de/mobile-setup)