



Wersja systemu operacyjnego: Android 15 lub nowsza

Migracja Samsung DB Workplace Mobile

DB Systel GmbH | 15 sierpnia 2026 r.

Spis treści

1 Przegląd procesu migracji	4
2 Kroki niezbędne 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 Utworzenie tymczasowej legitymacji pracownika DB (TAP) – tryb ekspercki	6
3 Rozpocznij migrację: zresetuj smartfon/tablet	7
3.1 Samodzielne resetowanie 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 Konfiguracja Wi-Fi	11
4.4 Konfiguracja Wi-Fi w budynkach DB	12
5 Instalacja aplikacji Samsung E	13
5.1 Konfiguracja profilu służbowego	14
5.2 Konfiguracja blokady ekranu	15
5.3 Instalacja aplikacji DB	16
5.4 Konto Google – nie jest wymagane	16
5.5 Aktywacja usług Google	17
5.6 Automatyczna instalacja aplikacji bazodanowych	18
6 Utwórz tymczasową legitymację pracownika DB dla	19
6.1 Utwórz tymczasową legitymację pracownika DB (TAP)	19
6.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika	22
7 Aktywacja urządzenia w DB	24
7.1 Skonfiguruj dostęp do wszystkich aplikacji i stron internetowych DB	25
7.2 Aplikacje DB	27
8 Wymagane ustawienia	28
8.1 Sprawdź dostępność aktualizacji systemu operacyjnego	28
8.2 Outlook	29
8.2.1 Konfiguracja programu Outlook / Utworzenie konta e-mail / Konfiguracja szyfrowania wiadomości e-mail	29

8.2.2 Konfiguracja podpisu e-mailowego	30
8.2.3 Synchronizacja wiadomości e-mail — wszystkie wiadomości zawsze aktualne	32
8.3 Aplikacja MS Defender — należy ją uruchomić	32
8.3.1 Konfiguracja aplikacji MS Defender	32
8.3.2 Przyznanie uprawnień	34
8.4 DB M 365	36
8.5 Wyłącz przycisk Bixby	37
8.6 Ponowne włączenie aplikacji Microsoft Authenticator do uwierzytelniania	38

1 Proces migracji w skrócie

Cały proces migracji do DB MOBIL podsumowano poniżej:



Planowanie migracji

- **Gdy tylko otrzymasz wiadomość e-mail: Umów się na spotkanie w narzędziu PME**
> zobacz [sekcję 2.1 Rezerwacja terminu migracji](#)



Techniczne przygotowanie do migracji

- **E-mail z przypomnieniem** na krótko przed terminem spotkania, potwierdzający, że migracja może się rozpocząć



Osobiste przygotowania do migracji

- **Utwórz kopię zapasową danych**
> Zobacz [sekcję 2.2: Tworzenie kopii zapasowej danych](#)
- *Jeśli korzystasz z aplikacji do uwierzytelniania*
> zobacz [sekcję 2.3 Aplikacja Authenticator – opcjonalnie](#)
- **Przeprowadź aktualizację systemu** – sprawdź to w Ustawieniach systemowych



Migracja do DB Workplace Mobile

- **Zresetuj** smartfon/tablet
> patrz [rozdział 3 Rozpoczęcie migracji: zresetuj smartfon/tablet](#)
- **Utwórz i zapisz** tymczasową legitymację pracownika DB (TAP)
> patrz [rozdział 6: Utwórz tymczasową legitymację pracownika DB \(TAP\)](#)
- **Aktywuj** smartfon/tablet w usłudze Microsoft Intune
> patrz [rozdział 7: Aktywacja urządzenia w bazie danych](#)

Ważne!

Smartfon/tablet jest
podłączony do sieci DB, gdy posiada
tymczasowa legitymacja pracownika DB (TAP)
została wprowadzona w *aplikacji Intune*.
Aplikacje Outlook lub Teams nie są do tego odpowiednie!

Postępuj zgodnie z poniższymi instrukcjami krok po kroku!

2 Czynności wymagane przed migracją

2.1 Umów się na termin migracji

- **Zarezerwuj termin migracji w narzędziu PME pod adresem db.de/pme, gdy tylko otrzymasz wiadomość e-mail z prośbą o to:**
 - Jeśli nie możesz tego zrobić samodzielnie, poproś kierownika miejsca powstawania kosztów lub upoważnionego nabywcę o zarezerwowanie terminu w Twoim imieniu. Terminy można rezerwować od poniedziałku do piątku na następny dzień roboczy (poniedziałek–piątek) do godziny 12:00.
- **Jeśli nie możesz dotrzymać terminu migracji:** Możesz anulować termin do godziny 12:00 w dniu poprzedzającym (poniedziałek–piątek)!
- **Od zarezerwowanej daty migracji masz 28 dni** na migrację swojego smartfona/tabletu. Ostateczny termin jest wyświetlany w PME. Po upływie tego terminu Twoje urządzenie zostanie automatycznie usunięte i przeniesione do DB MOBIL za pomocą usługi Microsoft Intune.

2.2 Utwórz kopię zapasową danych

> **Uwaga:** Film instruktażowy znajdziesz pod adresem db.de/mobile-videoanleitung

- **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 dotyczy:

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

> Instrukcje dotyczące tworzenia kopii zapasowej danych znajdziesz na [stronie](#)

2.3 Aplikacja Authenticator – opcjonalna

Uwaga: Niniejsze informacje dotyczą wyłącznie użytkowników, którzy aktywnie korzystają z aplikacji Authenticator, na przykład w celu uzyskania dostępu administracyjnego za pośrednictwem tzw. „2-account” lub w celu uwierzytelniania dwuetapowego, np. w przypadku sieci VPN na komputerze MAC w ramach Basic Workplace.

- Należy pamiętać, że podczas migracji nie można korzystać z aplikacji Authenticator do uwierzytelniania
- Nie są wymagane żadne dalsze kroki
- Po migracji aplikację należy ponownie aktywować; procedura ta została opisana w [sekcji 8.6 Ponowna aktywacja aplikacji Microsoft Authenticator dla uwierzytelniania](#)
- Jeśli podczas migracji konieczne jest korzystanie z aplikacji Authenticator, należy użyć innego smartfona lub tabletu, aby połączyć się z aplikacją Authenticator. W tym celu należy

postępować zgodnie z instrukcją krok po kroku dotyczącą konfiguracji uwierzytelniania wieloskładnikowego (MFA)

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

Jeśli posiadasz tylko jeden smartfon/tablet DB i możesz zresetować urządzenie samodzielnie, utwórz tymczasową legitymację pracownika DB (TAP) przed jego zresetowaniem.

- > W tym celu przejdź do rozdziału 6.1 Tworzenie tymczasowej legitymacji pracownika DB (TAP)
- Następnie zresetuj urządzenie

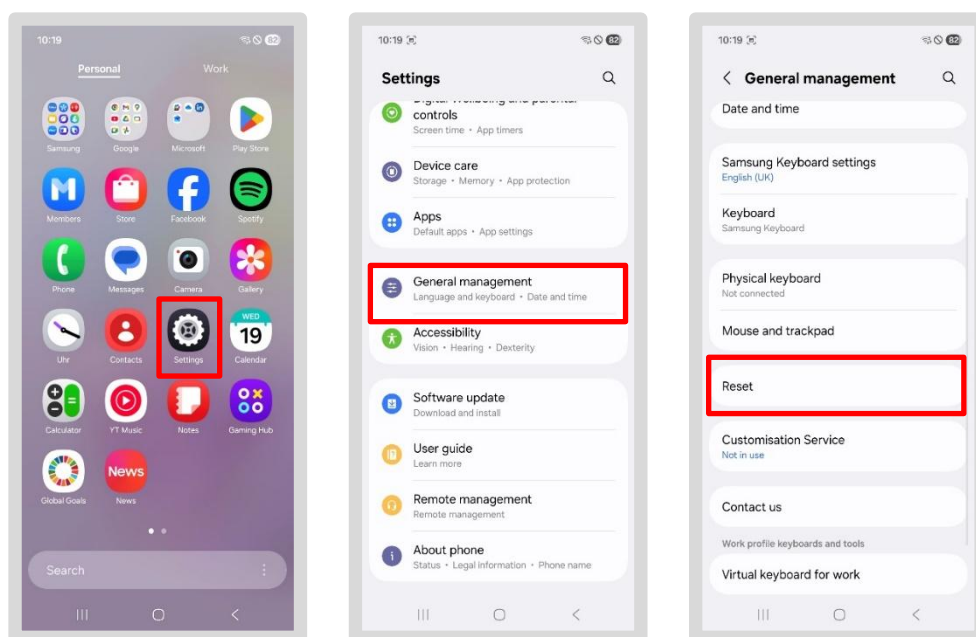
3 Rozpocznij migrację: Zresetuj smartfon/tablet

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

3.1 Samodzielne resetowanie smartfona/tabletu

> **Uwaga:** Film instruktażowy znajdziesz pod adresem db.de/mobile-videoanleitung

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



- Następnie wybierz opcję „Przywróć ustawienia fabryczne”
 - Pojawi się komunikat wyjaśniający, jakie dane zostaną usunięte w wyniku resetowania
 - Sprawdź, czy wykonałeś kopię zapasową danych służbowych (instrukcje: [Tworzenie kopii zapasowej danych](#))
 - Następnie dotknij przycisku „Resetuj”, wprowadź kod dostępu do ekranu blokady, a następnie dotknij „Usuń wszystko”
 - Poczekaj kilka minut; urządzenie zresetuje się automatycznie
- > Następnie przejdź do [rozdziału 4: Ponowna konfiguracja](#)

3.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk

Jeśli smartfon/tablet przestał działać, wykonaj następujące czynności:

- Otwórz aplikację IT ServiceDesk i w sekcji „*Nowe zgłoszenie serwisowe*” prześlij zgłoszenie dotyczące zresetowania smartfona/tabletu
- 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 tutaj opcję menu 0
- Centrum obsługi IT DB Cargo
 - Tel. 91 7777 (wewnętrzny)
 - Tel. 00800 327 978 35 (zewnętrzny)
 - Wybierz tutaj opcję menu 0
- Jeśli pojawią się inne problemy, należy z wyprzedzeniem rozważyć następujące kwestie:
 - **Gdzie** wystąpiły **problemy**?
 - **Zidentyfikuj źródło 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.

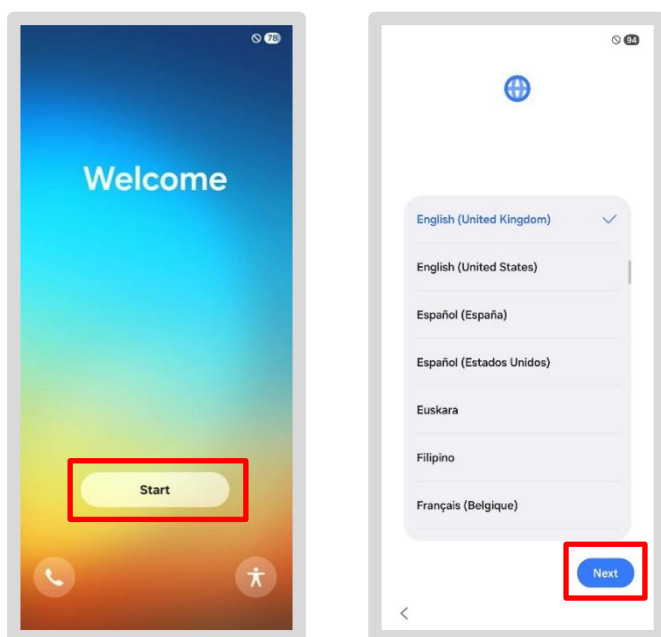
> Następnie przejdź do rozdziału 4: Skonfiguruj ponownie

4 Ponowna konfiguracja

4.1 Wybierz język

> **Uwaga:** Film instruktażowy znajdziesz pod adresem db.de/mobile-videoanleitung

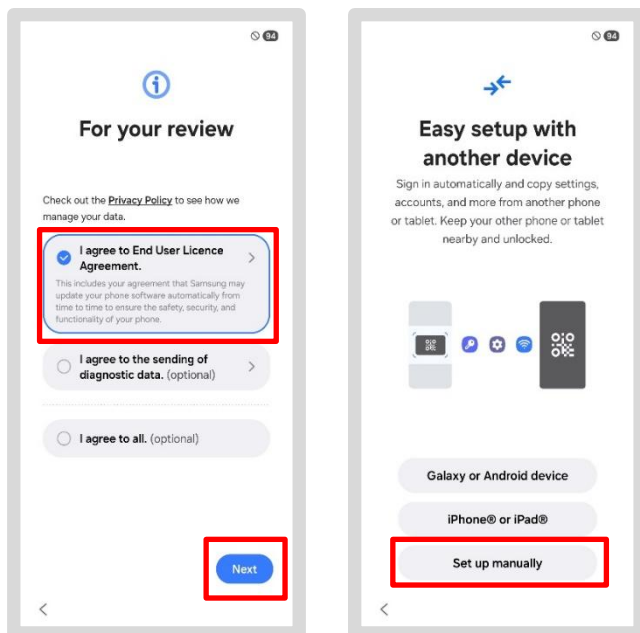
- Trzymaj tablet w **orientacji pionowej**, aby ekrany wyświetlały się dokładnie tak, jak w instrukcji
- Włącz smartfon/tablet
- Upewnij się, że smartfon/tablet jest podłączony do źródła zasilania lub ma wysoki poziom naładowania baterii podczas migracji
- Naciśnij „Start”
- Na następnym ekranie wybierz 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 dotknąć opcji „Dalej”
- W sekcji „Konfiguracja za pomocą innego urządzenia” naciśnij „Konfiguruj ręcznie”



> Przejdź do sekcji 4.3 Konfiguracja Wi-Fi

4.3 Konfiguracja Wi-Fi

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

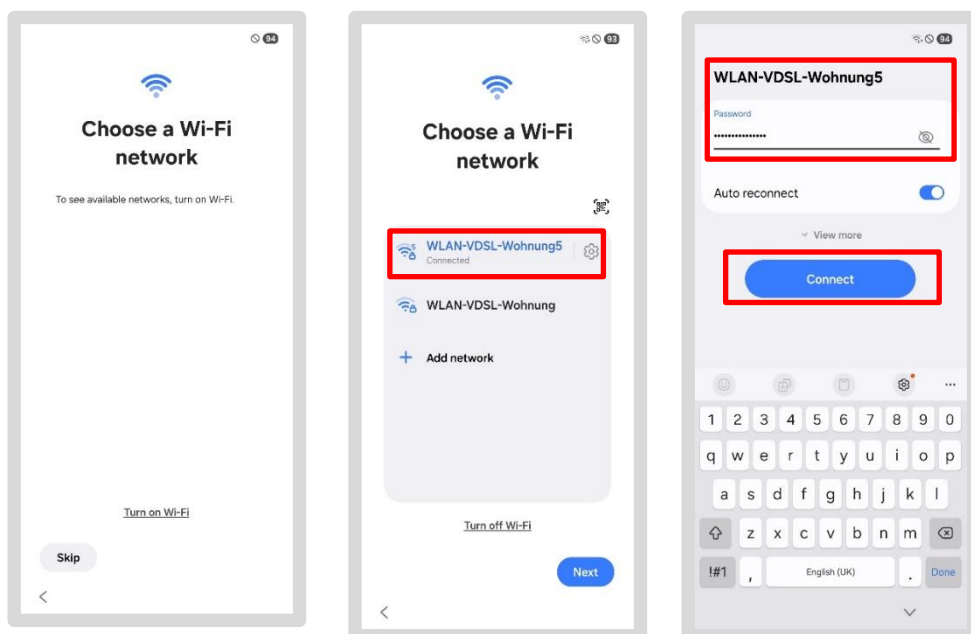
- Skorzystaj z **mobilnego transferu danych**, pod warunkiem, że w smartfonie lub tablecie znajduje się karta SIM (może to wiązać się z opłatą!)
- Skonfiguruj hotspot przy użyciu swojego smartfona lub tabletu

lub

- Skorzystaj z hotspotu na smartfonie DB kolegi
- Skorzystaj z domowej sieci Wi-Fi, jeśli pracujesz z domu

Aby wybrać inną sieć Wi-Fi, wykonaj następujące czynności:

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



Gdy smartfon/tablet połączy się z siecią Wi-Fi, rozpocznie się nawiązywanie połączenia z siecią DB.

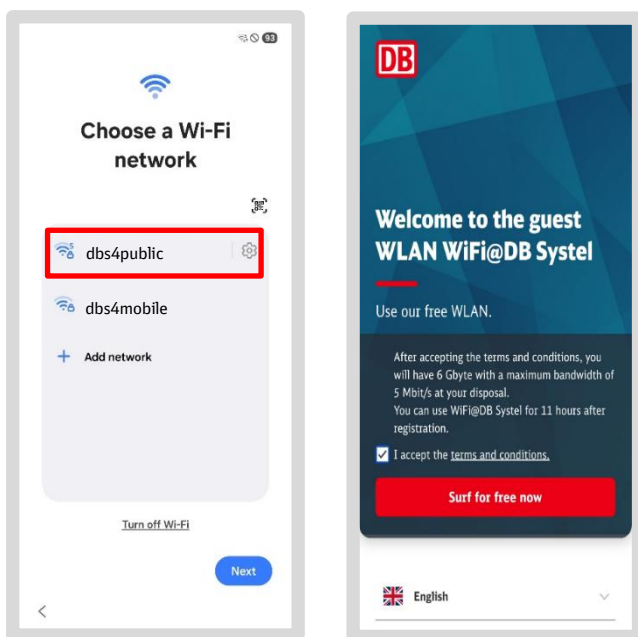
> Przejdź do rozdziału 5: Instalacja urządzeń Samsung

4.4 Konfiguracja Wi-Fi w budynkach DB

Ponieważ sieć Wi-Fi „dbs4public” w budynkach DB nie zawsze działa prawidłowo, zalecamy wykonanie jednej z czynności opisanych w [rozdziale 3.2 Konfiguracja Wi-Fi](#).

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

- Wybierz sieć Wi-Fi „dbs4public”
- Otworzy się okno dialogowe; zaakceptuj warunki korzystania
- Wybierz opcję „Surfuj za darmo teraz”
- Wybierz opcję „Zamknij”



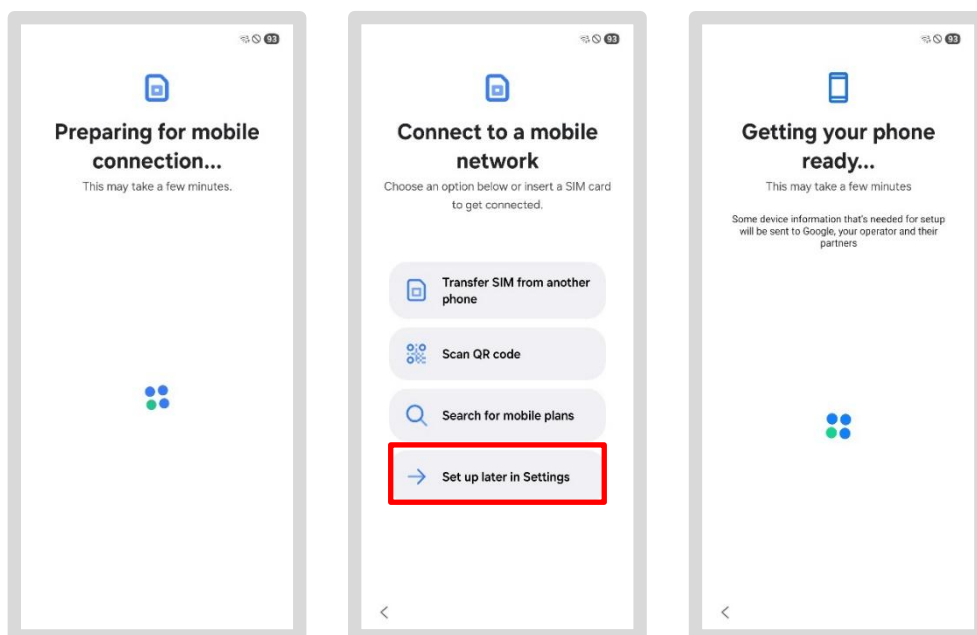
Gdy tylko smartfon/tablet połączy się z siecią Wi-Fi, rozpocznie się nawiązywanie połączenia z siecią DB.

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

5 Instalacja aplikacji Samsung E-

W kolejnym kroku smartfon lub tablet DB musi zostać ponownie podłączony do sieci DB (a konkretnie do systemu Enterprise Mobility Management, w skrócie EMM). Podczas aktualizacji informacji należy poczekać, aż pojawią się instrukcje. W zależności od połączenia sieciowego ekrany mogą migotać lub szybko się zmieniać.

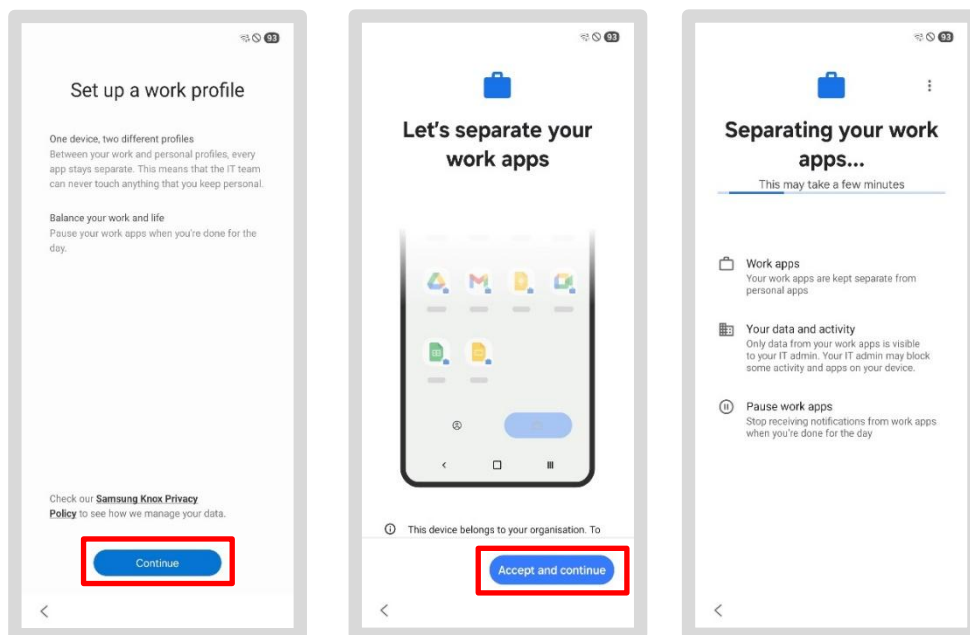
- Jeśli do tej pory trzymałeś tablet w orientacji poziomej, trzymaj go teraz w orientacji **pionowej**
- Poszczególne ekrany będą się teraz przewijać
- Naciśnij „*Skonfiguruj później*”; pojawi się teraz kilka ekranów, bez konieczności wykonywania jakichkolwiek czynności



5.1 Skonfiguruj profil służbowy

Profil służbowy jest wymagany, aby można było przypisać aplikacje służbowe do smartfona/tabletu. Należy go skonfigurować tutaj:

- Trwa konfiguracja smartfona/tabletu
- Potwierdź poniższy komunikat, *dotykając „Dalej”*
- Gdy pojawi się komunikat „Skonfiguruj profil służbowy”, dotknij „Dalej” lub „Zgadzam się”
- Gdy pojawi się komunikat „Administrator IT może kontrolować to urządzenie i blokować aplikacje” (tekst może być ucięty), dotknij „Dalej”



- Aktualizacja urządzenia może potrwać chwilę lub dość długo, więc prosimy o cierpliwość!
- Zostaną zainstalowane wymagane aplikacje
- Może pojawić się prośba o skonfigurowanie konta osobistego

> W takim przypadku przejdź do sekcji 5.4 Konto Google – nie jest to konieczne

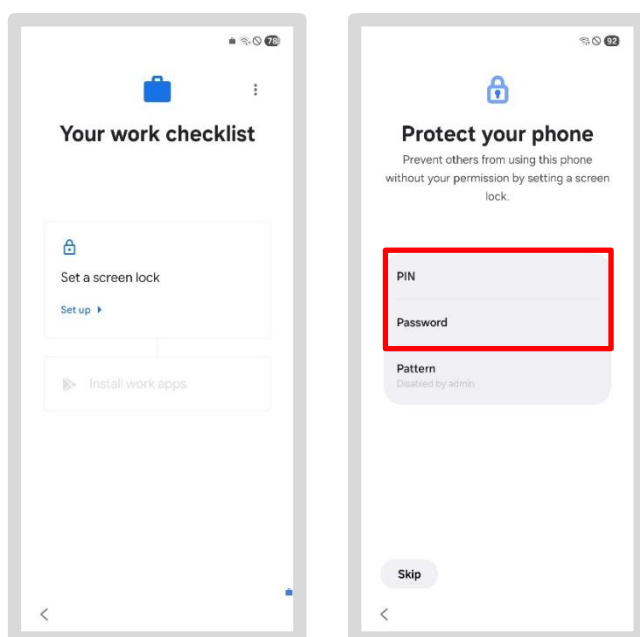
- Jeśli ten komunikat się nie pojawi, postępuj zgodnie z instrukcjami jak zwykle

> Przejdź do sekcji 5.2 „Konfiguracja blokady ekranu”

5.2 Skonfiguruj blokadę ekranu

W następnym kroku skonfigurujesz blokadę ekranu dla swojego urządzenia. Jest to wymagane przez DB ze względów ochrony danych i zapewnia niezawodną ochronę Twoich danych.

- Naciśnij „Skonfiguruj”
- Wybierz opcję, która najbardziej Ci odpowiada
- Dotknij jednej z dwóch opcji (kod PIN lub hasło), a następnie ustaw własną blokadę ekranu
- Upewnij się, że nowe hasło jest nową kombinacją 6 cyfr
- Gdy pojawi się komunikat „Skonfiguruj dane biometryczne”, dotknij „Pomiń”

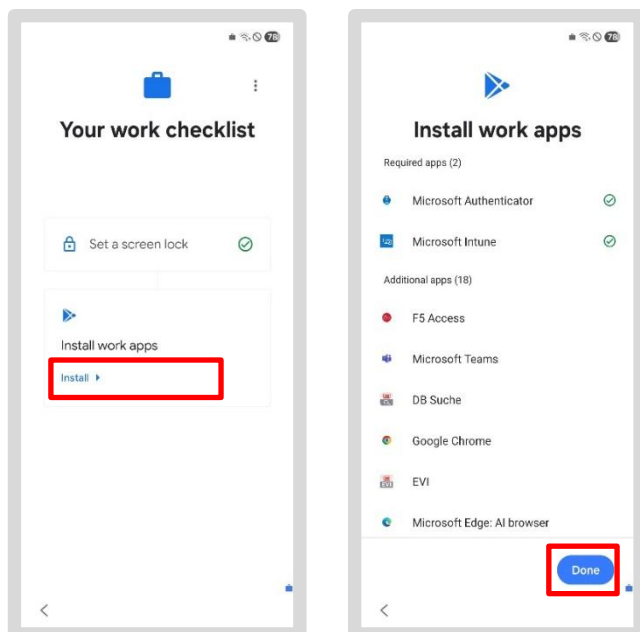


- Zapoznaj się z informacjami dotyczącymi prywatności i użytkowania zawartymi w przewodniku po pierwszej konfiguracji
- Potwierdź, dotykając „Dalej”, a następnie „OK” po dwukrotnym wprowadzeniu hasła
- Jeśli pojawi się ekran „Konta prywatne”: dotknij „Później”, gdy pojawi się monit
- W tym miejscu może pojawić się monit dotyczący usług Google
- > W takim przypadku przejdź do sekcji 5.5: Aktywacja usług Google
- Jeśli ten komunikat się nie pojawi, postępuj zgodnie z instrukcjami jak zwykle
- > Przejdź do sekcji 5.3: Instalowanie aplikacji bazodanowych

5.3 Instalacja aplikacji DB

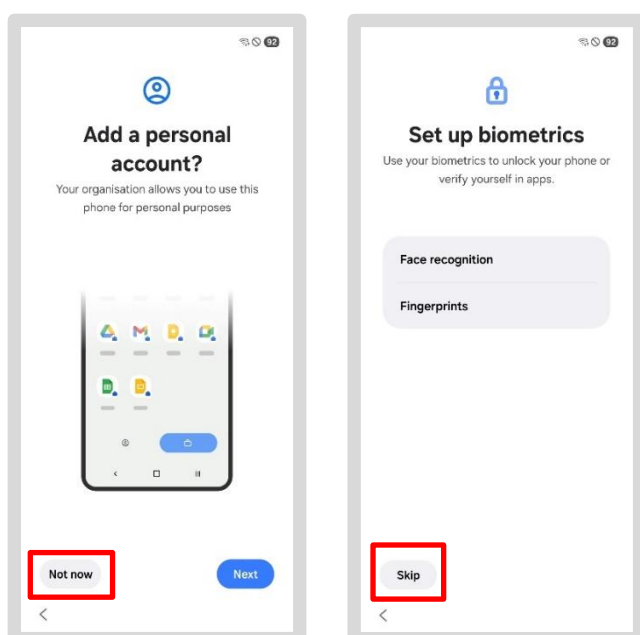
W następnym kroku wszystkie aplikacje DB zostaną ponownie zainstalowane na smartfonie/tablecie DB. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

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



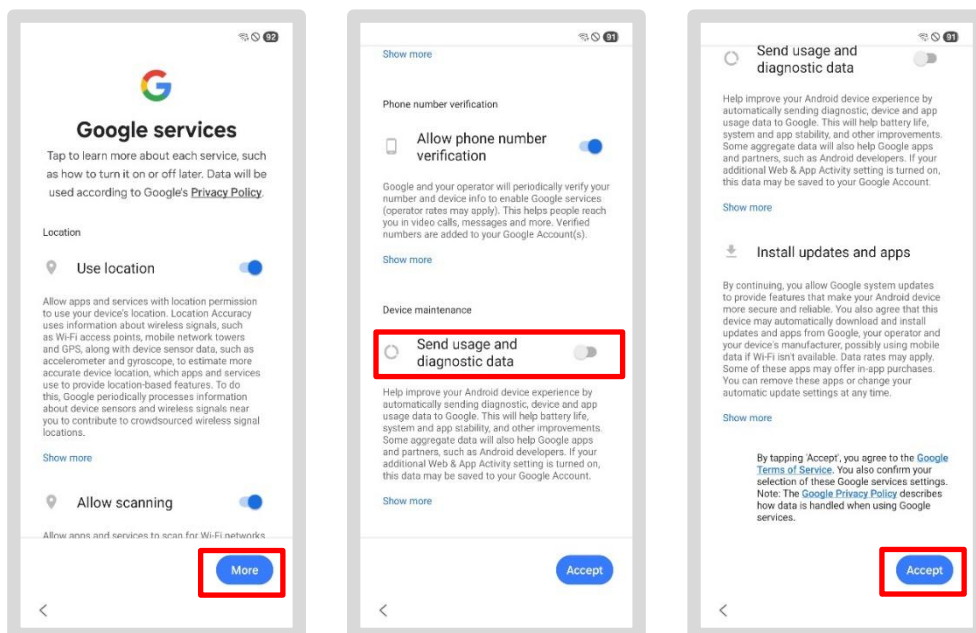
5.4 Konto Google – nie jest wymagane

- **Nie** potrzebujesz **osobistego** konta Google, aby korzystać ze smartfona lub tabletu DB!
- W razie potrzeby możesz to zrobić później
- Więc dotknij „Później”
- Gdy pojawi się komunikat „Skonfiguruj dane biometryczne”, dotknij „Pomiń”



5.5 Włącz usługę Google

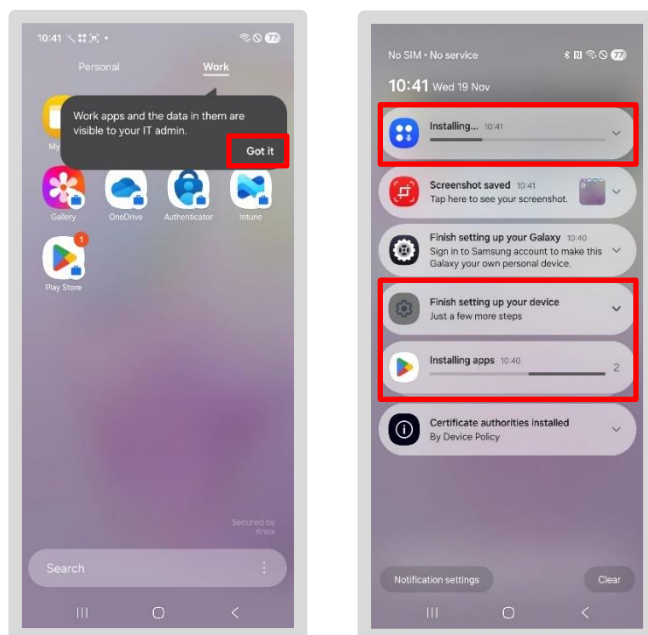
- W sekcji usług Google dotknij „Więcej”
- W sekcji „Wysyłaj dane dotyczące użytkowania i diagnostyki”: dotknij przełącznika dźwigienkowego, aby wyłączyć tę funkcję
- Przewiń w dół, a następnie dotknij „Akceptuj”



> Przejdź do rozdziału 5.6 Automatyczna instalacja aplikacji z DB

5.6 Automatyczna instalacja aplikacji z bazy danych

- Pojawia się następujące ekrany... poczekaj, aż pojawi się ekran główny
- Przesuń palcem w górę od dołu, aby wyświetlić podział na sekcje *Osobiste/Służbowe*
- Naciśnij „OK”
- Przesuń palcem w dół od góry. Powiadomienia w tym miejscu pokażą, czy jakieś aplikacje są nadal pobierane lub instalowane
- Dotknij powiadomienia, a zobaczysz, ile aplikacji pozostało do zainstalowania



- **Uwaga:** Komunikat „Zakończ konfigurację urządzenia” nie jest konieczny do skonfigurowania smartfona/tabletu z systemem DB. Zignoruj go!
- 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. W tym celu przejdź do rozdziału 3 Rozpocznij migrację: Zresetuj smartfon/tablet

Ważne!

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

Pobierz **tymczasową legitymację pracownika DB (TAP)** i wprowadź go w *aplikacji Intune*.

Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku zawartymi w
> Rozdział 6: Aktywacja urządzenia — Utworzenie tymczasowej legitymacji pra-

6 Utwórz tymczasową legitymację pracownika DB (TAP) d

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

- Ważna tymczasowa legitymacja pracownika DB (TAP) – db.de/tap
- nazwa użytkownika DB i hasło DB
- aplikacja Intune

Uwaga:

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

- > **Hasło** do konta **użytkownika DB** można zresetować pod adresem db.de/passwort
- > Instrukcje dotyczące **zmiany hasła** znajdziesz w sekcji „[Zmiana hasła użytkownika DB](#)”
- > Informacje o tym, **jak uzyskać dane użytkownika DB**, znajdziesz w sekcji „[Wymagania wstępne: użytkownik DB](#)”
- > **Nazwę użytkownika DB** można znaleźć w systemie *DeBI* pod adresem: db.de/debi

6.1 Utwórz tymczasową legitymację pracownika DB

- > **Uwaga:** Film instruktażowy znajdziesz pod adresem db.de/mobile-videoanleitung

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

Opcja 1:

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

Opcja 2:

Pomoc może udzielić Ci **współpracownik** z tej samej firmy (np. z DB Sales lub DB Long-Distance), o ile posiada smartfon/tablet DB (lub iPhone'a/iPada) albo komputer BKU/Basic Workplace. Przejdź do:

- > [Rozdział 6.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika](#)

Opcja 3 – Tryb ekspercki:

Masz **tylko jeden smartfon/tablet** i udało Ci się z niego korzystać wystarczająco długo, aby utworzyć tymczasową legitymację pracownika DB przed zresetowaniem urządzenia. Zanotuj swoją legitymację pracownika DB i przejdź do:

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

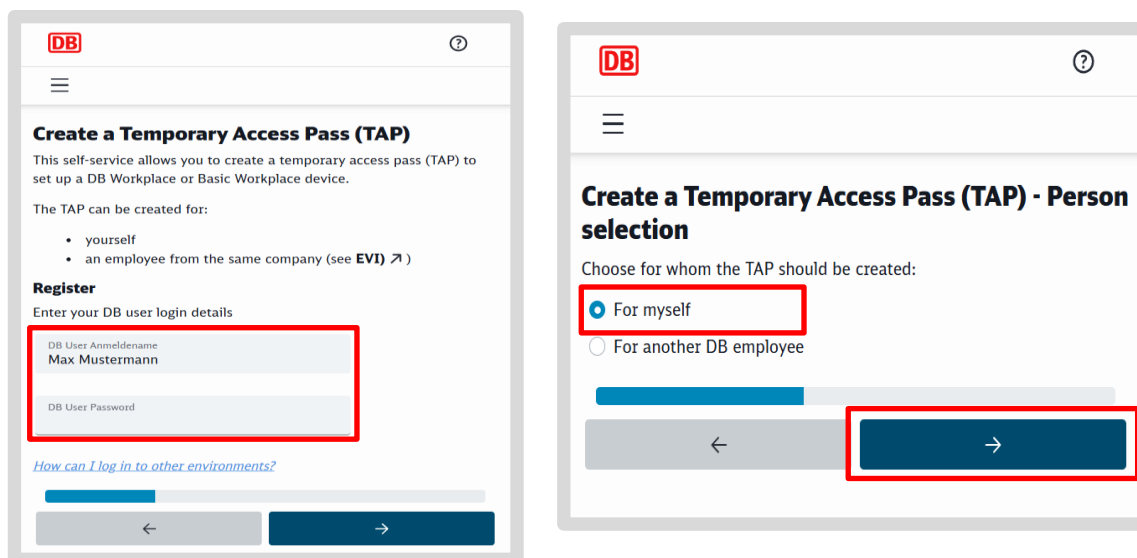
Uwaga: Twój kod Tap jest ważny tylko przez 60 minut i można go używać na wielu smartfonach/tabletach!

Jeśli nadal masz zainstalowaną aplikację Welcome:

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

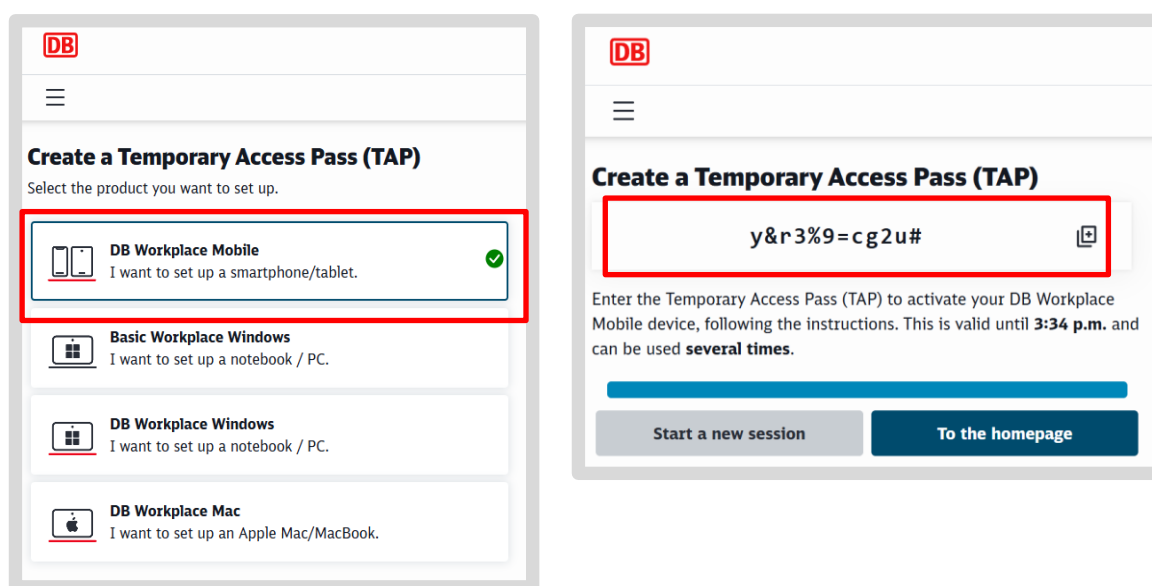
Jeśli nie zainstalowałeś jeszcze aplikacji Welcome:

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



- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku

Uwaga: Będzie on potrzebny później podczas konfiguracji **aplikacji portalu firmowego!**



Ważne!

Kod **TAP** należy wprowadzić wyłącznie w **aplikacji Intune**, nawet jeśli zostaniesz o to poproszony w innej aplikacji DB lub na innym urządzeniu.

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

> Przejdź bezpośrednio do rozdziału 7: Aktywacja urządzenia w DB

Ważne!

Twój smartfon/tablet nie jest jeszcze podłączony do sieci 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 sieci 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 „Welcome”:

- Otwórz aplikację „Welcome” i dotknij opcji „Pomoc”
- Następnie kliknij „Tymczasowa legitymacja pracownika DB (TAP)”, aby ją utworzyć

Jeśli korzystasz z DB Workplace na systemie Windows lub Mac:

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

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen. It includes a title, a description, and options to create a TAP for 'yourself' or 'an employee from the same company (see EVI)'. Below this is a 'Register' section with a red box highlighting the input fields for 'DB User Anmeldenname' (Max Mustermann) and 'DB User Password'. The right screenshot shows the 'Create a Temporary Access Pass (TAP) - Person selection' screen. It has a red box highlighting the selection of 'For another DB employee' and a search bar containing 'Max Mustermann'. Below the search bar, a list of user details is shown: 'DB User: Name: [redacted]', 'E-mail: [redacted]', 'Department: [redacted]', and 'Company: DB Systel GmbH'. A checkbox at the bottom is checked, indicating 'I confirm that I have established the employee's identity.'

- Wybierz właściwą osobę i potwierdź jej tożsamość
- Przekaż kontrolę w aplikacji Teams współpracownikowi (współpracownikom) (jeśli pracujesz zdalnie za pośrednictwem aplikacji Teams)

lub

- Niech kolega skorzysta z komputera
- Pracownik DB wprowadza hasło użytkownika DB
- Następnie wyświetli się legitymacja pracownika DB; **jest ona ważna przez 60 minut i można ją używać na wielu smartfonach/tabletach**
- Jeśli korzystałeś z aplikacji Teams, przejmij ponownie kontrolę nad ekranem
- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku

Issue a Temporary Access Pass (TAP) for Lisa Mustermann

The TAP recipient must now sign in.

Sign in

DB user login name
Lisa Mustermann

DB user password

Important note for recipients: Sign in personally with your DB user credentials. Never share this information with anyone else.

← →

Create a Temporary Access Pass (TAP)

y&r3%9=c g2u#

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 skonfigurowania i aktywacji urządzenia 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 sieci 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 bazie danych

7 Aktywacja urządzenia w bazie danych

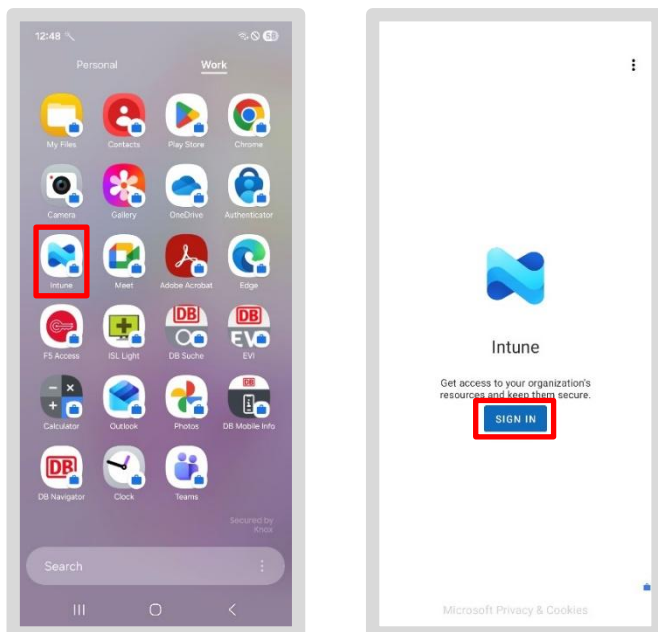
> **Uwaga:** Sprawdź, czy utworzyłeś i otrzymałeś tymczasową legitymację pracownika DB (TAP) zgodnie z opisem w Rozdziale 6: Utwórz tymczasową legitymację pracownika DB (TAP)!

> **Uwaga:** Film instruktażowy można znaleźć pod adresem db.de/mobile-videoanleitung

Otwórz aplikację „Intune”



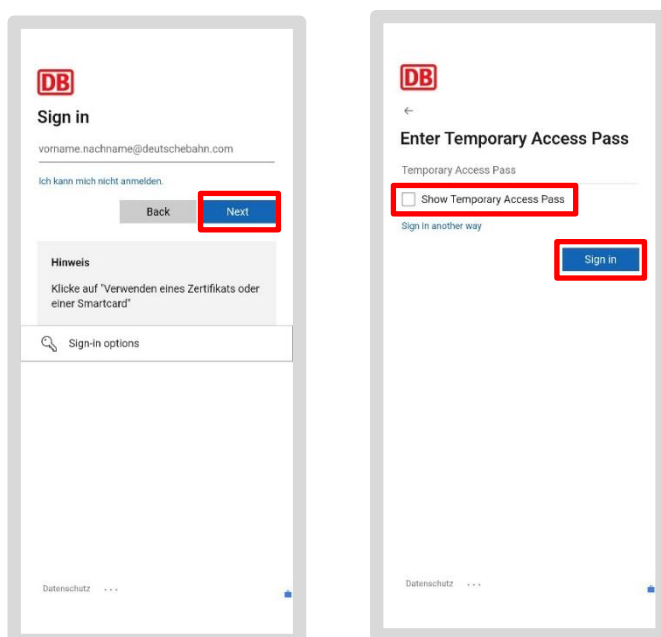
Następnie dotknij przycisku „Zaloguj się”



Wprowadź **adres e-mail użytkownika bazy danych** (nie: nazwa użytkownika bazy danych) i dotknij „Kontynuuj”

Zaznacz pole obok opcji „Pokaż tymczasową legitymację pracownika DB”

Wprowadź tymczasową legitymację pracownika DB i dotknij „Zaloguj się”



Jeśli pojawi się komunikat o błędzie:

- utwórz nowe tymczasowe hasło dostępu i powtórz proces logowania zgodnie z opisem w rozdziale 6: Aktywacja urządzenia – Utworzenie tymczasowej legitymacji pracownika DB (TAP)
- > W przeciwnym razie przejdź do rozdziału 7.1: Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB

Uwaga: Dopóki tymczasowa legitymacja pracownika DB (TAP) jest ważna (w ciągu 60 minut) i otworzysz np. aplikację Outlook, Teams lub IT ServiceDesk, zostaniesz poproszony o podanie tymczasowej legitymacji pracownika DB; wprowadź tutaj również tymczasową legitymację pracownika DB, którą zapisałeś.

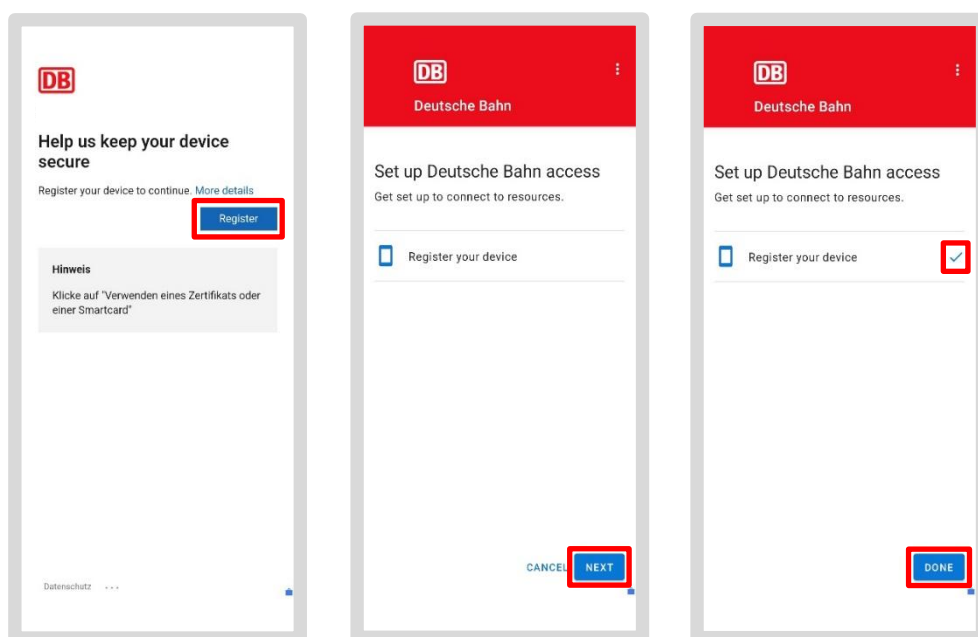
7.1 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB

Trwa konfiguracja dostępu 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 6 „Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)”



Uwaga:

Po rejestracji poczekaj od 5 minut do 1 godziny

, aż wszystkie informacje i certyfikaty zostaną przesłane na smartfon lub tablet. Następnie będzie można korzystać z aplikacji, takich jak *Outlook*, *Teams* itp.

7.2 Aplikacje DB

Uwaga: Wydanie 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 Teams, zostaną pobrane automatycznie.

Następnie zostaną załadowane aplikacje specyficzne dla Twojej firmy lub branży.

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

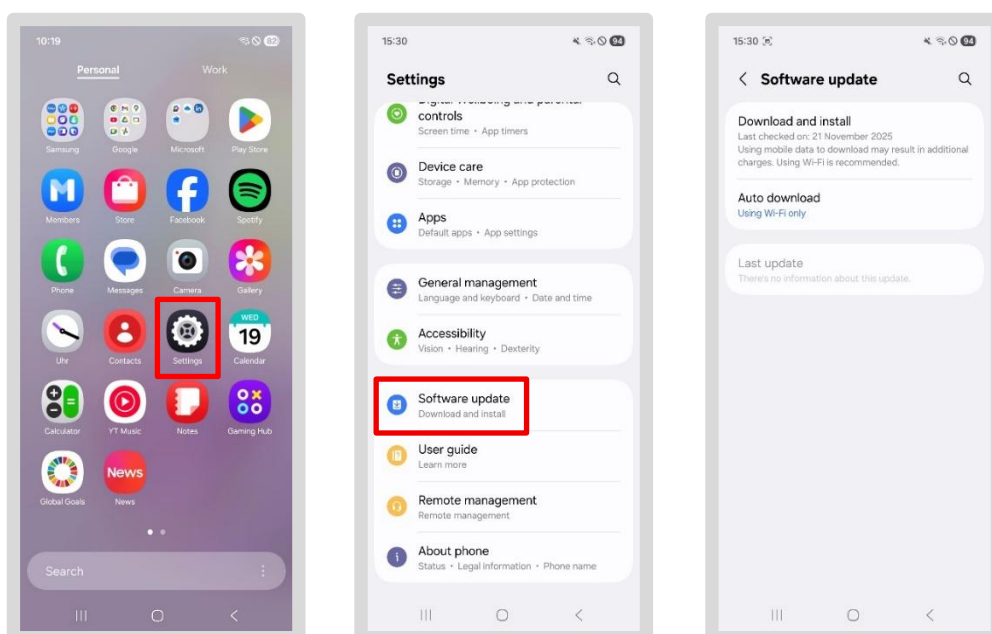
Aplikacja „Welcome” nie jest już dostępna na smartfonie/tablecie DB; zamiast niej znajduje się **aplikacja „DB MOBIL”**, która zawiera wszystkie informacje, przydatne linki i dane dotyczące Twojego smartfona/tabletu DB.

8 Wymagane ustawienia

Uwaga: Wydanie 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

- Na smartfonie/tablecie przejdź do sekcji „Osobiste”
- Naciśnij aplikację „Ustawienia”
- Naciśnij „Aktualizacja systemu”
- Zostanie wyświetlona informacja, czy dostępna jest aktualizacja. Zainstaluj wszystkie oczekujące aktualizacje, dotykając opcji „Zainstaluj aktualizację”

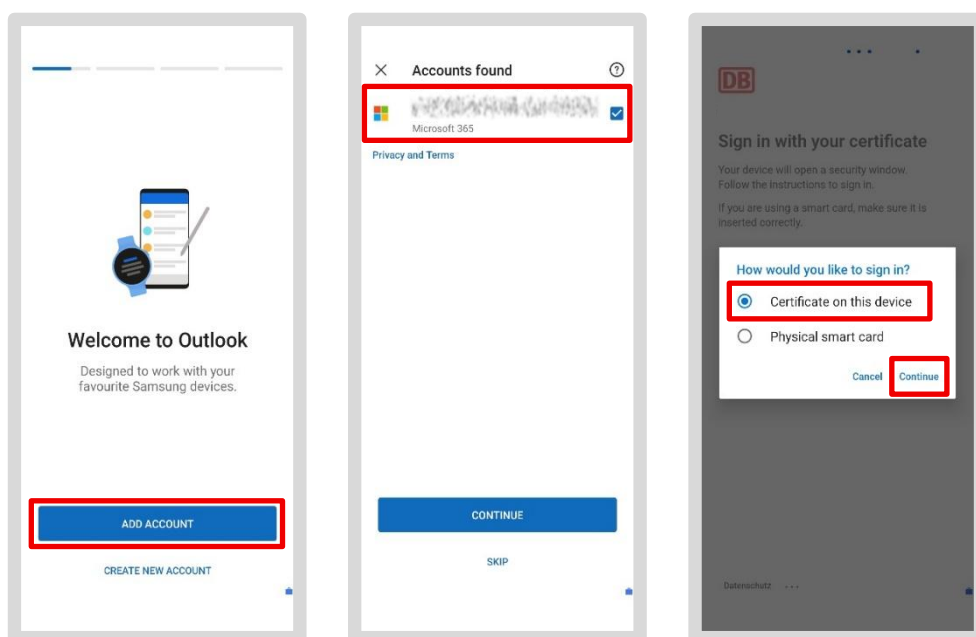


8.2 Outlook

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

> **Uwaga:** Film instruktażowy znajdziesz pod adresem db.de/mobile-videoanleitung

- Przejdź do sekcji „Praca/Biznes” i dotknij aplikacji „Outlook”
- Twoje konto e-mail powinno być już skonfigurowane automatycznie – jeśli nie, dotknij „Dodaj konto”
- W następnym kroku wybierz swój adres e-mail i dotknij „Dalej”



Podczas logowania może pojawić się prośba o podanie kodu TAP:

- Jeśli Twoja tymczasowa legitymacja pracownika DB jest nadal ważna, wprowadź ją tutaj lub utwórz nową zgodnie z opisem w [sekcji 6.1 Tworzenie tymczasowej legitymacji pracownika DB \(TAP\)](#)
- Alternatywnie: wybierz „Wybierz inną opcję logowania”, a następnie „Certyfikat na tym urządzeniu”
- Naciśnij „Wybierz”, gdy pojawi się monit o podanie certyfikatu

Jeśli chcesz wysłać pocztą elektroniczną dane wymagające szczególnej ochrony (np. dane osobowe), musisz również zastosować szyfrowanie w treści wiadomości e-mail

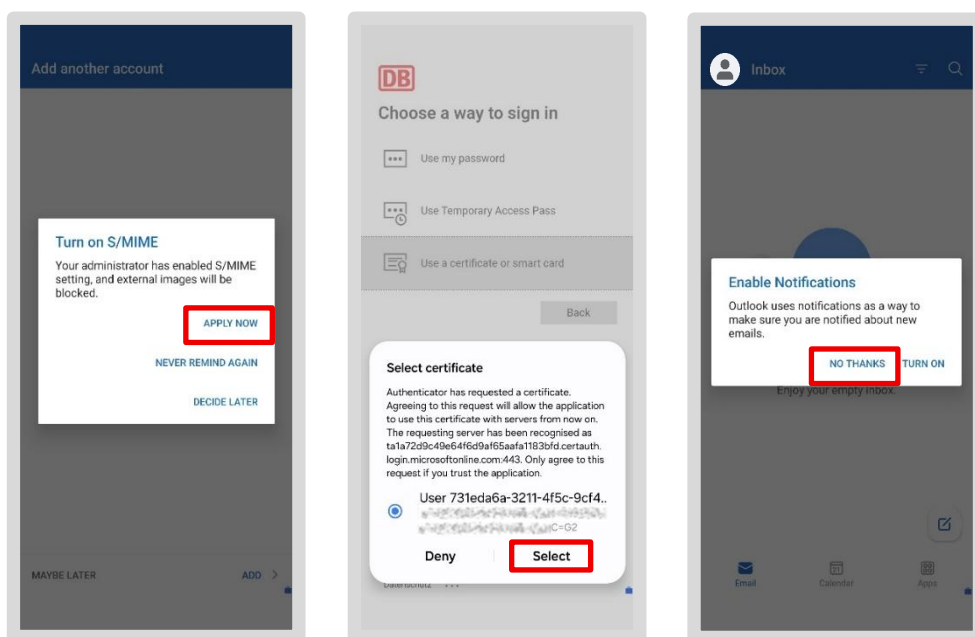
- DB udostępnia w tym celu szyfrowanie S/MIME
- Gdy pojawi się pytanie, czy chcesz włączyć S/MIME, naciśnij „Zastosuj teraz”

Następnie pojawi się monit o certyfikat. Certyfikat, który jest dla Ciebie ważny, możesz rozpoznać w następujący sposób:

- Pierwszy wiersz: „**User** ds2232... (po czym następują cyfry i litery)
- Drugi wiersz: „CN- Nazwa **użytkownika** DB”, np. LisaMustermann 89sd7es0ßwd (po czym następują cyfry i litery)
- Zaznacz ten fragment tekstu i naciśnij „Wybierz”

Twoje konto e-mail jest teraz konfigurowane:

- Gdy pojawi się pytanie, czy chcesz dodać kolejne konto, dotknij „Może później”
- Następnie naciśnij „Nie, dziękuję”, aby wyłączyć powiadomienia



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

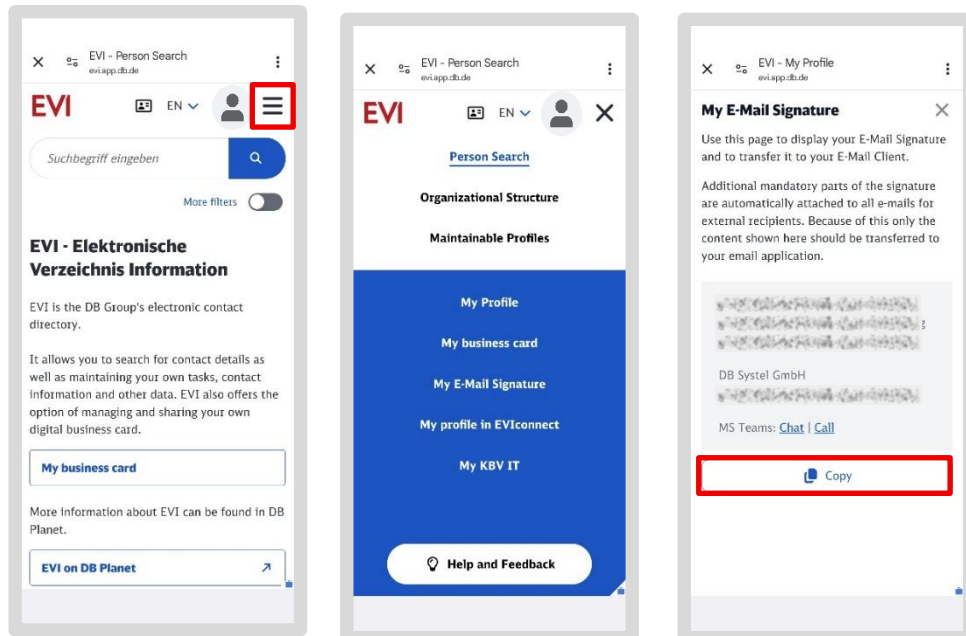
Android 16: Na smartfonach/tabletach z systemem Android 16 można pominąć krok aktywacji S/MIME. W takim przypadku musisz zakończyć konfigurację aplikacji Outlook i uruchomić ją ponownie! Pojawi się wtedy monit o aktywację.

8.2.2 Skonfiguruj podpis e-mailowy

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 oraz oficjalna siedziba firmy w DB. Tekst podpisu e-mailowego znajdziesz w centralnym katalogu DB, znanym jako „EVI”.

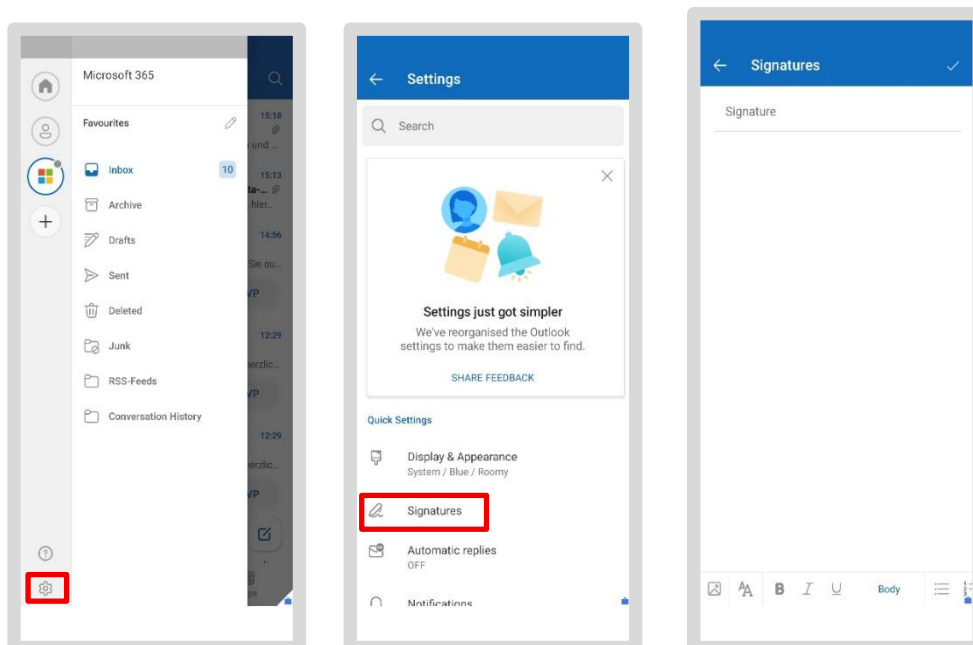
Oto jak pobrać podpis e-mailowy z EVI:

- Otwórz aplikację EVI
- Naciśnij trzy linie w prawym górnym rogu obok zdjęcia profilowego
- Następnie dotknij opcji „Mój podpis e-mailowy”
- Twój osobisty podpis wyświetli się w szarym polu. Skopiuj go, klikając „Kopiuj”



Wklej podpis do aplikacji Outlook:

- Otwórz aplikację Outlook i dotknij swojego zdjęcia profilowego w lewym górnym rogu
- Dotknij ikony koła zębatego w lewym dolnym rogu
- Teraz dotknij „Podpis”



- Otworzy się pole na podpis. Jeśli znajduje się tam już wpis, usuń go, dotykając opcji „✕”

- Teraz naciśnij i przytrzymaj 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 nowych wiadomości e-mail

Uwaga: Jeśli skonfigurowałeś wiele kont e-mail, możesz użyć suwaka „Podpis dla każdego konta”, aby ustawić osobny 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 połączonym kontem Office. Oznacza to, że bez względu na to, jakiego smartfona lub tabletu używasz – czy to iPhone'a, iPada, komputera BKU czy komputera Basic Workplace – zawsze będziesz na bieżąco.

8.3 Aplikacja MS Defender – należy ją uruchomić

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 zainstalowane aplikacje w poszukiwaniu złośliwego oprogramowania. Aby aktywować ochronę, wystarczy raz otworzyć aplikację.

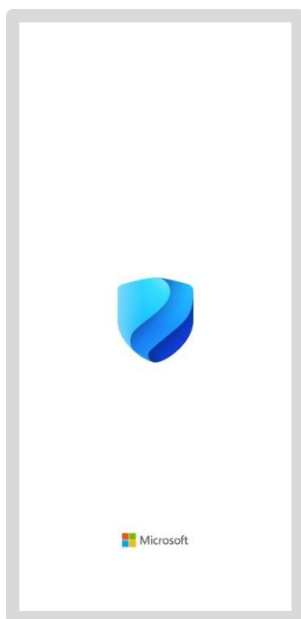
Ze względu na dużą różnorodność smartfonów i tabletów DB mogą występować niewielkie różnice w opisie poszczególnych kroków.

8.3.1 Konfiguracja aplikacji MS Defender

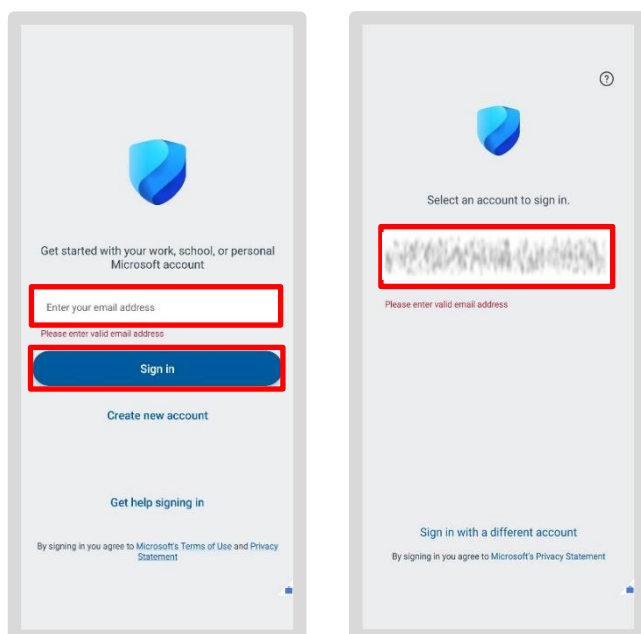
Aby skonfigurować aplikację MS Defender na smartfonie lub tablecie, należy wykonać następujące czynności:

- Przejdź do sekcji „Praca/Biznes” i otwórz „Sklep Google Play”
- Wyszukaj aplikację „Microsoft Defender: Antivirus” i dotknij opcji „Zainstaluj”

- Dotknij ikony *aplikacji MS Defender*, aby ją otworzyć

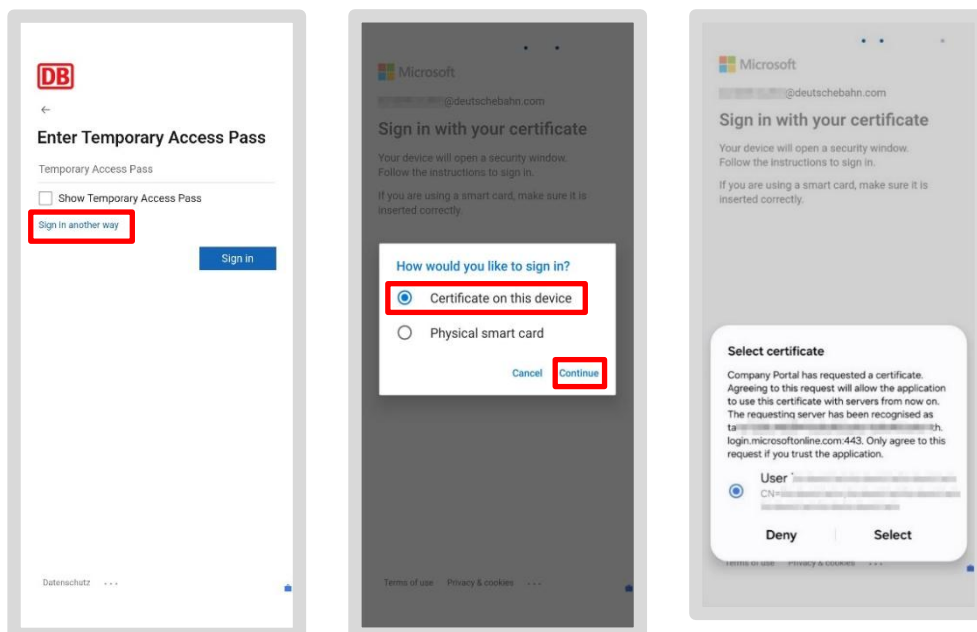


- Zostaniesz poproszony o podanie służbowego adresu e-mail
- Naciśnij przycisk „Zaloguj się” lub aplikacja automatycznie przeniesie Cię do następnego ekranu, na którym wyświetli się Twój adres e-mail
- Naciśnij swój służbowy adres e-mail



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

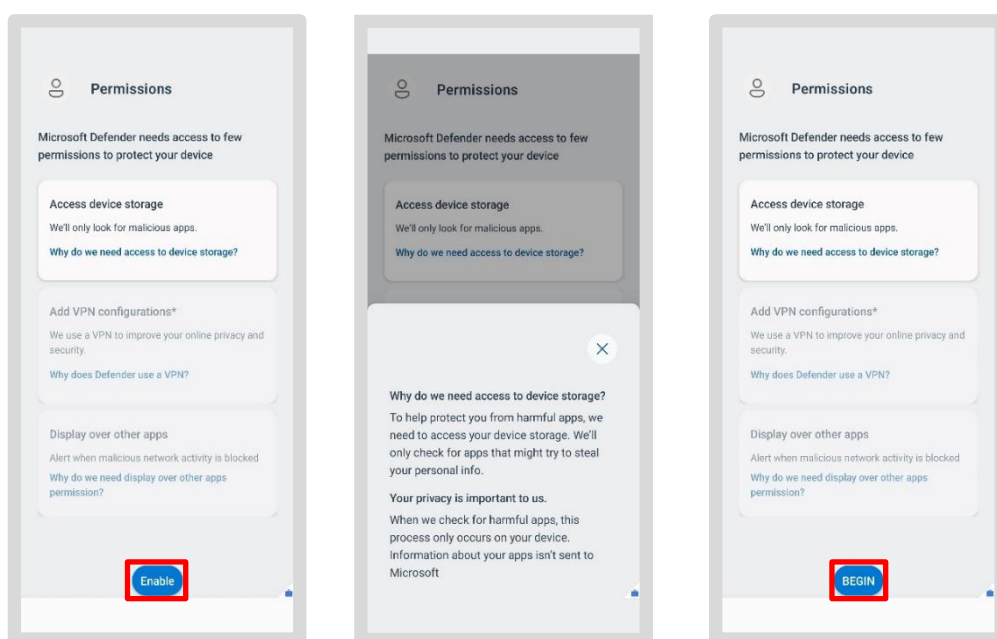
- Naciśnij „Zaloguj się inną metodą”
- Gdy pojawi się monit, dotknij opcji „*Certyfikat na tym urządzeniu*”, a następnie dotknij „Dalej”
- Wybierz certyfikat



8.3.2 Przyznaj uprawnienia

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

- Naciśnij „Aktywuj”
- Następnie dotknij „Start”
- Otworzy się aplikacja „*Ustawienia*” na smartfonie/tablecie

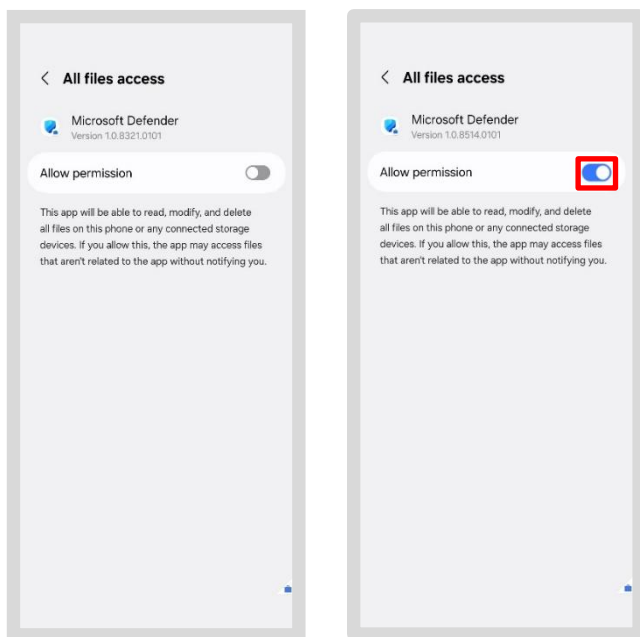


Informacje ogólne dotyczące uprawnień:

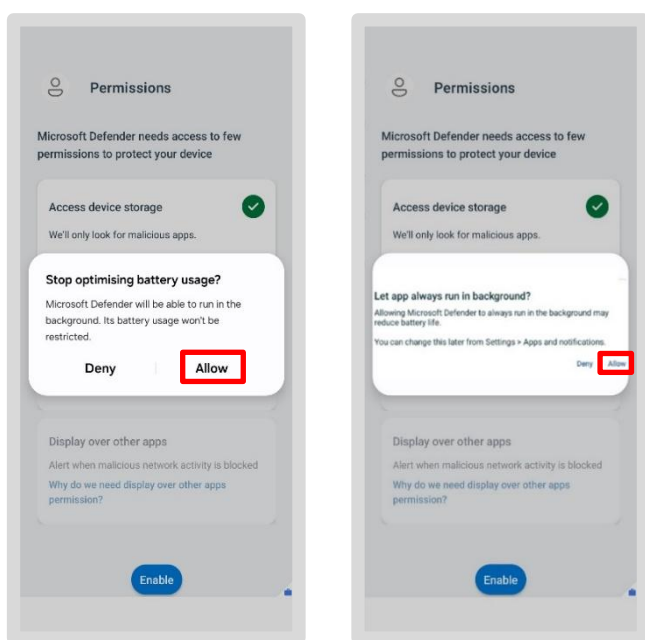
Uprawnienia te są niezbędne do prawidłowego działania aplikacji oraz zapewnienia bezpieczeństwa urządzenia.

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

- Teraz przesunij suwak w prawo, aby przyznać uprawnienie
- Po wyświetleniu monitu dotknij „Zezwól”



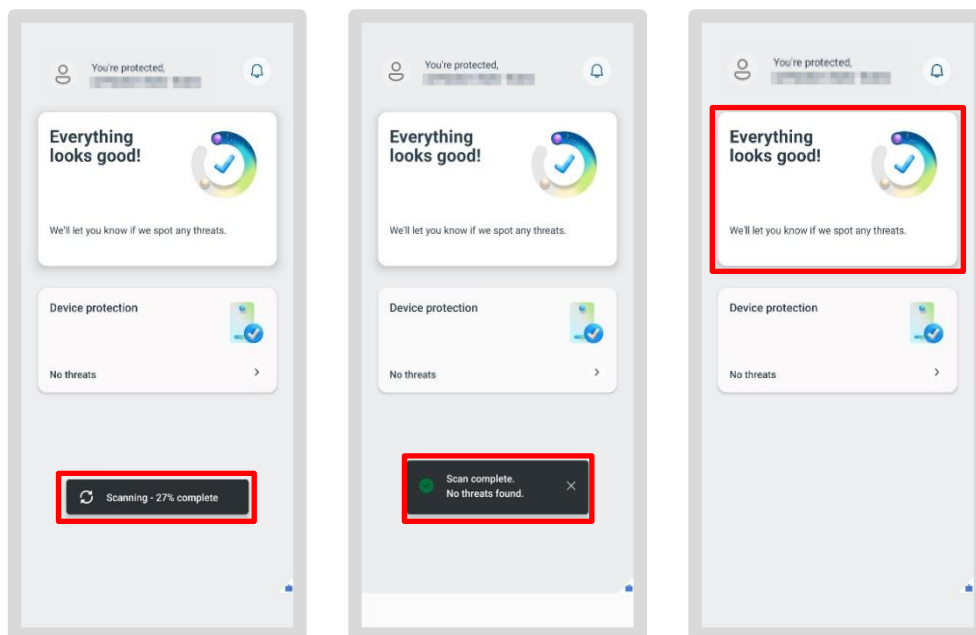
- W przypadku wszystkich kolejnych monitów wybierz „Zezwól”



Uwaga: W zależności od typu urządzenia mogą zostać wyświetlone prośby o inne uprawnienia! W związku z tym może pojawić się tylko jeden z pokazanych komunikatów.

Następnie zostaniesz przeniesiony na ekran główny aplikacji MS Defender. Skanowanie smartfona/tabletu w poszukiwaniu złośliwego oprogramowania rozpocznie się automatycznie od razu. Podczas skanowania wyświetlane będą informacje o postępie.

Wynik zostanie wyświetlony na ekranie głównym. Jeśli widoczny jest zielony znaczek, oznacza to, że nie wykryto złośliwego oprogramowania.



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

8.4 DB M 365

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

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

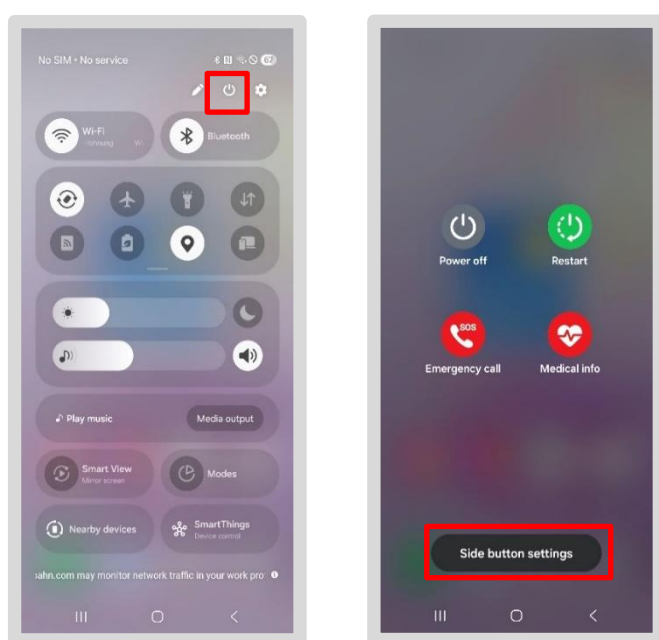


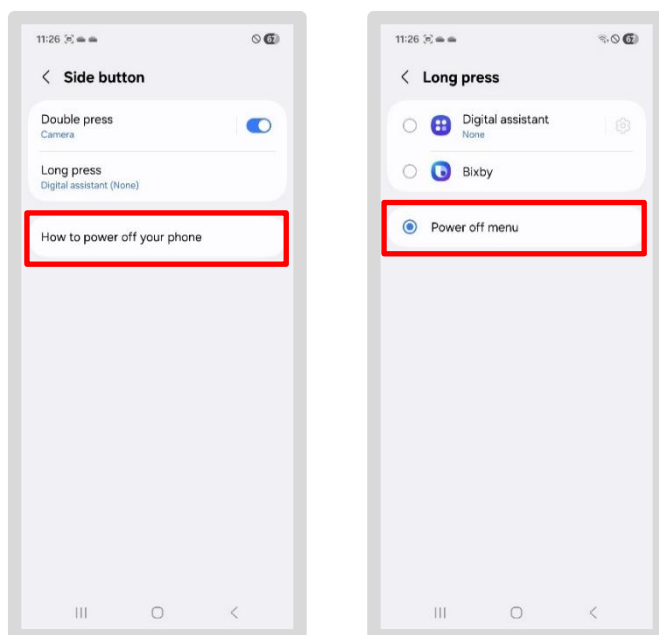
- Następnie dotknij „Zainstaluj”
- Po otwarciu pliku aplikacja uruchomi się automatycznie

Uwaga: Można otworzyć tylko jeden plik na raz. Nie jest możliwe, na przykład, jednoczesne otwarcie kilku plików Word.

8.5 Wyłącz przycisk Bixby

- Domyślnie przycisk zasilania uruchamia asystenta głosowego Bixby. Ze względów bezpieczeństwa należy tę funkcję wyłączyć:
- Przesuń palcem raz w dół od góry ekranu. Otworzy się Centrum sterowania
- Dotknij ikony zasilania w prawym górnym rogu, obok ikony ustawień
- Wybierz opcję „Ustawienia klawiszy skrótów”
- Zmień funkcję w opcji „Długie naciśnięcie” na „Menu wyłączania”

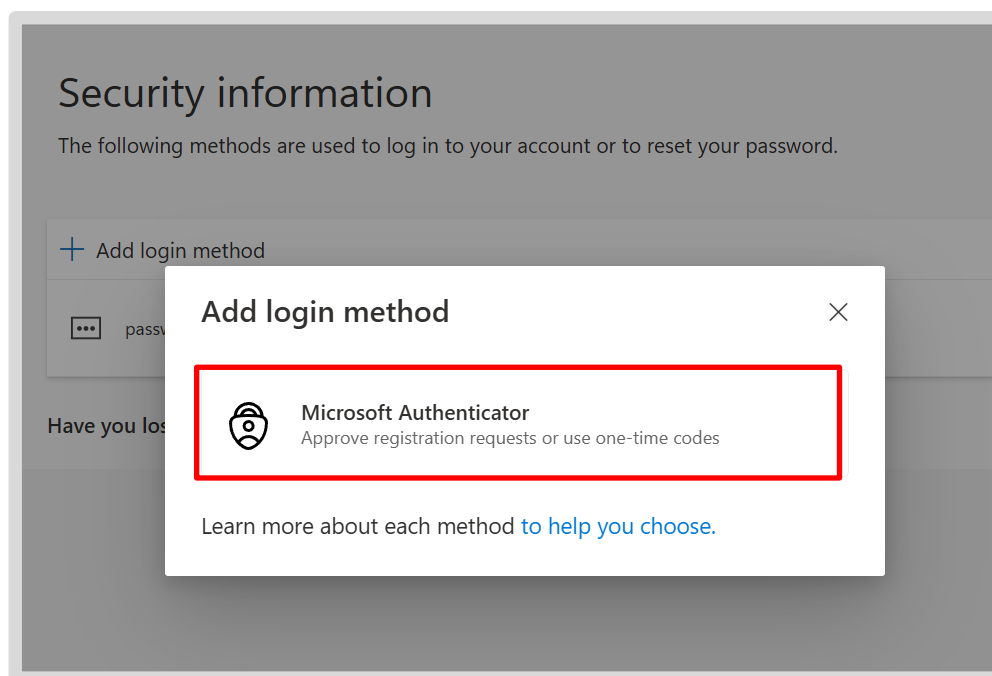




8.6 Ponownie aktywuj aplikację Microsoft Authenticator do uwierzytelniania

Jeśli korzystałeś z aplikacji Authenticator do uwierzytelniania, wykonaj następujące czynności:

- Kliknij „db.de/authenticator” na komputerze BKU lub Basic Workplace
- Naciśnij „ikonę *plusa*”, a następnie 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, naciśnij przycisk „Przewodnik po konfiguracji uwierzytelniania wieloskładnikowego” i postępuj zgodnie z podanymi wskazówkami
- Następnie możesz używać aplikacji Microsoft Authenticator do uwierzytelniania na smartfonie lub tablecie
- Jeśli korzystałeś z **aplikacji Authenticator do uwierzytelniania na stronach internetowych lub w narzędziach**, ponownie aktywuj 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, a następnie postępuj zgodnie z instrukcjami.

Gratulacje!

Pomyślnie przeprowadziłeś migrację służbowego smartfona/tabletu!

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

> Informacje o tym, jak zapisać kontakty w usłudze OneDrive i zaimportować je z powrotem, znajdziesz w przewodniku konfiguracji w sekcji „Tworzenie kopii zapasowej kontaktów w usłudze OneDrive”

> Szczegółowy przewodnik konfiguracji znajdziesz pod adresem db.de/mobile-setup