

**Przejdźcie na DB Workplace Mobile
Przejdźcie na Intune**

**Smartfon/tablet Samsung
(system operacyjny Android 15 i nowsze)
15 kwietnia 2026 r.**

Spis treści

1 Przegląd procesu migracji	4
2 Konieczne kroki przed migracją	5
2.1 Umów się na termin migracji	5
2.2 Utwórz kopię zapasową danych	5
2.3 Aplikacja do uwierzytelniania – opcjonalnie	5
2.4 Tworzenie tymczasowej legitymacji pracownika DB (TAP) – tryb ekspercki	6
3 Rozpocznij migrację: zresetuj smartfon/tablet	7
3.1 Samodzielne zresetowanie smartfona/tabletu	7
3.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk	8
4 Ponowna konfiguracja	9
4.1 Wybór języka	9
4.2 Zaakceptuj umowę licencyjną użytkownika końcowego	10
4.3 Skonfiguruj Wi-Fi	11
4.4 Konfiguracja Wi-Fi w budynkach DB	12
5 Instalacja Samsung	13
5.1 Skonfiguruj profil służbowy	14
5.2 Ustawianie blokady ekranu	15
5.3 Instalacja aplikacji DB	16
5.4 Konto Google – nie jest konieczne	17
5.5 Aktywacja usług Google	18
5.6 Automatyczna instalacja aplikacji bazodanowych	19
6 Utwórz tymczasową legitymację pracownika DB (TAP)	20
6.1 Utwórz tymczasową legitymację pracownika DB (TAP)	20
6.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika	23
7 Aktywacja urządzenia w DB	25
7.1 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB	27
7.2 Aplikacje DB	28
8 Wymagane ustawienia	29
8.1 Sprawdź dostępność aktualizacji systemu operacyjnego	29
8.2 Outlook	30
8.2.1 Konfiguracja programu Outlook / Utworzenie konta e-mail / Konfiguracja szyfrowania wiadomości e-mail	30
8.2.2 Konfiguracja podpisu e-mail	33

8.2.3 Synchronizacja poczty – wszystkie wiadomości zawsze aktualne	35
8.3 Aplikacja MS Defender	35
8.3.1 Konfiguracja aplikacji MS Defender	35
8.3.2 Przyznaj uprawnienia	38
8.4 DB M 365	41
8.5 Wyłącz przycisk Bixby	42
8.6 Ponowna aktywacja aplikacji do uwierzytelniania Microsoft Authenticator	43
Gratulacje!	43

1 Proces migracji w skrócie

Cały proces migracji do DB MOBIL podsumowano tutaj:



Planowanie migracji

- **Gdy tylko otrzymasz wiadomość e-mail: Umów się na spotkanie w narzędziu PME**
> zobacz rozdział 2.1 Rezerwacja terminu migracji



Techniczne przygotowanie do migracji

- **E-mail z przypomnieniem** na krótko przed terminem, że można rozpocząć migrację



Osobiste przygotowania do migracji

- **Utwórz kopię zapasową danych**
> zobacz sekcję 2.2 Tworzenie kopii zapasowej danych
- *Jeśli korzystasz z aplikacji do uwierzytelniania*
> patrz rozdział 2.3 Aplikacja Authenticator – opcjonalnie
- **Zaktualizuj system** – sprawdź to w ustawieniach systemowych



Migracja do DB Workplace Mobile

- **Zresetuj** smartfon/tablet
> patrz rozdział 3 Rozpocznij migrację: zresetuj smartfon/tablet
- **Utwórz i zapisz** tymczasową legitymację pracownika DB (TAP)
> zobacz rozdział 6 Utwórz tymczasową legitymację pracownika DB (TAP)
- **Aktywuj** smartfon/tablet w Microsoft Intune
> zobacz rozdział 7 Aktywuj urządzenie w bazie danych

Ważne!

Twój smartfon/tablet jest połączony wyłącznie z Sieć DB po
tymczasowa legitymacja pracownika DB (TAP)
w aplikacji Intune.
Outlook ani Teams nie są odpowiednimi aplikacjami do tego celu!

Postępuj zgodnie z poniższą instrukcją krok po kroku!

2 Kroki niezbędne przed migracją

2.1 Umów się na termin migracji

- **Zarezerwuj termin migracji w narzędziu PME db.de/pme, jak tylko otrzymasz e-mail z prośbą o to:**
 - Jeśli nie możesz tego zrobić samodzielnie, poproś przełożonego miejsca powstawania kosztów lub upoważnionego nabywcę o rezerwację w Twoim imieniu. Terminy można rezerwować od poniedziałku do piątku na następny tydzień (poniedziałek–piątek) do godziny 12:00.
- **Jeśli nie możesz dotrzymać terminu migracji:** Możesz anulować termin do godziny 12:00 poprzedniego dnia (poniedziałek–piątek)!
 - **Od zarezerwowanej daty migracji masz 28 dni** na migrację swojego smartfona/tabletu. Ostatni możliwy dzień jest wyświetlany w PME. Po tym terminie Twoje urządzenie zostanie automatycznie usunięte i przeniesione do DB MOBIL za pomocą Microsoft Intune.

2.2 Utwórz kopię zapasową danych

- > **Uwaga:** Instrukcje wideo znajdziesz na [stronie db.de/mobile-videoanleitung](https://db.de/mobile-videoanleitung)
- **Zrób kopię zapasową danych**, jak 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 prywatnych 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](#)

2.3 Aplikacja Authenticator – opcjonalnie

Uwaga: Niniejsza informacja dotyczy wyłącznie użytkowników, którzy aktywnie korzystają z aplikacji Authenticator, np. w celu uzyskania dostępu administracyjnego za pomocą tzw. konta dwuetapowego 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 migracji
- Nie są wymagane żadne dalsze kroki
- Po migracji aplikację należy ponownie aktywować. Jest to opisane w [rozdziale 8.5 Ponowna aktywacja aplikacji Microsoft Authenticator dla uwierzytelniania](#)
- Jeśli podczas migracji konieczne będzie użycie aplikacji Authenticator, należy połączyć się z nią za pomocą innego smartfona lub tabletu. W tym celu należy

postępować zgodnie z instrukcjami krok po kroku dotyczącymi konfiguracji uwierzytelniania wieloskładnikowego (MFA)

2.4 Tworzenie tymczasowej legitymacji pracownika DB (TAP) – tryb ekspercki

Jeśli posiadasz wyłącznie smartfon/tablet DB i możesz zresetować urządzenie samodzielnie, utwórz tymczasową legitymację pracownika DB (TAP) przed resetowaniem.

> Aby to zrobić, przejdź do rozdziału 6.1 Tworzenie tymczasowej legitymacji pracownika DB (TAP)

- Następnie zresetuj urządzenie

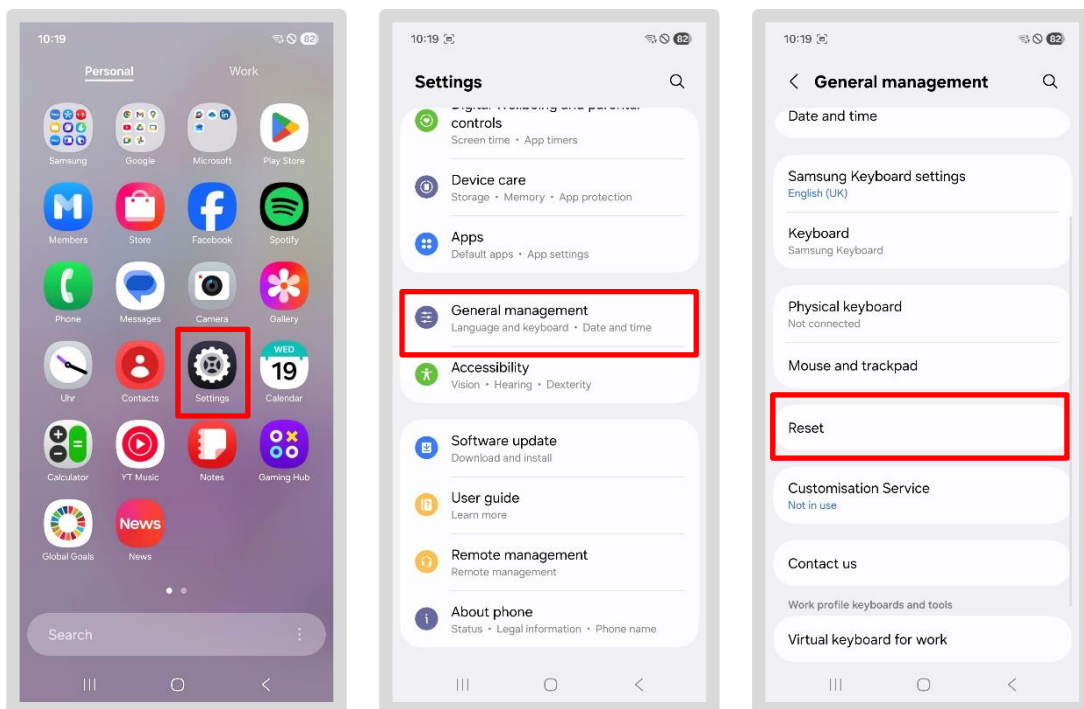
3 Rozpocznij migrację: Zresetuj smartfon/tablet

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

3.1 Samodzielne resetowanie smartfona/tabletu

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

- Przejdź do sekcji „Osobiste” na smartfonie/tablecie
- Kliknij 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 dotknij przycisku „Resetuj”, wprowadź hasło blokady ekranu, a następnie dotknij „Usuń wszystko”
- Poczekaj kilka minut, a urządzenie zostanie automatycznie zresetowane

> Następnie przejdź do [rozdziału 4](#) i skonfiguruj urządzenie ponownie

3.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk

Jeśli smartfon/tablet przestał działać, wybierz ten krok:

- Otwórz aplikację IT ServiceDesk i złóż 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 0
- Biuro obsługi IT DB Cargo
 - Tel. 91 7777 (wewnętrzny)
 - Tel. 00800 327 978 35 (zewnętrzny)
 - Wybierz opcję menu 0
- Jeśli pojawią 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.

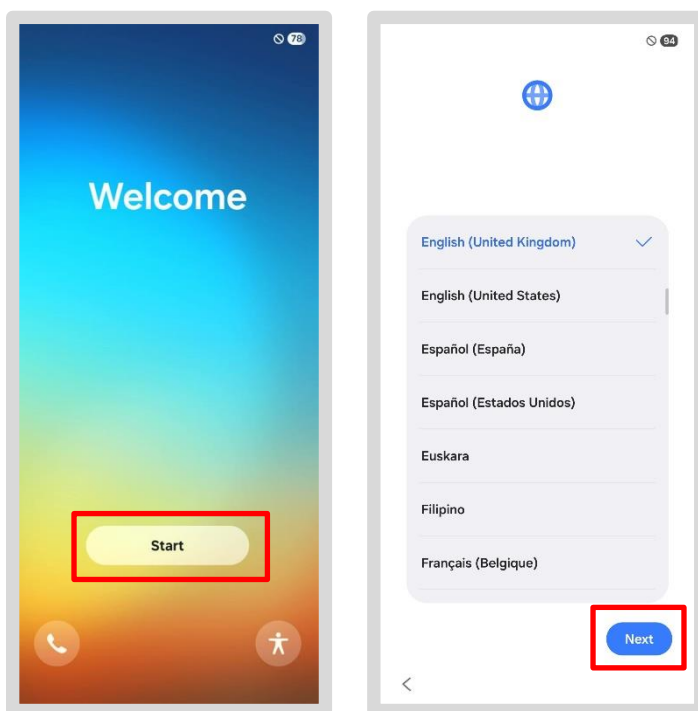
> Następnie przejdź do rozdziału 4 i skonfiguruj ponownie

4 Konfiguracja ponowna

4.1 Wybierz język

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

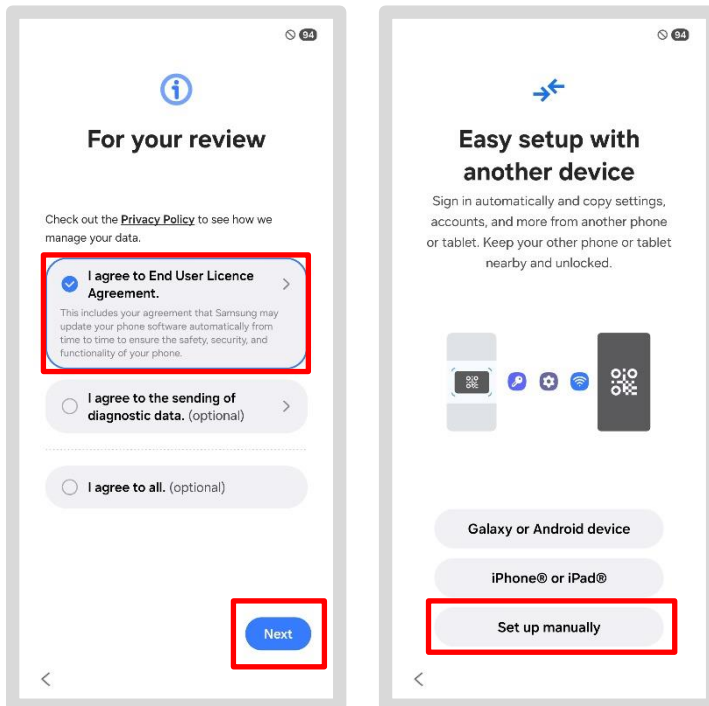
- Trzymaj tablet w **orientacji pionowej**, aby wyświetlać ekrany w takim samym układzie, jak pokazano w instrukcji
- Włącz smartfon/tablet
- Upewnij się, że smartfon/tablet jest podłączony do źródła zasilania lub ma wysoki poziom naładowania baterii podczas procesu renowacji
- Naciśnij „Start”
- Na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



> Przejdź do rozdziału 4.2. Zaakceptuj umowę licencyjną użytkownika końcowego

4.2 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 4.3 Konfiguracja Wi-Fi

4.3 Konfiguracja Wi-Fi

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

- Użyj **danych komórkowych**, jeśli smartfon/tablet ma kartę SIM (może to wiązać się z opłatami!).

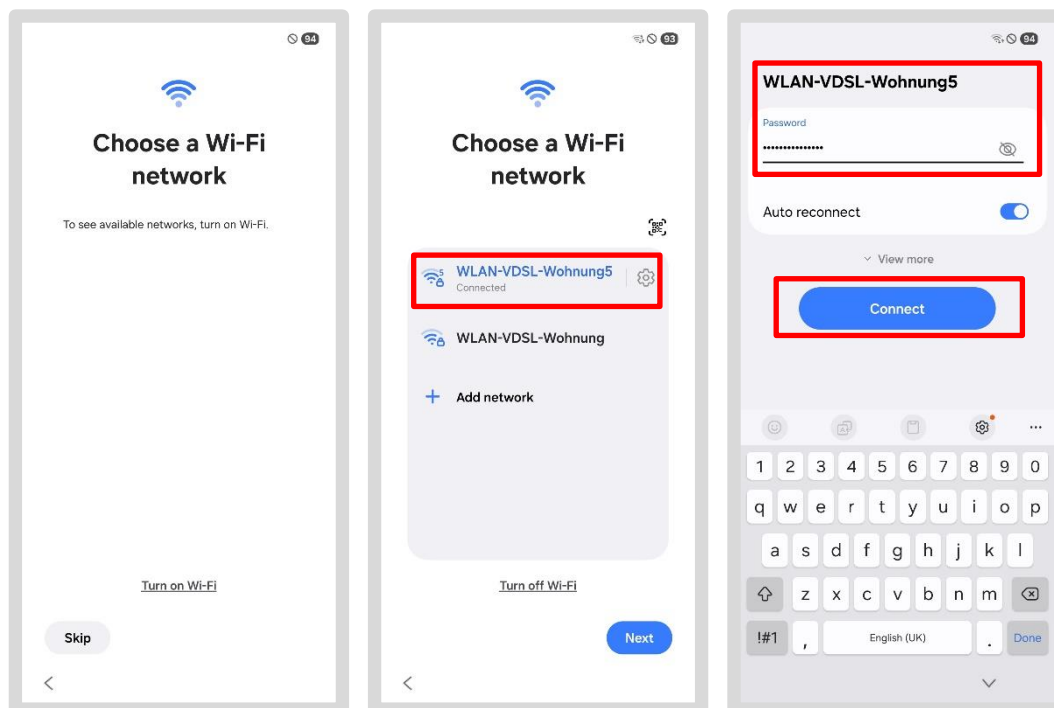
- Skonfiguruj hotspot na swoim prywatnym smartfonie/tablecie

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 ponowne zapytanie, dotknij opcji „Kontynuuj”



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

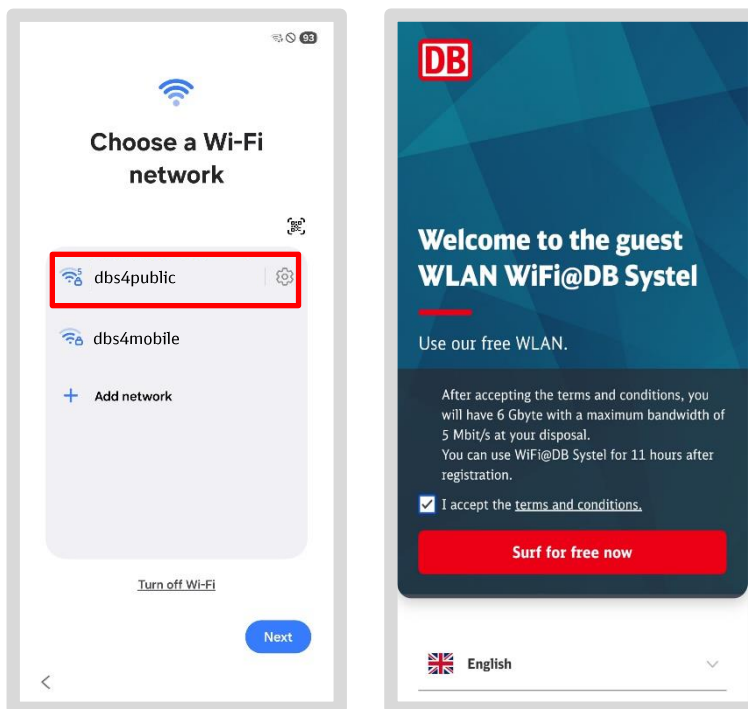
> Przejdź do [rozdziału 5 Instalacja Samsung](#)

4.4 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 [sekcji 4.3 Konfiguracja Wi-Fi](#).

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

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



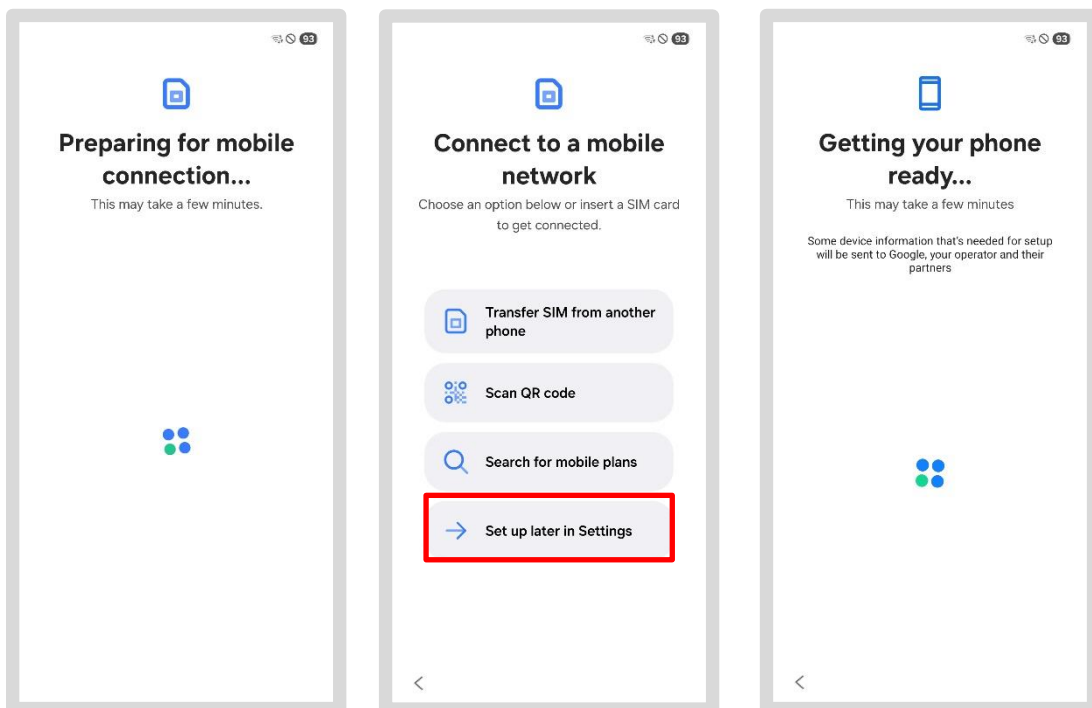
Gdy urządzenie połączy się z siecią Wi-Fi, rozpocznie się proces łączenia z siecią DB.

> Przejdź do [rozdziału 5 Rejestracja Samsunga w DB](#)

5 Zainstaluj aplikację Samsung

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.

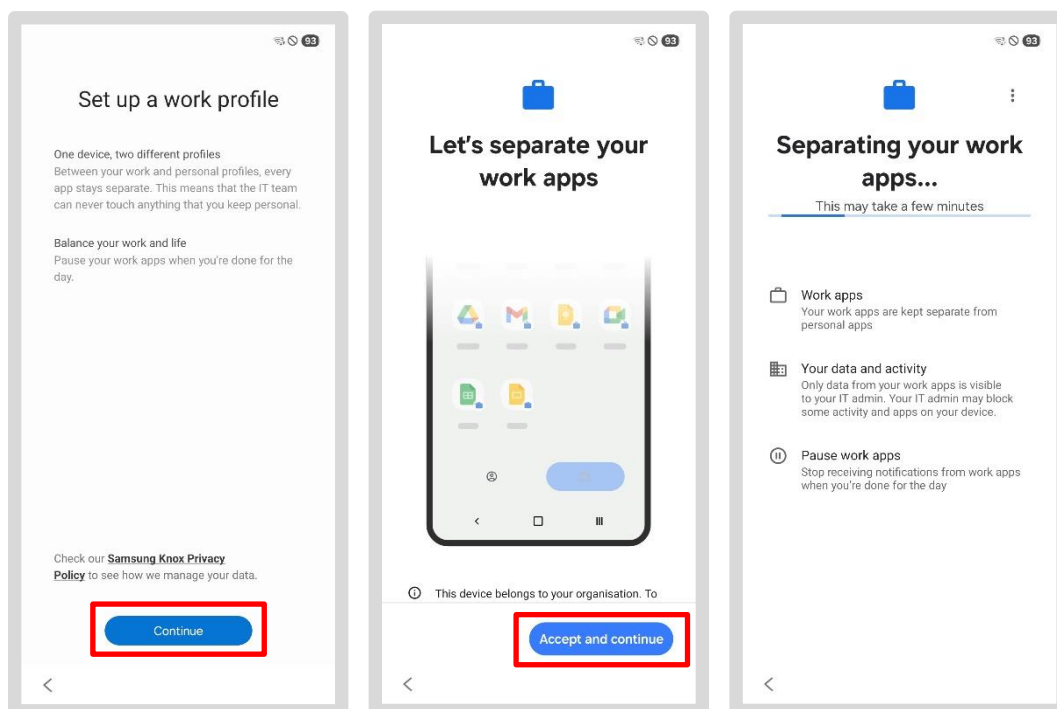
- Trzymaj tablet w **trybie pionowym**, jeśli do tej pory trzymałeś go w trybie poziomym
- Poszczególne ekrany będą teraz migać
- Naciśnij „Skonfiguruj później”, a kilka ekranów wyświetli się ponownie bez konieczności wykonywania jakichkolwiek czynności



5.1 Skonfiguruj profil służbowy

Profil służbowy jest wymagany do przypisania aplikacji służbowych do smartfona/tabletu. Należy go skonfigurować tutaj:

- Smartfon/tablet jest konfigurowany
- Potwierdź następujące zapytanie, wybierając „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”

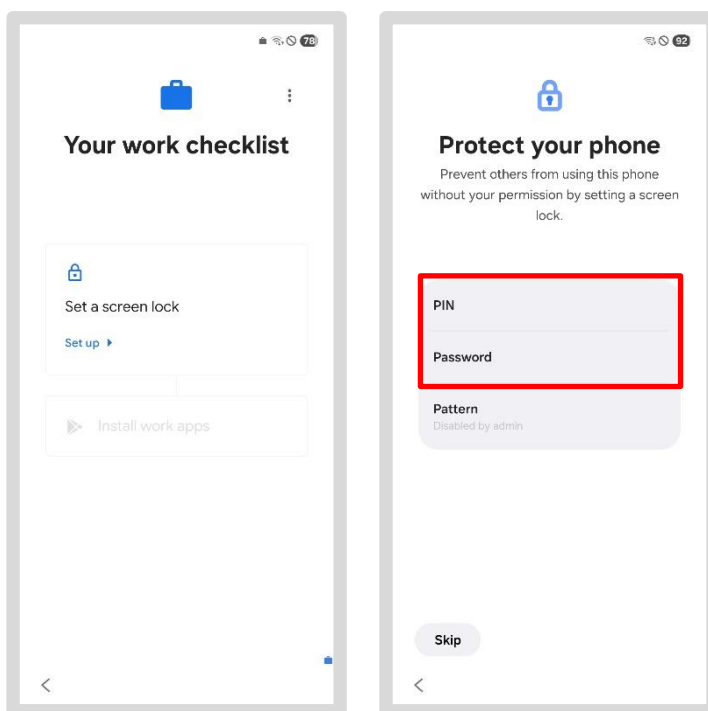


- Aktualizacja urządzenia może chwilę potrwać, a w niektórych przypadkach nawet bardzo długo, więc prosimy o cierpliwość!
- Trwa instalacja niezbędnych aplikacji
- Może pojawić się prośba o podanie konta prywatnego
 - > W takim przypadku przejdź do sekcji 5.4 Konto Google – nie jest to konieczne
- Jeśli ten komunikat się nie pojawi, postępuj zgodnie z instrukcjami jak zwykle.
 - > Przejdź do sekcji 5.2 Ustaw blokadę ekranu

5.2 Ustaw blokadę ekranu

Kolejnym krokiem jest skonfigurowanie blokady ekranu w urządzeniu. Jest to wymagane przez DB ze względu na ochronę danych i zapewnia niezawodną ochronę Twoich 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 6 cyfr
- Gdy pojawi się komunikat „Skonfiguruj dane biometryczne”, dotknij „Pomiń”



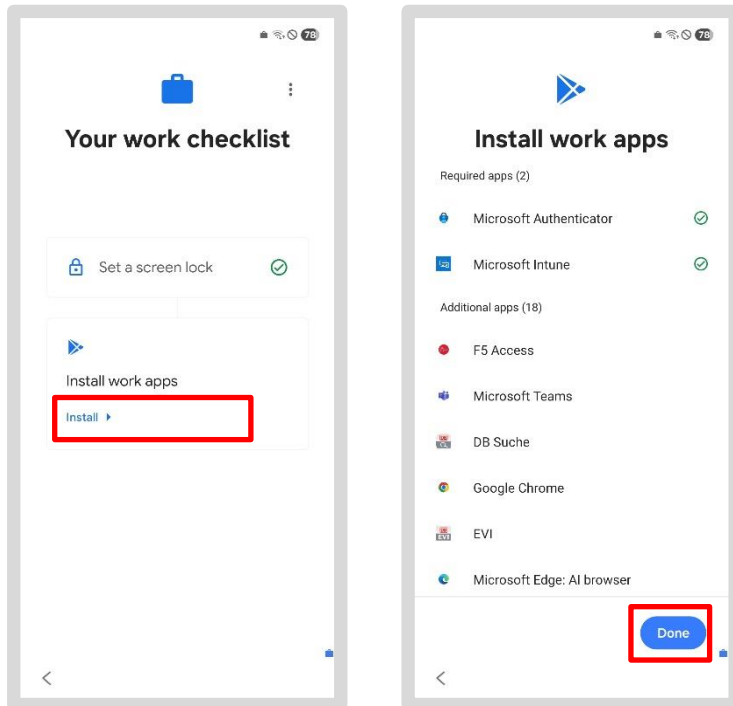
- Zwróć uwagę na informacje dotyczące prywatności i użytkowania zawarte w instrukcjach dotyczących konfiguracji początkowej
- Potwierdź, wybierając „Kontynuuj”, a następnie „OK” po dwukrotnym wprowadzeniu danych
- Jeśli pojawi się ekran „Konta prywatne”, dotknij „Później” po wyświetleniu monitu
- W tym miejscu może pojawić się pytanie dotyczące usług Google
 - > W takim przypadku przejdź do sekcji 5.5 Aktywacja usług Google
- Jeśli ten monit się nie pojawi, postępuj zgodnie z instrukcjami jak zwykle
 - > Przejdź do sekcji 5.3 Instalowanie aplikacji bazodanowych

5.3 Instalowanie aplikacji DB

W tym miejscu może najpierw pojawić się ekran „Aktywuj usługę Google”. Jeśli tak się stanie, przejdź do [sekcji 5.5 Aktywuj usługę Google](#).

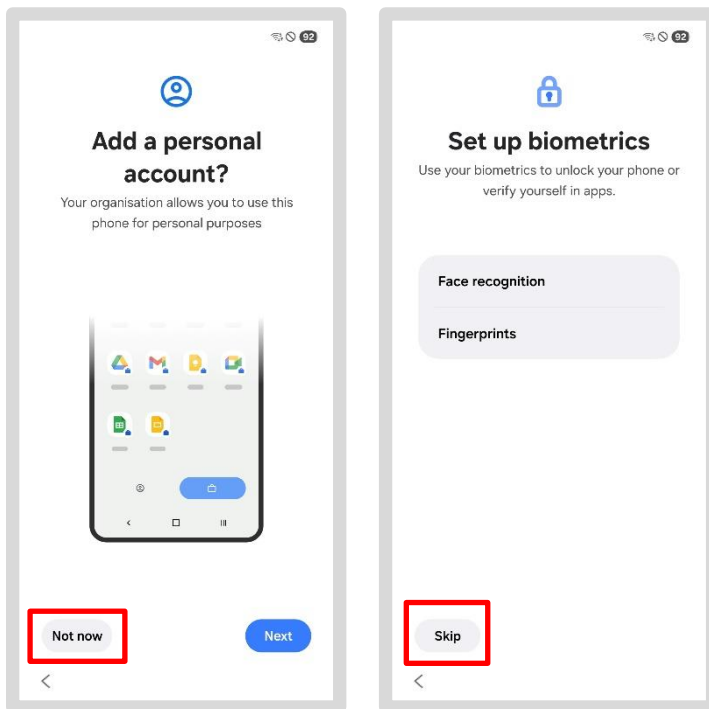
W następnym kroku wszystkie aplikacje DB zostaną ponownie zainstalowane na smartfonie/tablecie DB. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

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



5.4 Konto Google – nie jest konieczne

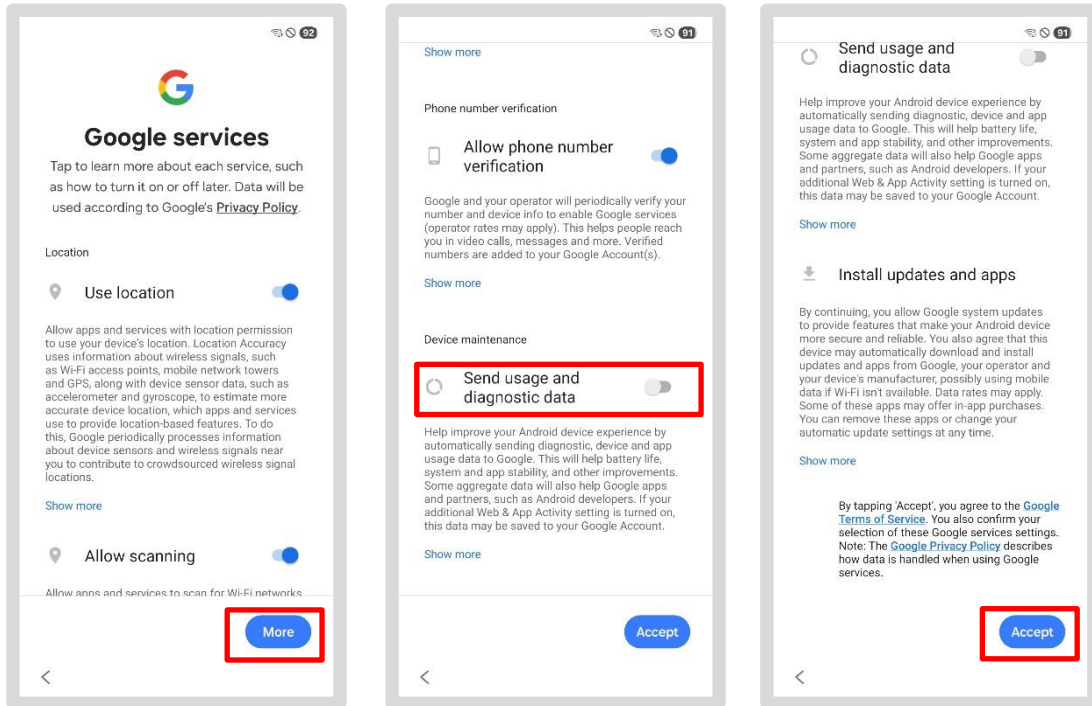
- Na smartfonie/tablecie DB **nie** jest wymagane **prywatne** konto Google!
- W razie potrzeby możesz to zrobić później
- Dlatego dotknij „*Nie teraz*”
- Gdy pojawi się komunikat „*Skonfiguruj dane biometryczne*”, dotknij „*Pomiń*”



- Konto Google jest potrzebne, aby otrzymywać prywatne wiadomości e-mail, na przykład przez Gmaila. Prywatne konto Google można również utworzyć później

5.5 Włącz usługę Google

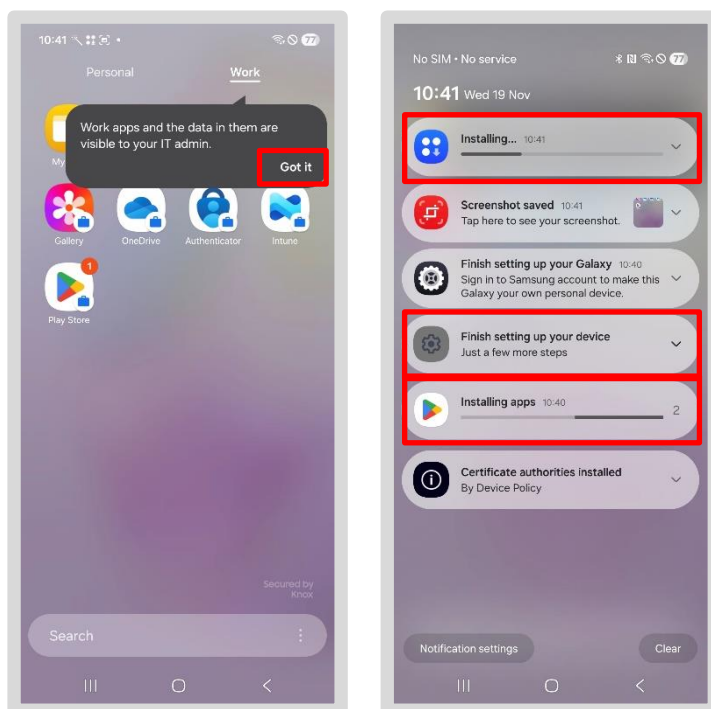
- Kliknij „Więcej” w sekcji Usługi Google
- Aby **wysłać dane dotyczące użytkowania i diagnostyki**: dotknij suwaka, aby wyłączyć tę funkcję
- Przewiń dalej, a następnie dotknij „Akceptuj”



> przejdź do sekcji 5.6 Automatyczna instalacja aplikacji z DB

5.6 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 „Rozumiem”
- 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:** „Dokończ konfigurację urządzenia” nie jest konieczne do skonfigurowania smartfona/tabletu z systemem DB. Zignoruj to!
- Poczekaj tutaj na komunikat „ ” do momentu, 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 3 Rozpocznij migrację: 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 6 Utwórz tymczasową legitymację pracownika DB (TAP)

6 Utwórz tymczasową legitymację pracownika DB (TAP)

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

- Ważna tymczasowa legitymacja pracownika DB – db.de/tap
- nazwa użytkownika DB i hasło użytkownika DB
- Aplikacja Intune

Dla Twojej informacji:

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

- Hasło użytkownika DB można zresetować [na stronie db.de/password](https://db.de/password)
- **Instrukcje dotyczące zmiany hasła** znajdziesz w sekcji „[Zmiana hasła użytkownika bazy danych](#)”
- Informacje o tym, **jak uzyskać nazwę użytkownika bazy danych**, można znaleźć w sekcji [Wymagania wstępne: Użytkownik bazy danych](#)
- **Nazwę użytkownika bazy danych** można znaleźć w DeBi pod adresem db.de/debi

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

6.1 Utwórz tymczasową legitymację pracownika DB (TAP)

> **Uwaga:** Instrukcje wideo znajdziesz na stronie 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 6.2 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. Zanonuj swoją legitymację pracownika DB i przejdź do:

> [Rozdział 3 Rozpocznij migrację: Zresetuj smartfon/tablet](#)

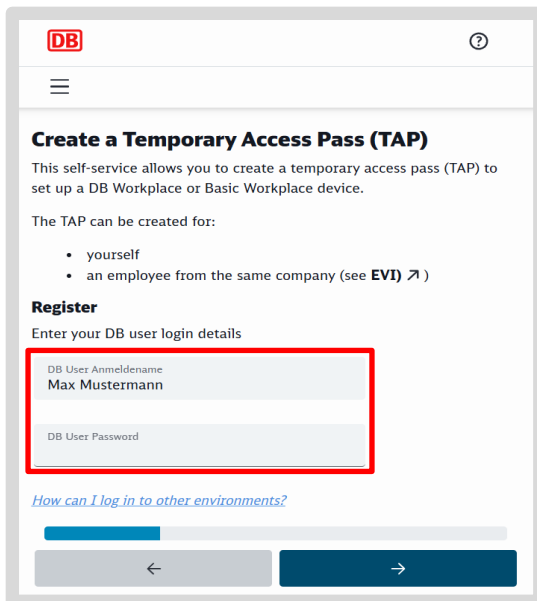
Uwaga: Twój Tap jest ważny tylko przez 60 minut i na wielu smartfonach/tabletach!

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](#))

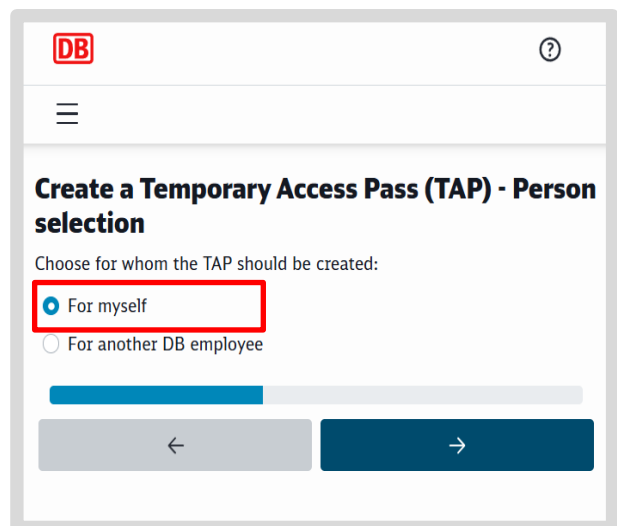
Register

Enter your DB user login details

DB User Anmeldenname
Max Mustermann

DB User Password

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

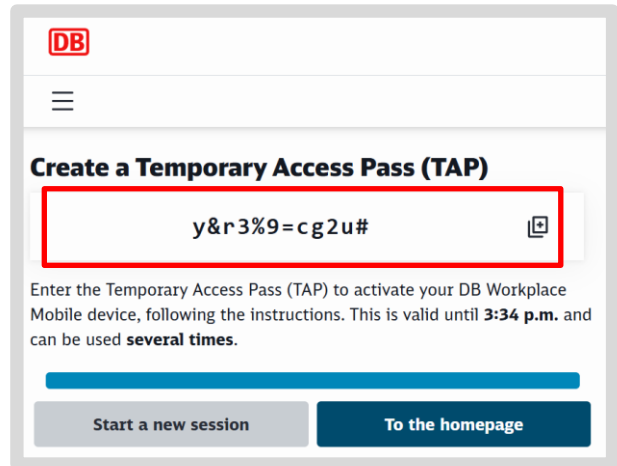
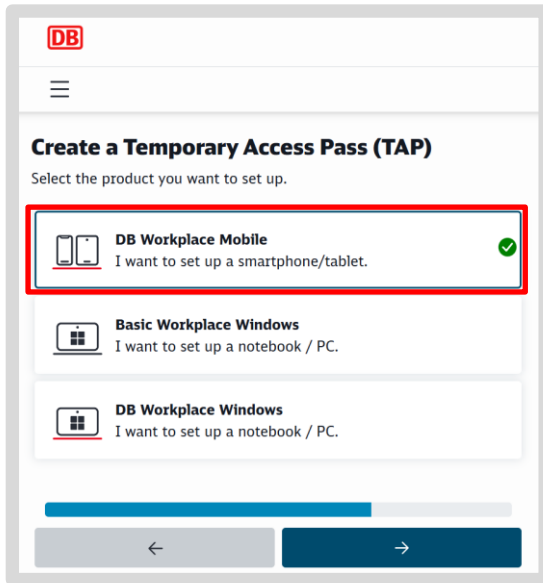


Create a Temporary Access Pass (TAP) - Person selection

Choose for whom the TAP should be created:

For myself

For another DB employee



Uwaga!
Kod **TAP** można wprowadzić wyłącznie w **aplikacji Intune**, nawet jeśli zostaniesz o to poproszony 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 7 Aktywacja urządzenia w aplikacji DB](#)

Ważne!

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

Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku zawartymi w
> [Rozdział 7 Aktywacja urządzenia w DB](#)

6.2 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 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
- Wprowadź swoją nazwę użytkownika DB i hasło użytkownika DB
- Wybierz opcję „Dla innego pracownika DB” i naciśnij niebieski przycisk

- 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 7 Aktywacja urządzenia w bazie danych

Ważne!


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

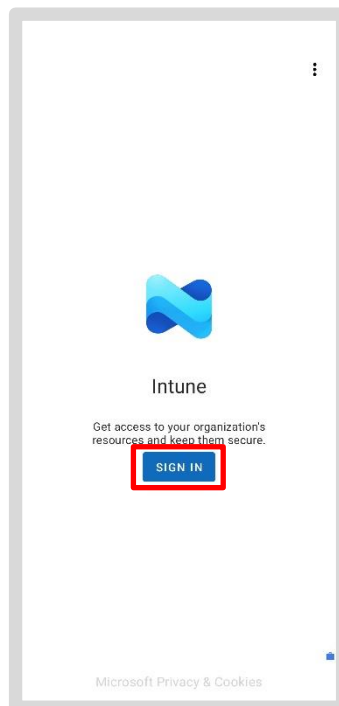
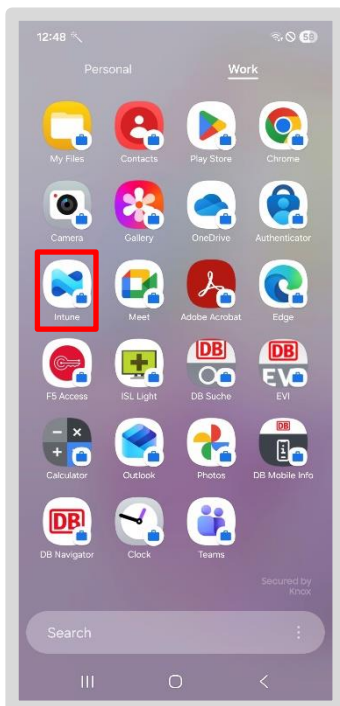
Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku zawartymi w
> Rozdział 7 Aktywacja urządzenia w DB

7 Aktywacja urządzenia w DB

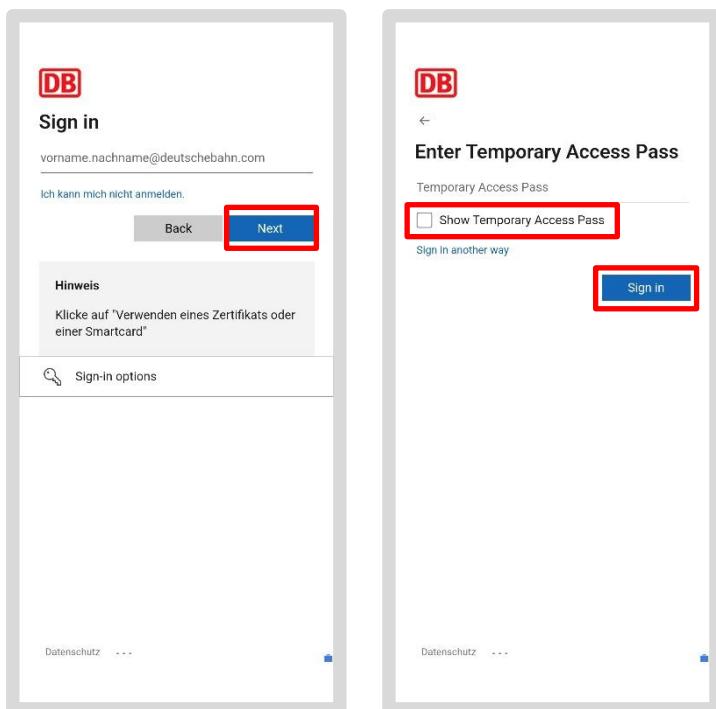
> **Uwaga:** Sprawdź, czy utworzyłeś i otrzymałeś tymczasową legitymację pracownika DB (TAP) zgodnie z opisem w Rozdziale 6 Utwórz tymczasową legitymację pracownika DB (TAP)!

> **Uwaga:** Instrukcje wideo można znaleźć pod adresem 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 rejestracji zgodnie z opisem w rozdziale 6 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)

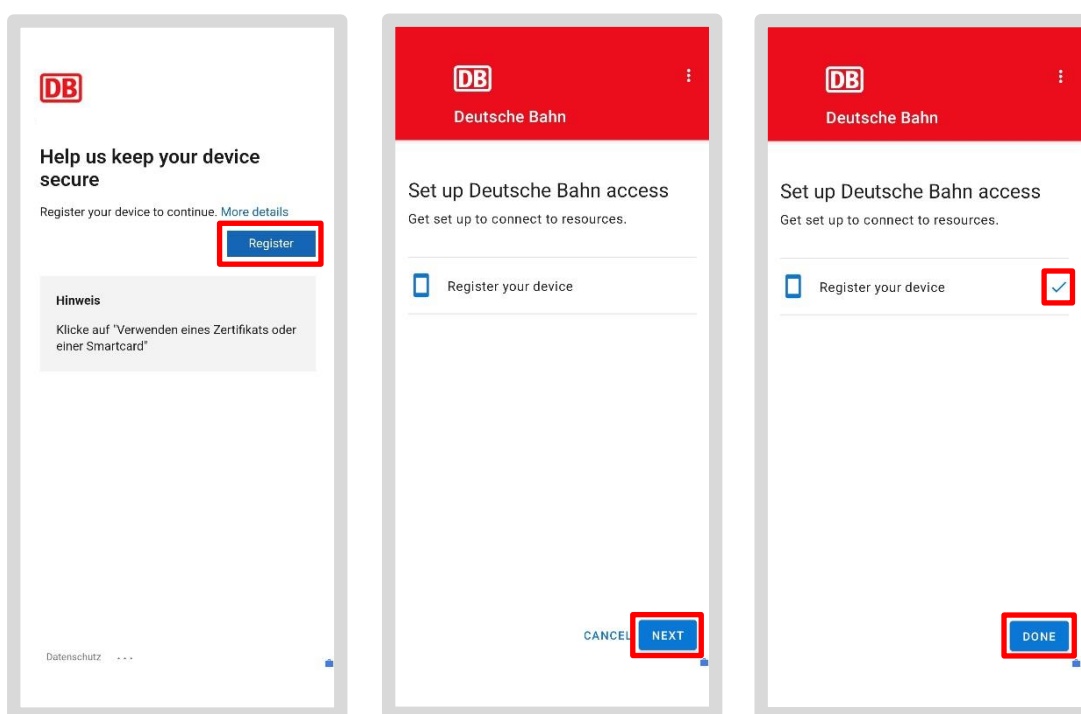
> Przejdź do rozdziału 7.1 Konfigurowanie dostępu do wszystkich aplikacji i stron internetowych DB

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.

7.1 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 pojawia się, aktywacja nie została zakończona
- Otwórz ponownie aplikację Intune i wykonaj krok po kroku czynności opisane w rozdziale 7, Aktywacja urządzenia w bazie danych



> 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.

7.2 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 aplikacji 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 Store (aplikacja z ikoną walizki) w sekcji „Praca”.

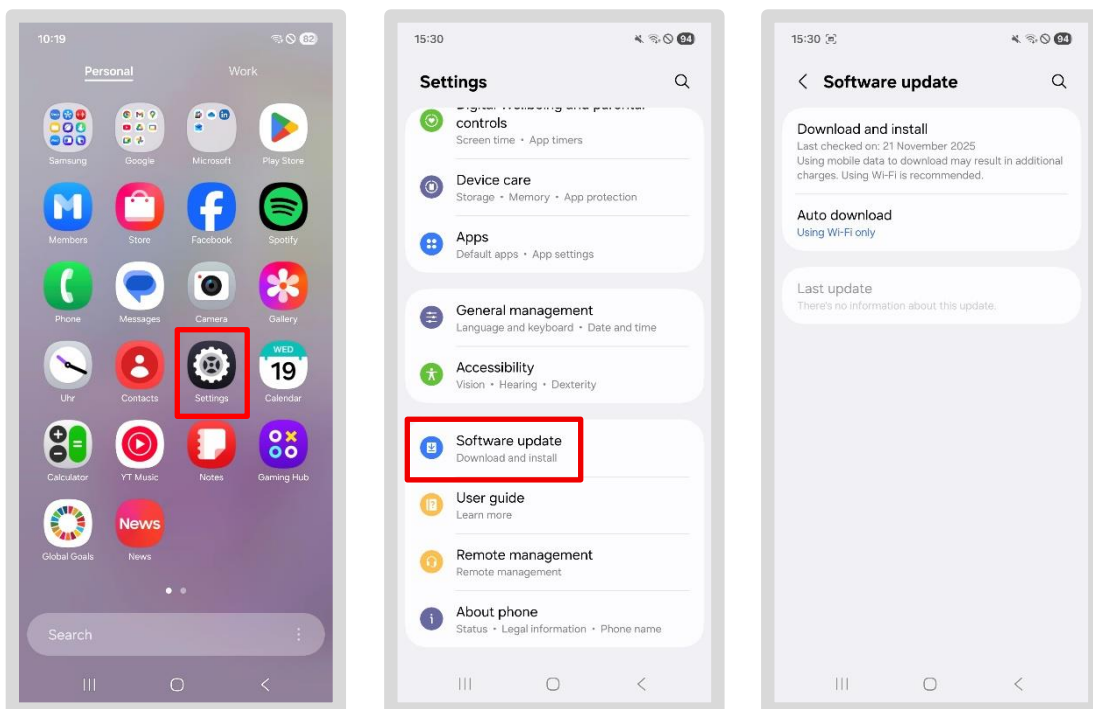
Aplikacja Welcome nie jest już dostępna na smartfonie/tablecie DB, ale dostępna jest **aplikacja DB MOBIL** zawierająca wszystkie potrzebne informacje, przydatne linki i dane dotyczące smartfona/tabletu DB.

8 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.

8.1 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”



8.2 Outlook

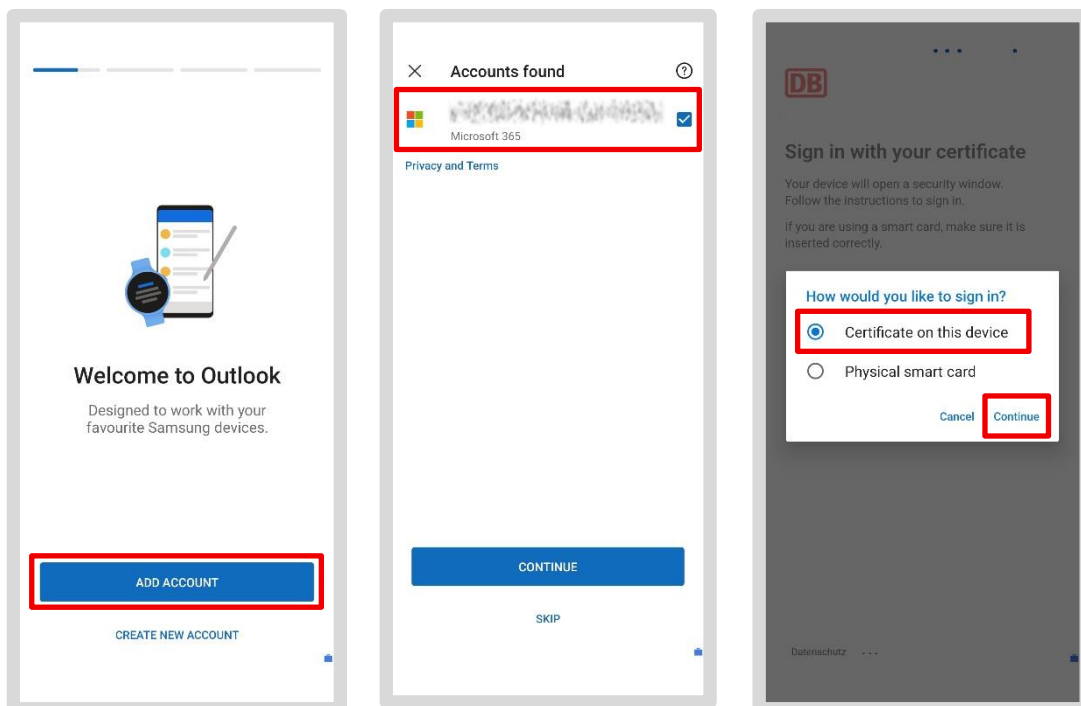
8.2.1 Skonfiguruj Outlook /Utwórz konto e-mail/Skonfiguruj szyfrowanie wiadomości e-mail

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

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

Gdy pojawi się monit o zalogowanie, możesz zostać poproszony o podanie tymczasowej legitymacji pracownika DB (TAP):

- Jeśli Twoja tymczasowa legitymacja pracownika DB jest nadal ważna, wprowadź ją tutaj lub utwórz nową zgodnie z opisem w [rozdziale 6.1 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



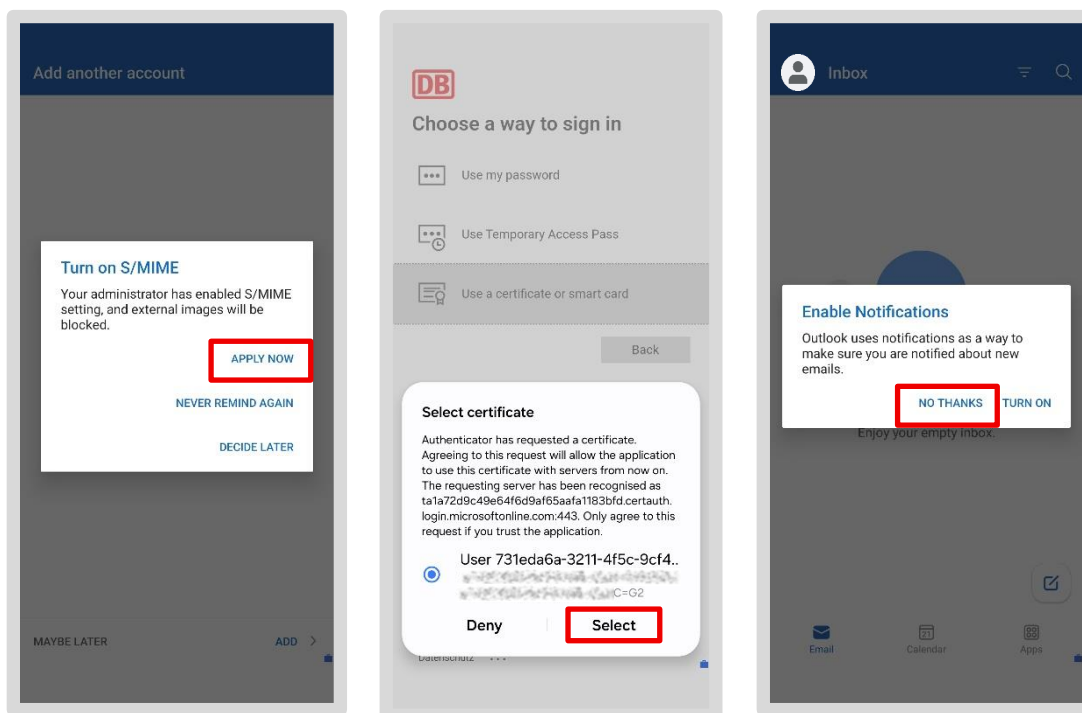
- Jeśli chcesz wysłać szczególnie wrażliwe dane (np. informacje osobowe) pocztą elektroniczną, musisz również zastosować szyfrowanie treści wiadomości e-mail
- DB zapewnia w tym celu szyfrowanie S/MIME
- Naciśnij „Zastosuj teraz”, gdy pojawi się pytanie, czy chcesz aktywować S/MIME

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

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

Twoje konto e-mail zostanie teraz skonfigurowane:

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



- Twoje wiadomości e-mail zostaną teraz załadowane (proces ten może potrwać kilka minut)
- Możesz teraz ponownie czytać i pisać wiadomości e-mail

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



8.2.2 Skonfiguruj podpis e-mail

Podpis e-mailowy jest obowiązkowym elementem komunikacji biznesowej. Pojawia się on na końcu wiadomości e-mail i zgodnie z prawem musi 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”.

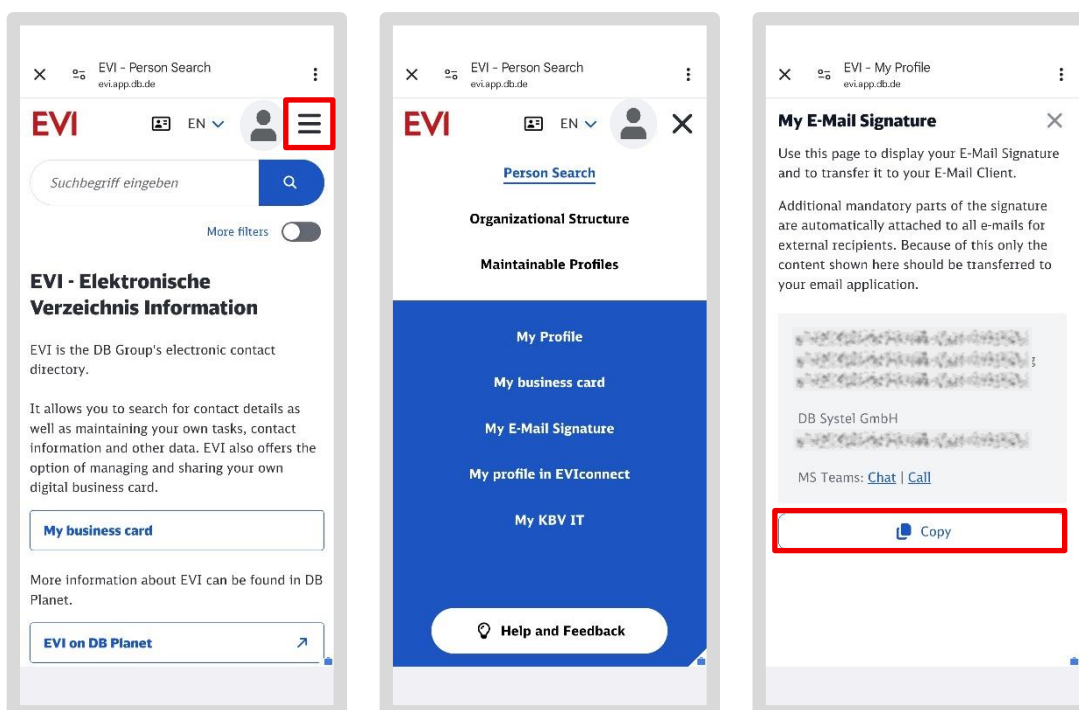
Jak uzyskać podpis e-mailowy z EVI:



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

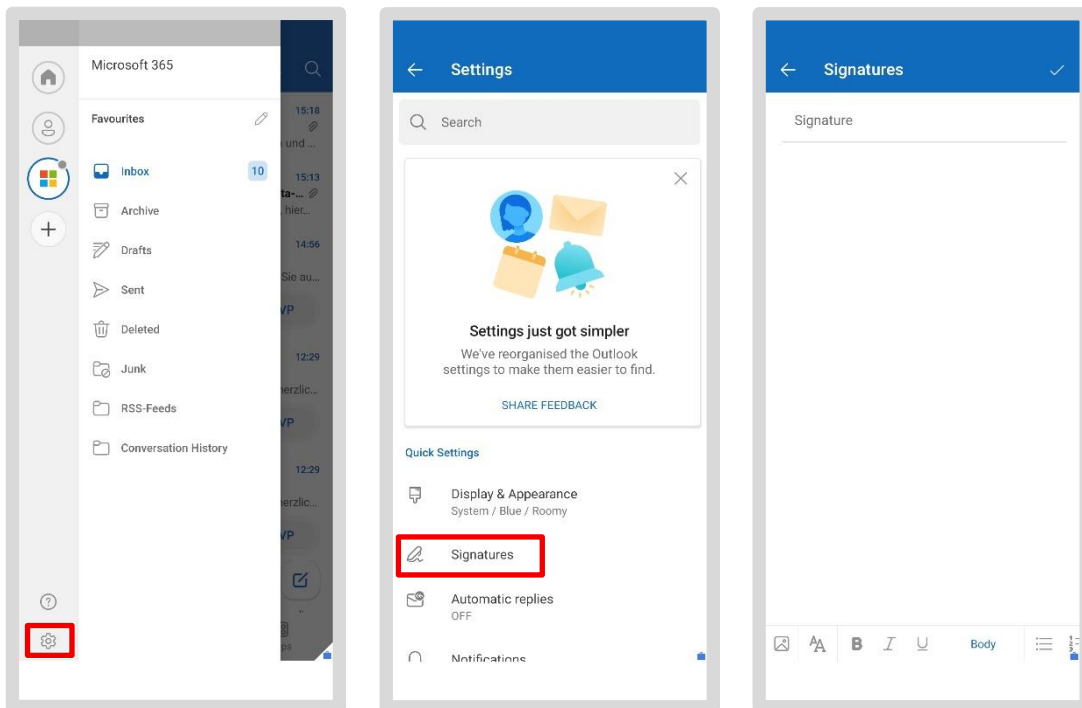
Otworzy się widok nowego EVI:

- 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 programu Outlook:

- Otwórz aplikację Outlook w sekcji „Praca/Biznes”
- Dotknij swojego zdjęcia profilowego w lewym górnym rogu
- Po lewej stronie otworzy się przegląd folderów poczty
- 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.

8.2.3 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/Basicworkplace, zawsze masz aktualne dane.

8.3 Aplikacja MS Defender

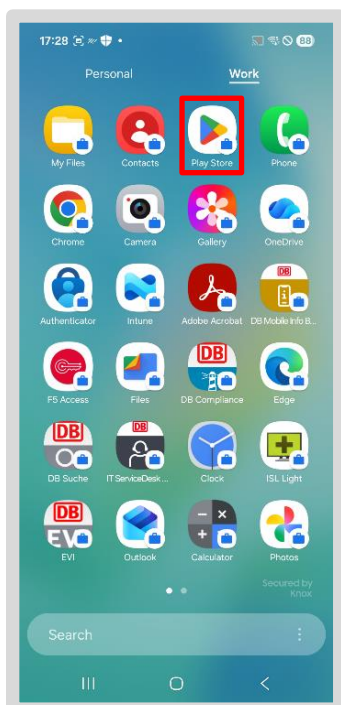
Po aktywowaniu aplikacji Outlook i Teams należy aktywować aplikację „Microsoft Defender for Endpoint Mobile” (w skrócie aplikacja MS Defender) na smartfonie/tablecie. Aplikacja chroni przed cyberatakami i skanuje istniejące aplikacje w poszukiwaniu złośliwego oprogramowania. Aby aktywować ochronę, należy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

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

8.3.1 Konfiguracja aplikacji MS Defender

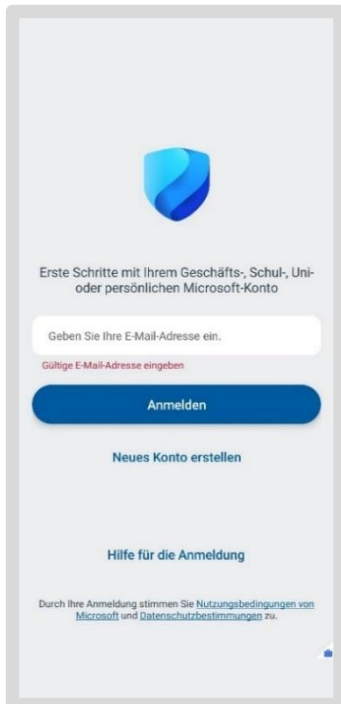
Aby skonfigurować aplikację MS Defender na smartfonie/tablecie, należy wykonać następujące czynności:

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

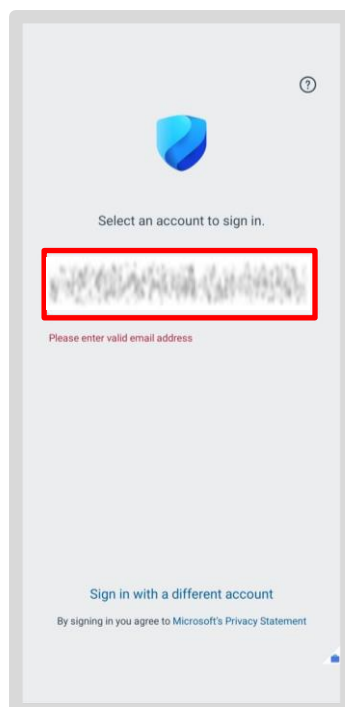
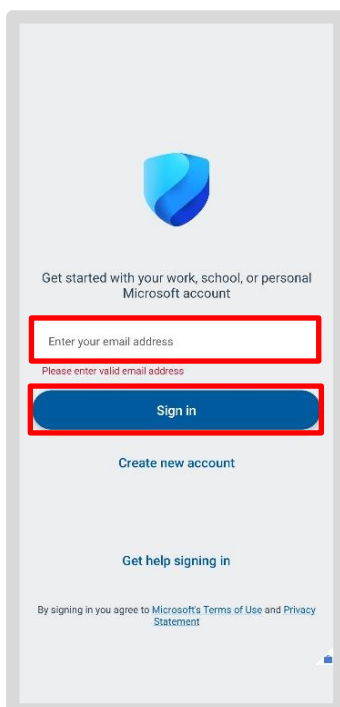


- Wyszukaj aplikację „Microsoft Defender: Antivirus” i kliknij „Zainstaluj”

- Naciśnij ikonę 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
- Naciśnij swój służbowy adres e-mail

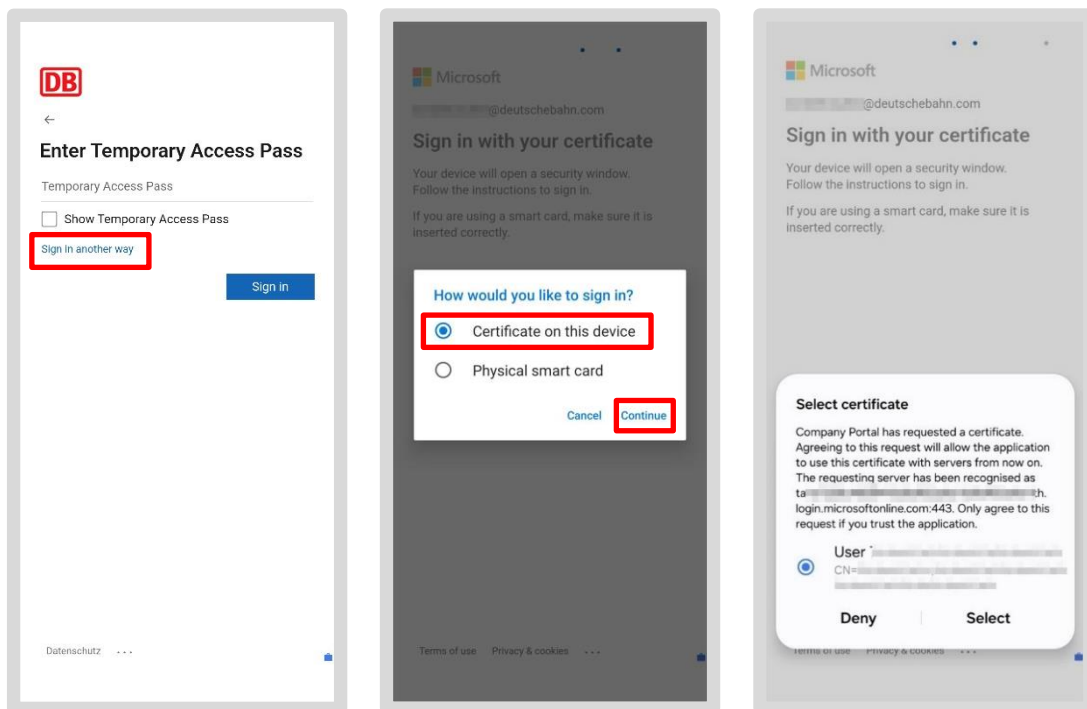


Jeśli w ciągu godziny aktywowałeś smartfon/tablet za pomocą aplikacji Intune, możesz zostać poproszony o ponowne wprowadzenie tymczasowej legitymacji pracownika DB.

- Wybierz opcję „Zaloguj się w inny sposób”

Następnie przejdź dalej:

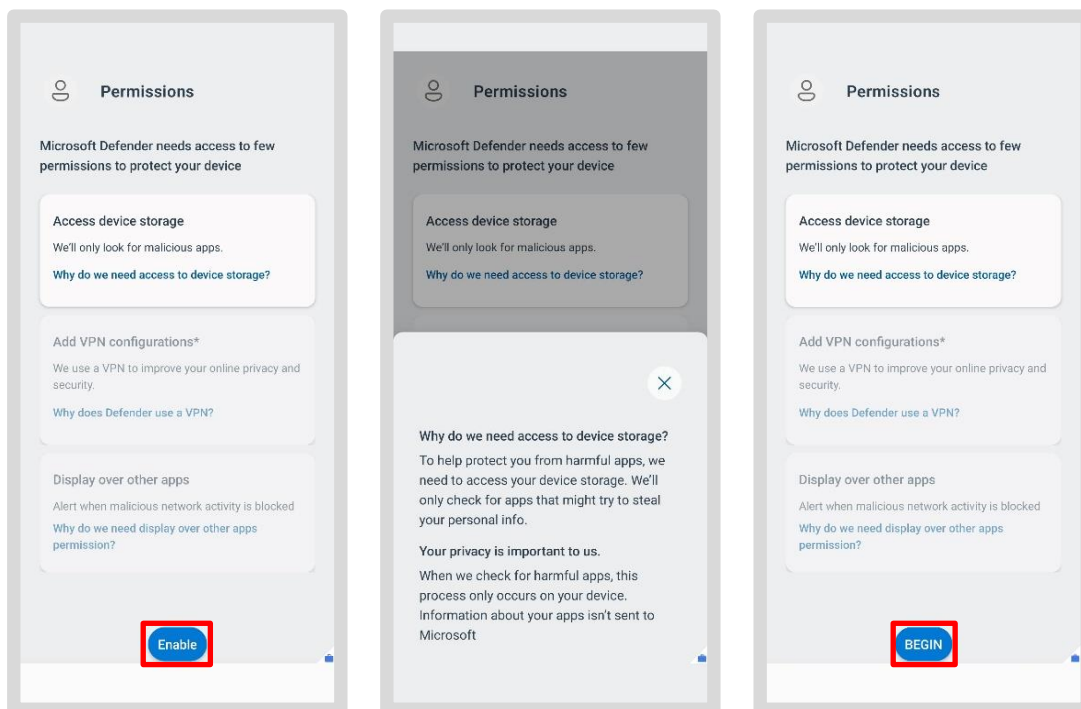
- Po wyświetleniu monitu dotknij opcji „Certyfikat na tym urządzeniu”, a następnie dotknij „Dalej”
- Wybierz certyfikat



8.3.2 Przyznaj uprawnienia

Aplikacja poprosi Cię teraz o udzielenie niezbędnych uprawnień. W tym momencie kolejność wyświetlanych ekranów może różnić się od podanej w instrukcji. Jeśli pierwszy ekran odpowiada temu na ilustracji:

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

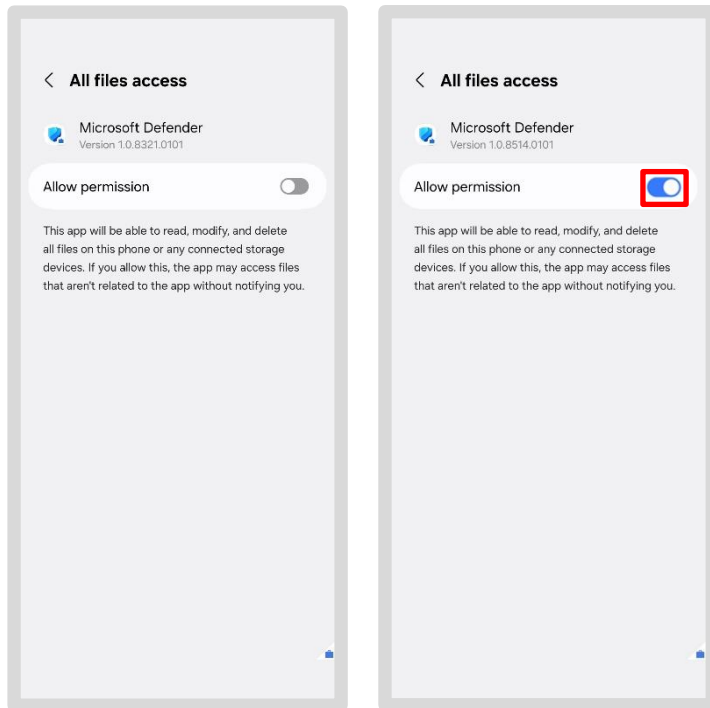


Informacje ogólne dotyczące uprawnień:

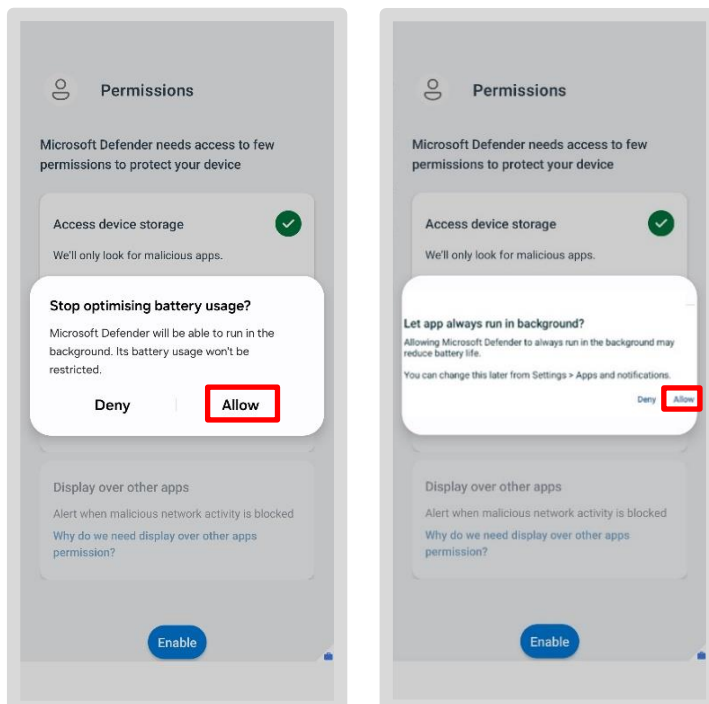
Uprawnienia te są wymagane do prawidłowego działania aplikacji i zapewnienia bezpieczeństwa urządzenia.

Możesz wyświetlić okno informacyjne dla każdego z poszczególnych 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”



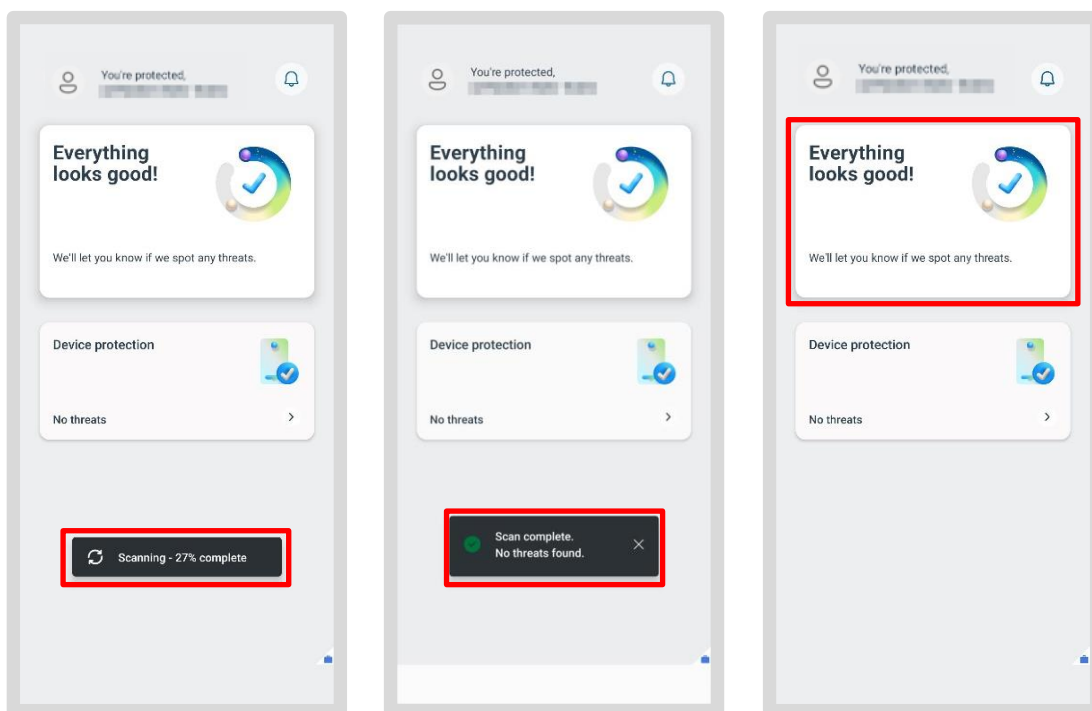
- Naciśnij „Zezwól” dla wszystkich kolejnych zapytań



Uwaga: W zależności od typu urządzenia wymagane są różne uprawnienia! Może to spowodować wyświetlenie tylko jednego z podanych 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.

8.4 DB M 365

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

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

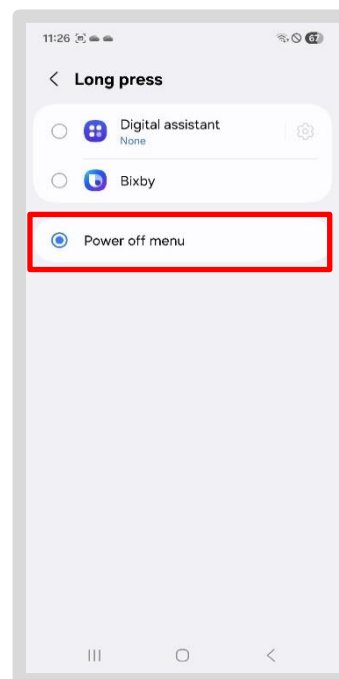
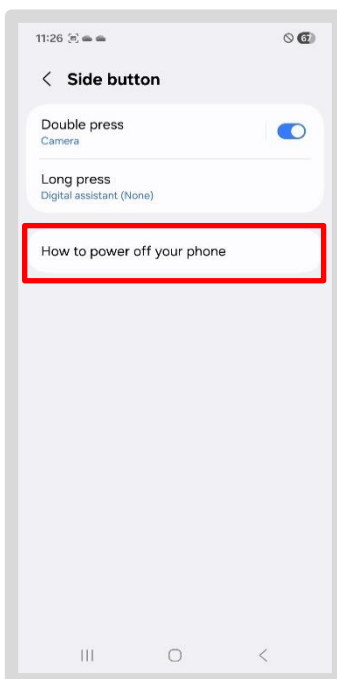
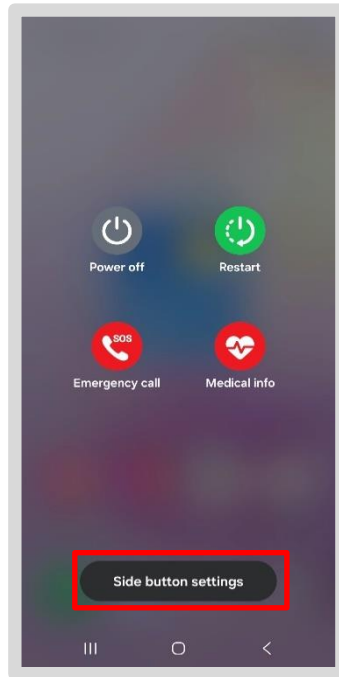


- Następnie kliknij „Zainstaluj”
- Po otwarciu pliku aplikacja uruchomi się automatycznie

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

8.5 Wyłącz przycisk Bixby

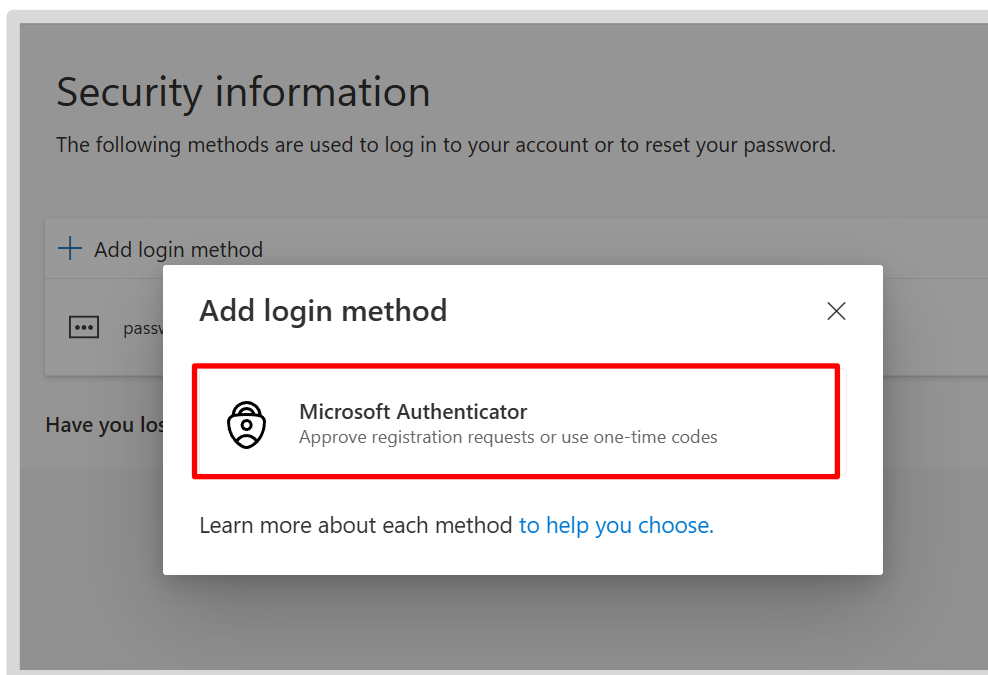
- Domyślnie przycisk zasilania uruchamia asystenta głosowego Bixby. Ze względów bezpieczeństwa należy go wyłączyć:
- Przesuń palcem w dół od góry ekranu
- Dotknij ikony zasilania w prawym górnym rogu, obok ikony ustawień
- Wybierz „Ustawienia klawiszy funkcyjnych”
- Zmień funkcję „Długie naciśnięcie”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



8.6 Ponowne uruchomienie aplikacji do uwierzytelniania Microsoft Authenticator

Jeśli korzystałeś z aplikacji do uwierzytelniania, wykonaj następujące czynności:

- Kliknij „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: „Resetuj aplikację Microsoft Authenticator (MFA)”: 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