



Wersja systemu operacyjnego z Androida 15

Samsung Recovery

DB Workplace Mobile

DB Systel GmbH | 15.10.2026

Spis treści

1 Niezbędne kroki przed powrotem do zdrowia	4
1.1 Kopia zapasowa danych	4
1.2 Aplikacja Authenticator – opcjonalna	4
1.3 Utwórz tymczasowy dostęp (TAP) – tryb ekspercki	4
2 Rozpocznij odzyskiwanie: Zresetuj smartfon/tablet	7
2.1 Samodzielnie zresetuj swój smartfon/tablet	7
2.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk	8
3 Konfiguracja ponownie w Microsoft Intune	9
3.1 Wybrany język	9
3.2 Zgoda na umowę licencyjną użytkownika końcowego	10
3.3 Konfiguracja Wi-Fi	11
3.4 Konfiguracja Wi-Fi w budynku DB	12
4 Zaloguj Samsunga do bazy danych	13
4.1 Ustaw swój profil pracy	14
4.2 Ustaw blokadę ekranu	15
4.3 Instalacja aplikacji bazy danych	16
4.4 Konto Google – Niepotrzebne	16
4.5 Aktywuj usługę Google	17
4.6 Kompletny zestaw – opcjonalny	18
5 Aktywuj urządzenie - Utworzenie tymczasowego dostępu (TAP)	19
5.1 Co jest konieczne do stworzenia Tymczasowego Przepustki Dostępu (TAP)	19
5.2 Utworzenie tymczasowego dostępu (TAP)	19
5.3 Utworzenie tymczasowej przepustki dostępu dla kolegi	22
6 Aktywuj swoje urządzenie za pomocą Tymczasowej Przepustki Dostępu (TAP)	24
6.1 Ustaw dostęp do wszystkich aplikacji i stron internetowych bazy danych	26
6.2 Aplikacje bazy danych	27
7 Niezbędne ustawienia	28
7.1 Instalacja aktualizacji systemu Android	28
7.2 Aplikacja MS Defender – wymagana aktywacja	28
7.3 Konfiguracja Outlooka / tworzenie konta e-mail / szyfrowanie poczty	33
7.3.1 Outlook: Konfiguracja podpisu e-mailowego	35
7.3.2 Outlook: Synchronizuj e-maile	36

7.3.3 Outlook: Utwórz nowe kontakty w	37
7.3.4 Outlook: Synchronizacja kontaktów	37
7.4 DB M 365	38
7.5 Wyłącz przycisk Bixby	38
7.6 Ponownie włącz aplikację Microsoft Authenticator	39

1 Niezbędne kroki przed powrotem do zdrowia

Jeśli Twój służbowy smartfon/tablet ma problemy takie jak wolna wydajność, zawieszanie się lub częste awarie, pomocne jest przywrócenie ustawień fabrycznych. Następujące kroki są konieczne:

1.1 Kopia zapasowa danych

Aby to zrobić, postępuj zgodnie z następującymi krokami:

- a) Zrób kopię zapasową danych i ustawień pracy
- b) Zabezpiecz swoje prywatne dane i ustawienia

- > Instrukcje można znaleźć w mobileworkplace.deutschebahn.com/mobile-daten-sichern
- > Poradnik wideo znajdziesz na: db.de/mobile-videoanleitung

1.2 Aplikacja Authenticator – opcjonalna

Uwaga: Informacje te dotyczą wyłącznie użytkowników, którzy aktywnie korzystają z *aplikacji Authenticator*, np. do dostępu administracyjnego z tzw. kontem dwuosobowym lub do uwierzytelniania wieloskładnikowego, np. dla VPN z podstawowym adresem MAC Workplace.

- **Uwaga:** Nie będziesz mógł *korzystać* z aplikacji Authenticator podczas procesu odzyskiwania
 - Nie są potrzebne dalsze kroki
 - Po przywróceniu aplikacji trzeba ją ponownie włączyć
- > Przejdź do [Rozdział 7.6 Ponowne włączenie aplikacji Microsoft Authenticator](#)

Jeśli podczas odzyskiwania konieczne jest użycie *aplikacji Authenticator*, użyj innego smartfona/tabletu, aby połączyć go z aplikacją *Authenticator*. Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku:

- > [Konfiguracja uwierzytelniania wieloskładnikowego \(MFA\)](#)

1.3 Utwórz tymczasowy dostęp (TAP) – tryb ekspercki

Po zrobieniu kopii zapasowej danych są dwie opcje:

Twój smartfon/tablet już w ogóle nie działa:

- > Przejdź do [rozdziału 2.2 Resetowanie smartfona/tabletu za pomocą aplikacji IT ServiceDesk](#)

Smartfon/tablet działa częściowo:

- > **Uwaga:** Poradnik wideo znajdziesz na db.de/mobile-videoanleitung

Kontynuuj na następnej stronie!

Aby utworzyć tymczasowy dostęp (TAP):

- Otwórz domyślną przeglądarkę i przejdź do db.de/tap
- Wprowadź swoją nazwę użytkownika do bazy danych oraz hasło użytkownika do bazy danych
- Wybierz dla siebie i stuknij niebieski przycisk
- Teraz wybierz "DB Workplace Mobile"
- Następnie zobaczysz Tymczasową Przepustkę Dostępu (TAP)
- Zapisz Tymczasową Przepustkę Dostępu (TAP) na kartce papieru lub zeszyście

Uwaga: TAP jest obecnie ważny przez 60 minut i na wielu smartfonach/tabletach.

Ważne!

The **TAP** może być używany tylko w **Aplikacja Intune** nawet jeśli zostaniesz poproszony o to w innej aplikacji bazy danych lub na innym smartfonie/tablecie.

- Będziesz go potrzebować później, po zresetowaniu telefonu/tabletu
 - Masz wystarczająco dużo czasu, żeby zresetować smartfon/tablet
- > Przejdź bezpośrednio do rozdziału 2.1 Samodzielne resetowanie smartfona/tabletu

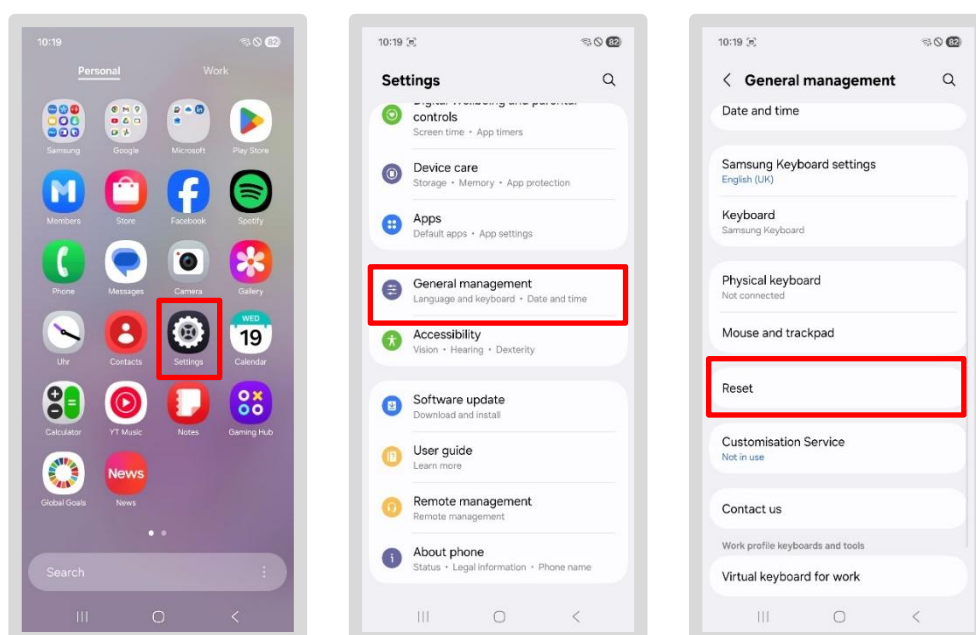
2 Rozpocznij odzyskiwanie: Zresetuj smartfon/tablet

Uwaga: Poniższe ekrany mogą mieć różny wyświetlacz w zależności od modelu urządzenia smartfona/tabletu.

2.1 Samodzielnie zresetuj swój smartfon/tablet

> **Uwaga:** Znajdziesz samouczek wideo pod db.de/mobile-videoanleitung

- Na telefonie/tablecie przejdź do sekcji Prywatne
- Otwórz aplikację Ustawienia
- Administracja Generalna Tap
- Przewijaj dalej w dół i kliknij Reset



- Następnie wybierz "Przywrócenie ustawień fabrycznych"
- Zobaczysz wskazówkę, co reset usuwa
- Sprawdź, czy zrobiłeś kopię zapasową danych z pracy (instrukcje: Kopia zapasowa danych)
- Następnie naciśnij przycisk "Reset", wejdź blokadę ekranu i "Usuń wszystko".
- Poczekaj kilka minut, urządzenie automatycznie się zresetuje

> Następnie przejdź do rozdziału 3 Re-Setup w Microsoft Intune

2.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk

Jeśli Twój smartfon/tablet przestaje działać, wybierz ten krok:

- Otwórz aplikację IT ServiceDesk i wpisz zamówienie na resetowanie smartfona/tabletu w sekcji "Nowe żądanie usługi"
- Jeśli nie możesz otworzyć aplikacji, wybierz ten numer:
 - IT ServiceDesk
 - Wewnętrzne: Tel. 91-5555
 - Zewnętrznie: Tel. 0361 430 8200
 - Wybierz tutaj pozycję menu 0
 - IT ServiceDesk DB Cargo
 - Tel. 91 7777 (wewnętrznie)
 - Tel. 00800 327 978 35 (zewnętrznie)
 - Wybierz tutaj pozycję menu 0
- Jeśli pojawią się inne rzeczy, pomyśl o tym wcześniej:
 - Gdzie pojawiły się **problemy?**
 - **Określ lokalizację usterki;** aby zapewnić szybsze wsparcie
 - **W przypadku problemów z certyfikatami:** Czekaj po rejestracji **od 5 minut do 24 godzin** Dopóki wszystkie informacje i certyfikaty nie zostaną przeniesione na smartfon/tablet.

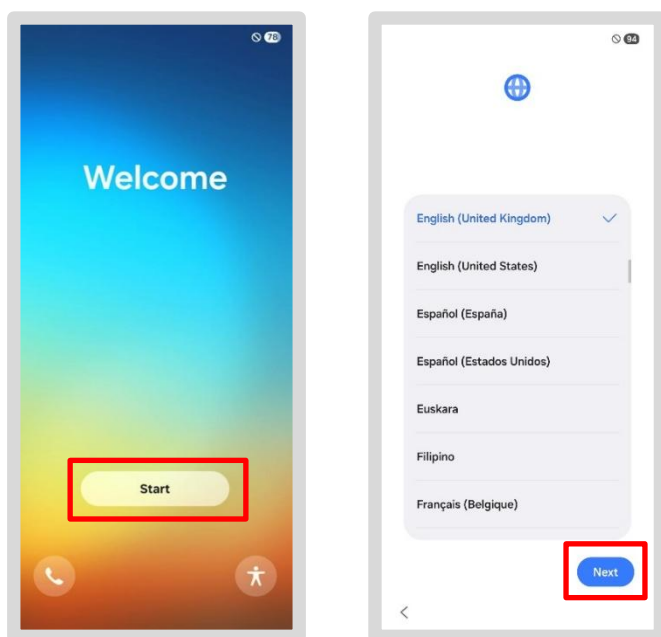
> Następnie przejdź do rozdziału 3 Re-Setup w Microsoft Intune

3 Konfiguracja ponownie w Microsoft Intune

3.1 Wybrany język

> **Uwaga:** Znajdziesz samouczek wideo pod db.de/mobile-videoanleitung

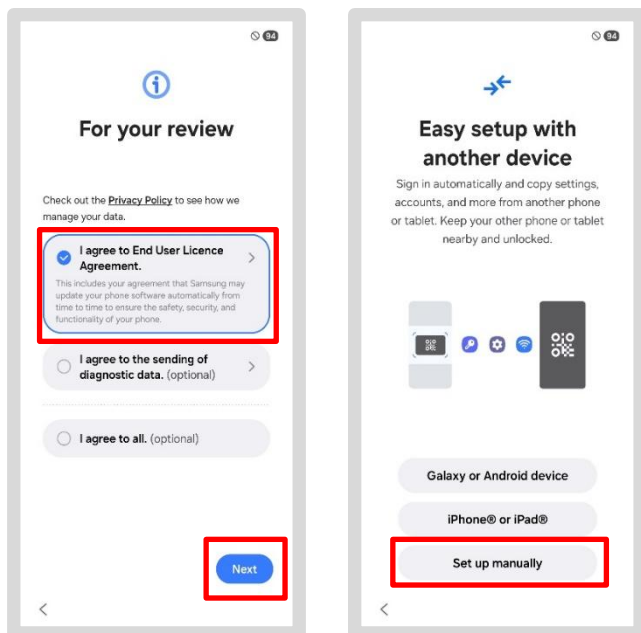
- Trzymaj tablet w **trybie pionowym** , aby ekrany były tak samo jak w instrukcji
- Włącz smartfon/tablet
- Upewnij się, że Twój telefon/tablet jest podłączony do zasilania lub ma wysoki poziom baterii podczas procesu przywracania
- Tap Start
- Na następnym ekranie wybierz język, który chcesz wybrać spośród wybranych, i kliknij Dalej



> Przejdź do Rozdział 3.2 Zgoda na umowę licencyjną użytkownika końcowego

3.2 Zgoda na umowę licencyjną użytkownika końcowego

- Wystarczy kliknąć "Zgadzam się na umowę licencyjną użytkownika końcowego", a następnie kliknąć na "Następny"
- Stuknij w "Konfiguruj z innym urządzeniem" na "Konfiguruj ręcznie"



> przejdź do rozdziału 3.3 Konfiguracja Wi-Fi

3.3 Konfiguracja Wi-Fi

Aby skonfigurować swoją sieć Wi-Fi, wybierz jedną z następujących opcji:

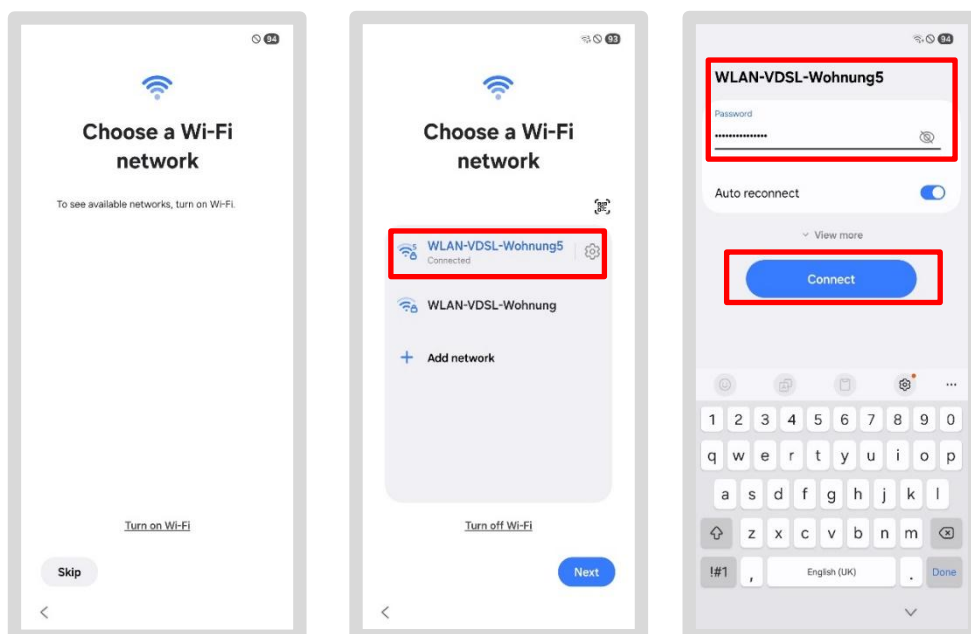
- Korzystaj z **danych mobilnych** , jeśli masz kartę SIM w smartfonie/tablecie (może to być objęte opłatą!)
- Ustaw hotspot na swoim prywatnym smartfonie/tablecie

lub

- Użyj hotspotu ze smartfona DB kolegi
- Korzystaj z prywatnego Wi-Fi, jeśli pracujesz z domu

Wybierając inną sieć Wi-Fi, należy postępować następująco:

- Dotknij wybranej sieci Wi-Fi
- Wprowadź swoje dane uwierzytelniające i kliknij Connect
- Aby uzyskać drugą prośbę, naciśnij Kontynuuj



Gdy tylko Twój smartfon/tablet zostanie połączony z Wi-Fi, rozpoczyna się połączenie z siecią bazy danych.

> przejdź do rozdziału 4 Logowanie Samsunga do bazy danych

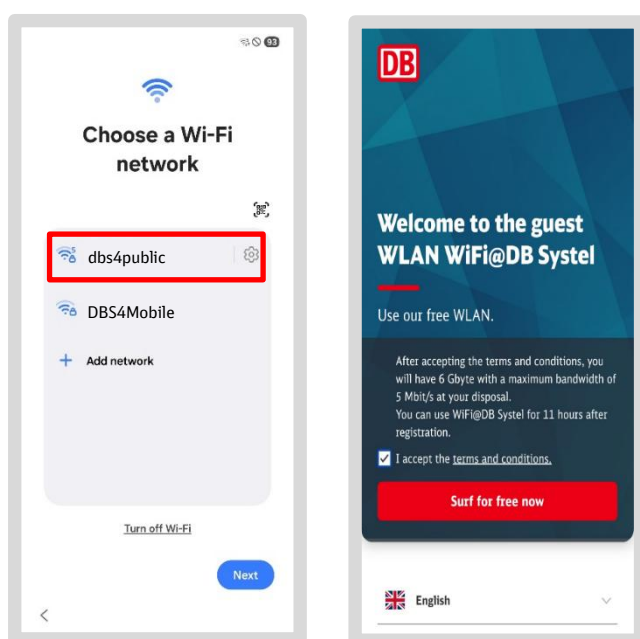
3.4 Konfiguracja Wi-Fi w budynku DB

Ponieważ WLAN "dbs4public" nie zawsze działa zadowalająco w budynkach DB, zalecamy wybranie jednego z następujących kroków:

> Rozdział 3.3 Konfiguracja Wi-Fi

Jeśli mieszkasz w budynku **bazy danych** i chcesz korzystać z Wi-Fi "dbs4public", postępuj zgodnie z tymi krokami:

- Stuknij w sieć Wi-Fi "dbs4public"
- Otworzy się dialog dialogowy, zaakceptuj warunki
- Kliknij darmowe przeglądanie już teraz
- Stuknij Zamknij



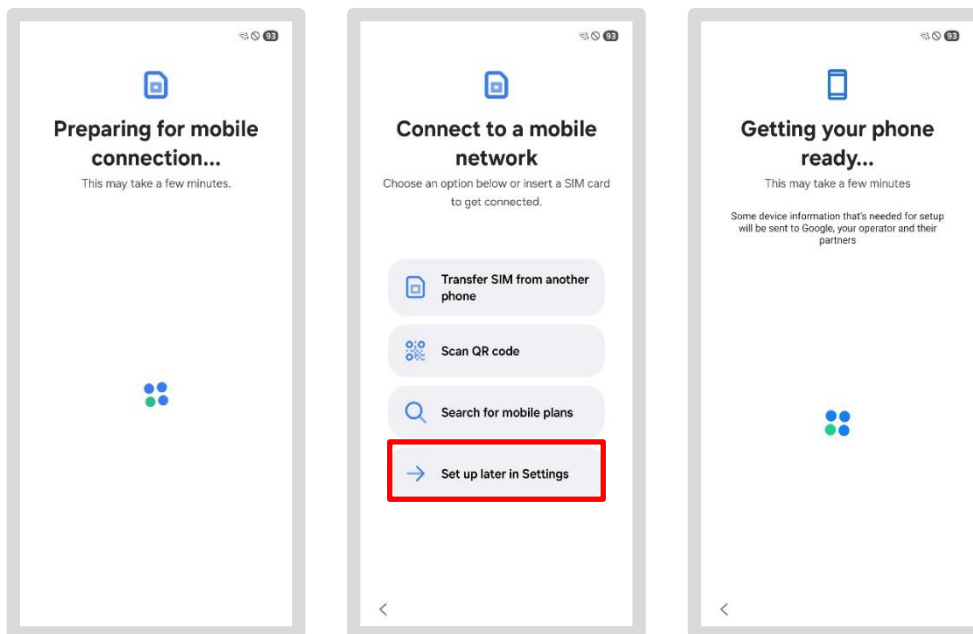
Gdy tylko Twój smartfon/tablet zostanie połączony z Wi-Fi, rozpoczyna się połączenie z siecią bazy danych.

> przejdź do rozdziału 4 Logowanie Samsunga do bazy danych

4 Zaloguj Samsunga do bazy danych

W kolejnym kroku Twój smartfon/tablet bazy danych musi być połączony z *Zarządzaniem bazą danych* (dokładniej w Enterprise Mobility Management, w skrócie EMM). Czekaj na zmianę informacji, aż pojawi się instrukcja. W zależności od połączenia sieciowego, ekrany będą syczeć lub się zmieniać.

- Trzymaj tablet w **trybie pionowym**, jeśli do tej pory trzymałeś go w trybie poziomym
- Obecnie indywidualne ekrany się zmieniają
- Tap "Setup After", Niektóre ekrany są teraz wyświetlane ponownie bez konieczności wykonywania jakichkolwiek działań

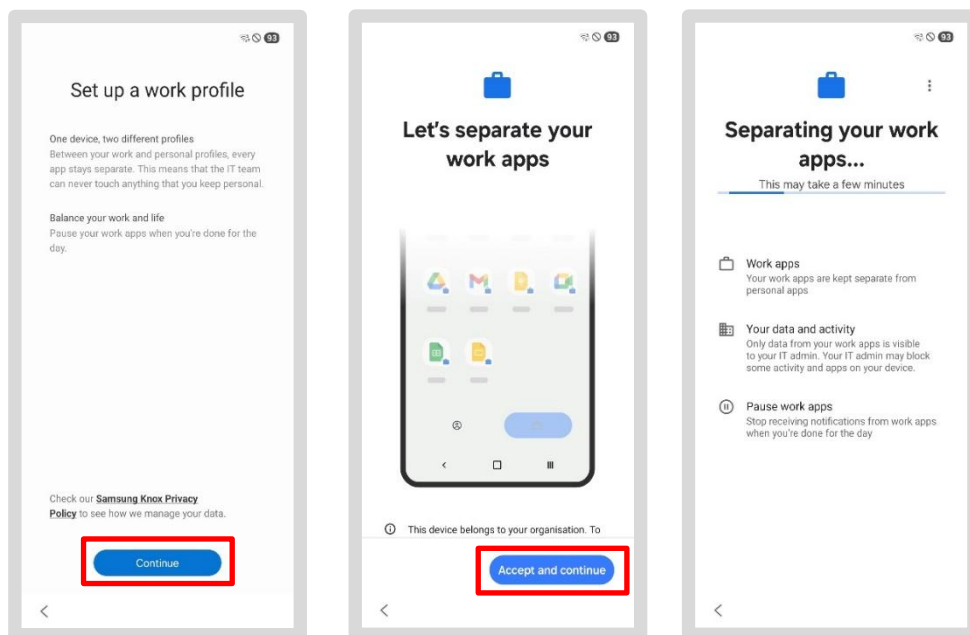


> przejdź do rozdziału 4.1 Tworzenie profilu pracy

4.1 Ustaw swój profil pracy

Aby aplikacje służbowe były przypisane na smartfonie/tablecie, potrzebujesz profilu służbowego. Należy go skonfigurować tutaj:

- Smartfon/tablet jest skonfigurowany
- Potwierdź następujące zapytanie za pomocą "Następny"
- Gdy pojawi się "Ustaw profil pracy", kliknij Dalej lub Zgodzi się
- Jeśli zobaczysz "Administrator IT może kontrolować to urządzenie i blokować aplikacje" (tekst może być odcięty), kliknij "Następny"

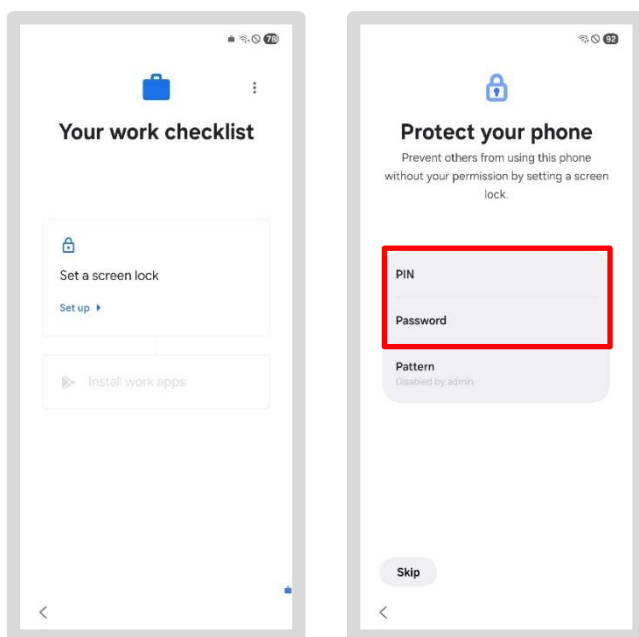


- Aktualizacja smartfona/tabletu może zająć trochę czasu, a czasem bardzo długo, bądźcie cierpliwi!
 - Niezbędne aplikacje zostaną zainstalowane
- > przejdź do rozdziału 4.2 Ustaw blokadę ekranu

4.2 Ustaw blokadę ekranu

Kolejnym krokiem jest skonfigurowanie blokady ekranu na swoim urządzeniu. Jest to obowiązkowe w DB ze względów ochrony danych i niezawodnie chroni Twoje dane.

- Ustawienie ekranu
- Wybierz sam, co jest dla Ciebie najlepsze
- Stuknij jedną z dwóch opcji (PIN lub hasło), a następnie ustaw własną blokadę ekranu
- Upewnij się, że nowe hasło to nowa kombinacja cyfr ma co najmniej 8 cyfr
- Gdy pojawi się "Ustaw biometrię", kliknij "Pomiń"

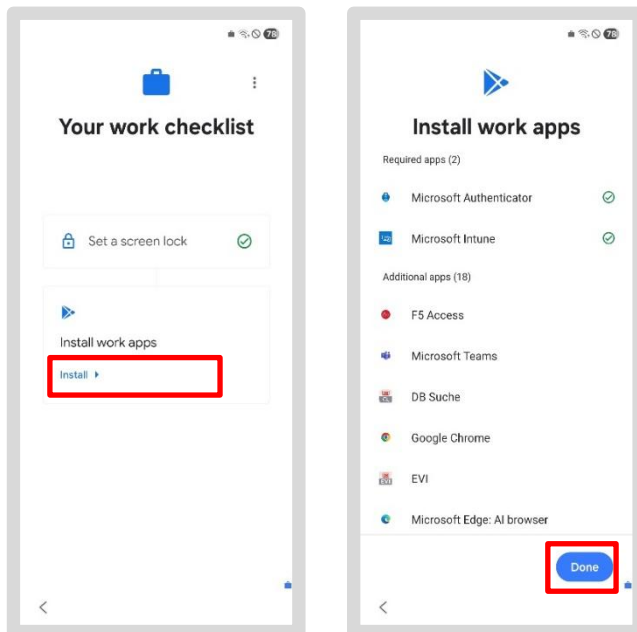


- Zwróć uwagę na informacje o prywatności i użytkowaniu w przewodniku po początkowej konfiguracji
 - Potwierdź "Następny", a potem "OK", jeśli wpiszesz to dwa razy
 - Jeśli pojawi się ekran "Prywatne konta" : Kliknij "Później" podczas wywoływania
- > przejdź do rozdziału 4.3 Instalacja aplikacji bazy danych

4.3 Instalacja aplikacji bazy danych

W kolejnym kroku wszystkie aplikacje bazy danych zostaną ponownie zainstalowane na smartfonie/tablecie bazy danych.

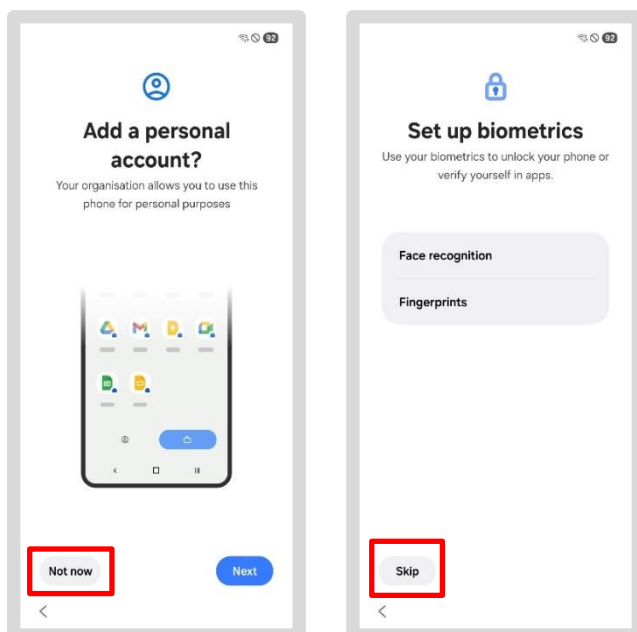
- Kliknij Instalacja, a potem Gotowe



> przejdź do konta Google rozdziału 4.4 – nie jest konieczne

4.4 Konto Google – Niepotrzebne

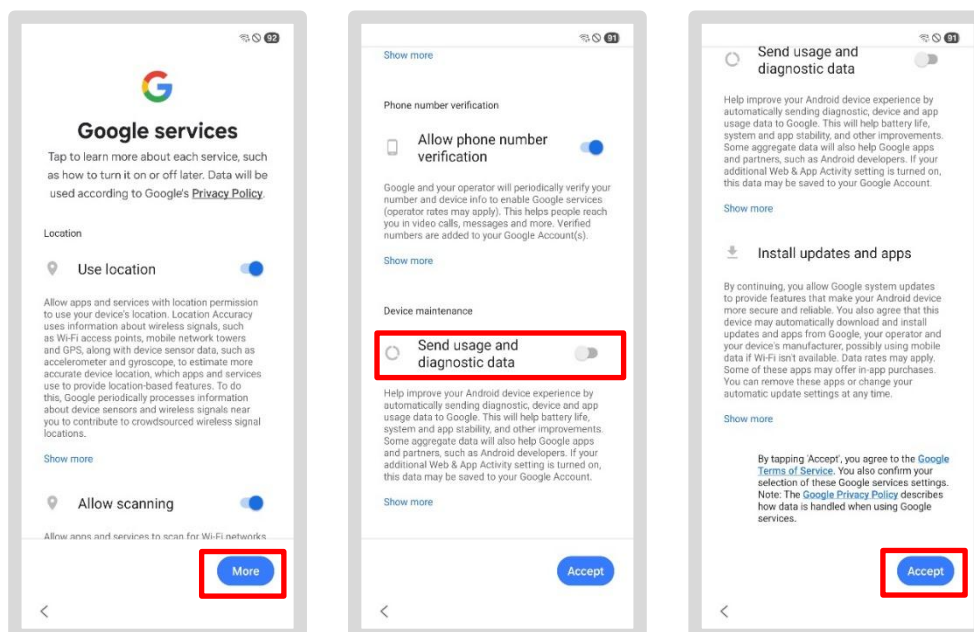
- Nie jest wymagane osobiste konto Google! Kliknij później
- Dlatego w kolejnym kroku kliknij "Pomiń"



> przejdź do rozdziału 4.5 Aktywuj usługę Google

4.5 Aktywuj usługę Google

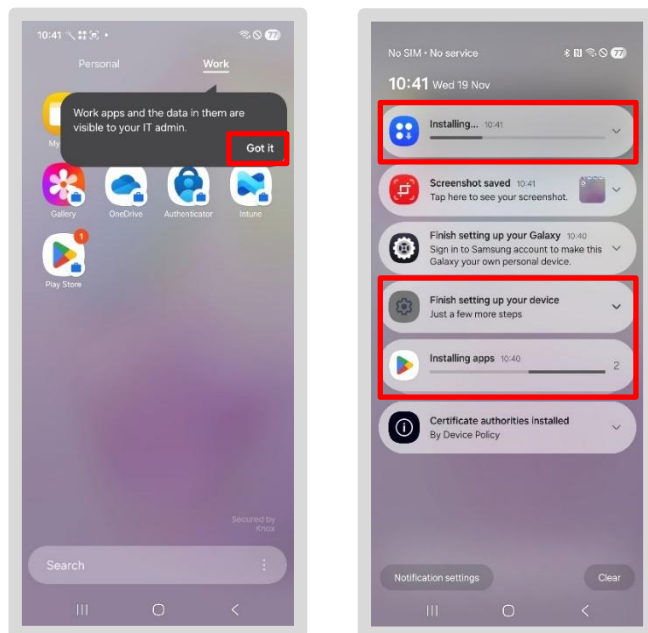
- Kliknij więcej w Google Services
- Wyślij **dane dotyczące użytkowania i diagnostyki**: Aby wyłączyć, kliknij suwak
- Przewijaj dalej, a potem kliknij Akceptuj



> idź do Rozdział 4.6 Ukończenie przygotowań – opcjonalne

4.6 Kompletny zestaw – opcjonalny

- Przesuń w górę ekranu, aby zobaczyć sekcję Osobiste/Praca
- Stuknij Dobrze
- Przesuń w dół ekranu, aby zobaczyć, czy jakieś aplikacje nadal się ładują lub instalują
- Stuknij powiadomienie, a zobaczysz, ile aplikacji zostało do zainstalowania



- **Uwaga:** "Kompletna konfiguracja urządzenia" nie jest konieczna, aby skonfigurować bazę danych, smartfona/tabletu. Zignoruj to!
- Poczekaj tu chwilę, aż wszystkie aplikacje zostaną zainstalowane

Uwaga: Jeśli urządzenie nie zachowuje się tak lub pokazuje ekrany z instrukcji, zresetuj je ponownie.

> Aby to zrobić, przejdź do Rozdziału 2 Start Recovery: Reset smartfona/tabletu

Ważne!

Twój smartfon/tablet nie jest jeszcze podłączony do
Zarządzanie bazą danych!

Zdobądź **Tymczasowa Przepustka Dostępu (TAP)**
i wpisz go do *Aplikacja Intune a.*

Postępuj zgodnie z instrukcjami krok po kroku w

> Rozdział 5 Aktywacja urządzenia – Tworzenie tymczasowego dostępu (TAP)

5 Aktywuj urządzenie - Utworzenie tymczasowego dostępu (TAP)

5.1 Co jest konieczne do stworzenia Tymczasowego Przepustki Dostępu (TAP)

Aby skonfigurować smartfon/tablet w sieci bazy danych, potrzebujesz następujących rzeczy:

- Ważny Tymczasowy Dostęp (TAP)
- Twoja nazwa użytkownika do bazy danych i hasło użytkownika do bazy
- aplikacja Intune

Jeśli już utworzyłeś Access Pass:

- > przejdź do rozdziału 6 Aktywuj urządzenie z tymczasową przepustką dostępu
- > W przeciwnym razie kontynuuj Rozdział 5.2 Tworzenie tymczasowego dostępu (TAP)

Dla informacji:

Użytkownik bazy danych to konto użytkownika wszystkich pracowników w Grupie Bazy Danych. Składa się z wybranego przez Ciebie hasła oraz automatycznie wygenerowanej nazwy logowania.

- > Jeśli zapomniałeś **hasła do bazy danych**, możesz je zresetować w db.de/passwort

Alternatywnie: otwórz aplikację *DB Mobile Info* na swoim starym smartfonie/tablecie, wybierz zakładkę "Usługa" i stuknij w linię "Resetuj hasło użytkownika bazy"

- > Aby zmienić **hasło**, zobacz Zmień hasło użytkownika bazy danych
- > Jak zdobyć **Użytkownika bazy danych** można znaleźć w Precondition: DB User
- > Twoje "**Nazwa użytkownika bazy danych**" można go znaleźć w DeBI pod: db.de/debi

5.2 Utworzenie tymczasowego dostępu (TAP)

- > **Uwaga:** Znajdziesz samouczek wideo pod db.de/mobile-videoanleitung

Wariant 1:

Masz drugi smartfon/tablet lub bazę danych, Workplace Windows lub Mac, który jest zalogowany do sieci bazy. W takim przypadku pozostań w bieżącym rozdziale.

Wariant 2:

Kolega z tej samej firmy (z.B. DB sprzedaży) wesprze cię, jeśli posiada smartfon/tablet z bazą danych (lub iPhone/iPad) albo bazę danych Workplace Windows lub Mac.

- > Przejdź do rozdziału 5.3 Utworzenie tymczasowej przepustki dostępu dla kolegi tutaj

Wariant 3 - Tryb Ekspert:

Posiadasz tylko jeden smartfon/tablet i mogłeś go używać na tyle, o ile utworzyłeś tymczasową przepustkę dostępu (TAP) przed resetem. Zannotuj swoją przepustkę.

- > To idź do Rozdział 6 Aktywuj urządzenie z tymczasowym dostępem (TAP)

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

Kontynuuj wariant 1:

- Otwórz domyślną przeglądarkę i przejdź do db.de/tap
- Wprowadź swoją nazwę użytkownika do bazy danych oraz hasło użytkownika do bazy danych
- Wybierz dla siebie i stuknij niebieski przycisk
- Teraz wybierz "DB Workplace Mobile"
- Następnie zobaczysz Tymczasową Przepustkę Dostępu (TAP)
- Zapisz Tymczasową Przepustkę Dostępu (TAP) na kartce papieru lub zeszyście

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 Anmeldename
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

Create a Temporary Access Pass (TAP)

Select the product you want to set up.

☒ **DB Workplace Mobile**
I want to set up a smartphone/tablet.

☐ **Basic Workplace Windows**
I want to set up a notebook / PC.

☐ **DB Workplace Windows**
I want to set up a notebook / PC.

☐ **DB Workplace Mac**
I want to set up an Apple Mac/MacBook.

Create a Temporary Access Pass (TAP)

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.

y&r3%9=cg2u#

Start a new session To the homepage

Uwaga: TAP jest obecnie ważny przez 60 minut i na wielu smartfonach/tabletach.

Ważne!

The **TAP** może być używany tylko w **Aplikacja Intune** nawet jeśli poproszą cię o to w innej aplikacji lub urządzeniu bazy danych.

- Teraz możesz aktywować telefon/tablet w *aplikacji Intune*
- > Przejdź do Rozdział 6 Aktywuj urządzenie z tymczasowym dostępem (TAP)

Ważne!

Twój smartfon/tablet nie jest jeszcze podłączony do Zarządzanie bazą danych (Intune)!

Wprowadź **tymczasową przepustkę dostępu (TAP)** w *Aplikacja Intune a.*

Postępuj zgodnie z instrukcjami krok po kroku w:

- > Rozdział 6 Aktywuj urządzenie z tymczasowym dostępem (TAP)

5.3 Utworzenie tymczasowej przepustki dostępu dla kolegi

Aby stworzyć dla kolegi: w TAP postępuj zgodnie z następującymi instrukcjami:

- Otwórz domyślną przeglądarkę i przejdź do db.de/tap
- Wprowadź swoją nazwę użytkownika do bazy danych oraz hasło użytkownika do bazy danych
- Wybierz "Dla innego pracownika DB"
- Wpisz nazwę użytkownika swojego kolegi (kolegów) w bazie danych i stuknij w lupę
- Wybierz właściwego kolegę/współpracowników: i potwierdź poniższy wpis
- Naciśnij niebieski przycisk

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen. It includes a 'Register' section where the user enters their DB user login details. The username 'Max Mustermann' is entered in the 'DB User Anmeldenname' field. The password field is empty. The right screenshot shows the 'Create a Temporary Access Pass (TAP) - Person selection' screen. It includes a search bar with 'Max Mustermann' entered. Below the search bar, a list of results is shown, including 'DB User: Name: Max Mustermann', 'E-mail: [redacted]', 'Department: [redacted]', and 'Company: DB Systel GmbH'. A checkbox 'I confirm that I have established the employee's identity.' is checked.

Kolega musi teraz wpisać hasło użytkownika do swojej bazy danych:

- Aby to zrobić, pozwól koledze: wejść do komputera

lub

- Przekazanie kontroli w *Teams* współpracownikowi: w
- Kolega z bazy: wpisz hasło użytkownika do bazy danych w
- Teraz wybierz "DB Workplace Mobile"
- Następnie zobaczysz Tymczasową Przepustkę Dostępu (TAP)
- Zapisz Tymczasową Przepustkę Dostępu (TAP) na kartce papieru lub zeszyście

Uwaga: TAP jest teraz ważny przez 60 minut i na wielu telefonach/tabletach. Będziesz go potrzebować później, gdy skonfigurujesz go w **aplikacji Intune!**

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=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

- Kolega może teraz aktywować swój smartfon/tablet w aplikacji Intune

> przejdź do rozdziału 6 Aktywuj urządzenie z tymczasowym dostępem (TAP)

Ważne!

Twój smartfon/tablet nie jest jeszcze podłączony do
Zarządzanie bazą danych (Intune)!

Wprowadź **tymczasową przepustkę dostępu (TAP)**
w *Aplikacja Intune a.*

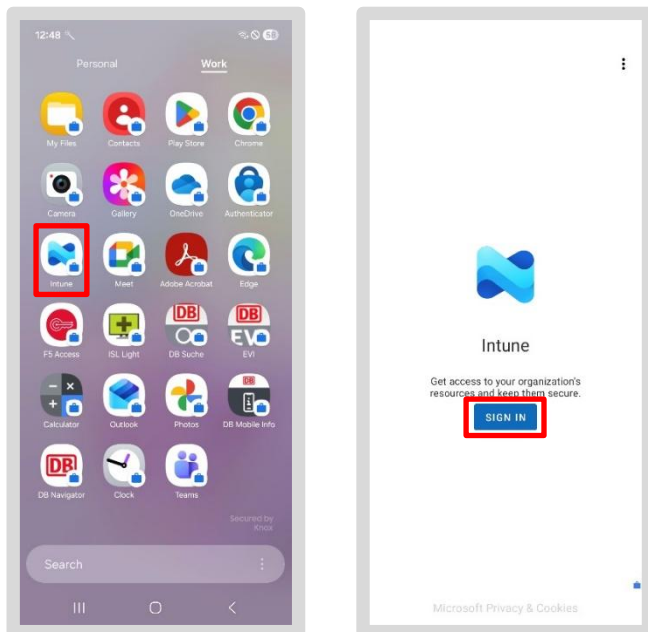
Postępuj zgodnie z instrukcjami krok po kroku w:

> Rozdział 6 Aktywuj urządzenie z tymczasowym dostępem (TAP)

6 Aktywuj swoje urządzenie za pomocą Tymczasowej Przepustki Dostępu (TAP)

> **Uwaga:** Znajdziesz samouczek wideo pod db.de/mobile-videoanleitung

- Najpierw sprawdź, czy otrzymałeś Tymczasową Przepustkę Dostępu (TAP)
- Otwórz aplikację Intune
- Następnie kliknij przycisk "Zaloguj się"



- Wpisz **swój adres e-mail użytkownika bazy** danych (nie: użytkownik bazy) i kliknij "Kontynuuj"
- **Wskazówka:** Zaznacz pole obok "Pokaż tymczasowy dostęp do karty"

- Wprowadź tymczasową przepustkę dostępu, a następnie stuknij Zaloguj się

The image displays two sequential screenshots of the DB mobile application's login interface.

Left Screenshot (Sign in):

- Logo: DB
- Title: Sign in
- Input field: vorname.nachname@deutschebahn.com
- Link: Ich kann mich nicht anmelden.
- Buttons: Back, Next (highlighted with a red box)
- Section: Hinweis
- Text: Klicke auf "Verwenden eines Zertifikats oder einer Smartcard"
- Section: Sign-in options
- Footer: Datenschutz

Right Screenshot (Enter Temporary Access Pass):

- Logo: DB
- Back arrow
- Title: Enter Temporary Access Pass
- Section: Temporary Access Pass
- Checkbox: Show Temporary Access Pass (highlighted with a red box)
- Text: Sign in another way
- Button: Sign in (highlighted with a red box)
- Footer: Datenschutz

Jeśli pojawi się komunikat o błędzie:

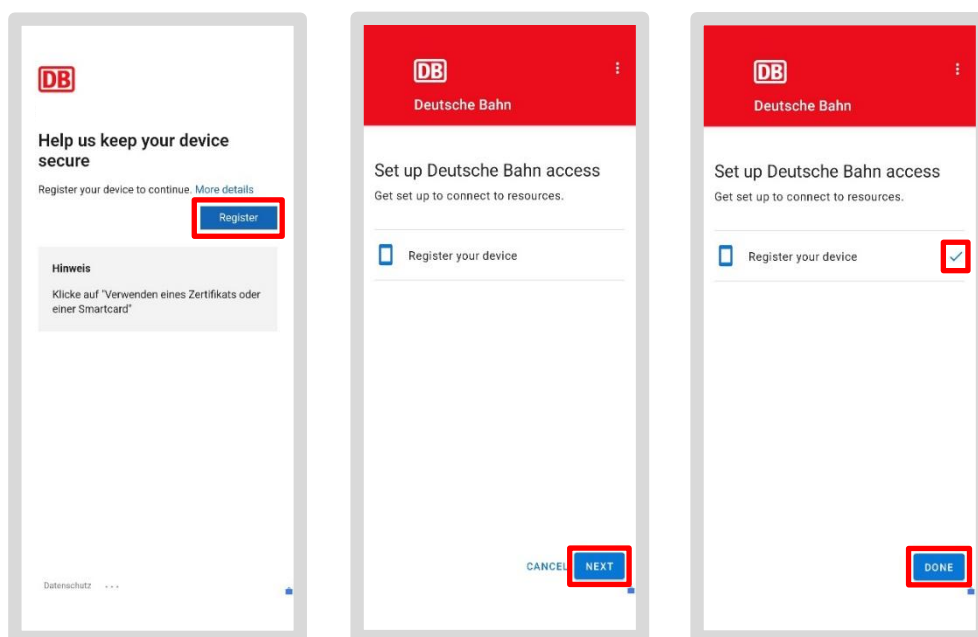
- Stwórz dziewięciu TAP i powtórz rejestrację!
- > Przejdź do Rozdział 5 Aktywuj urządzenie – Utworzenie tymczasowego dostępu (TAP) opisany
- > W przeciwnym razie kontynuuj Rozdział 6.1 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych bazy danych

Uwaga: Pod warunkiem, że Tymczasowa Przepustka Dostępu (TAP) jest ważna (w ciągu 60 minut) i Ty, na przykład, *Perspektywy*, *Drużyny* lub *IT ServiceDesk* zostaniesz poproszony o Tymczasową Przepustkę Dostępu, wpisz tutaj również swoją oznaczoną Przepustkę Tymczasowego.

6.1 Ustaw dostęp do wszystkich aplikacji i stron internetowych bazy danych

Teraz dostęp do zarządzania bazą danych jest skonfigurowany:

- Stuknij Zarejestruj się, a następnie kliknij Kontynuuj
- Gdy pojawi się znacznik "Rejestruj urządzenie", naciśnij przycisk "Gotowe"



Uwaga: Jeśli przycisk "Gotowe" się nie pojawi, aktywacja nie jest zakończona

- Otwórz ponownie aplikację Intune i przejdź przez kolejne kroki:
- > Rozdział 6 Aktywuj urządzenie z tymczasowym dostępem (TAP)

Uwaga: Czekaj od 5 minut do 24 godzin po rejestracji!

Następnie wszystkie informacje i certyfikaty zostały przeniesione na smartfon/tablet i możesz korzystać z aplikacji takich jak *Outlook*, *Teams* itd.

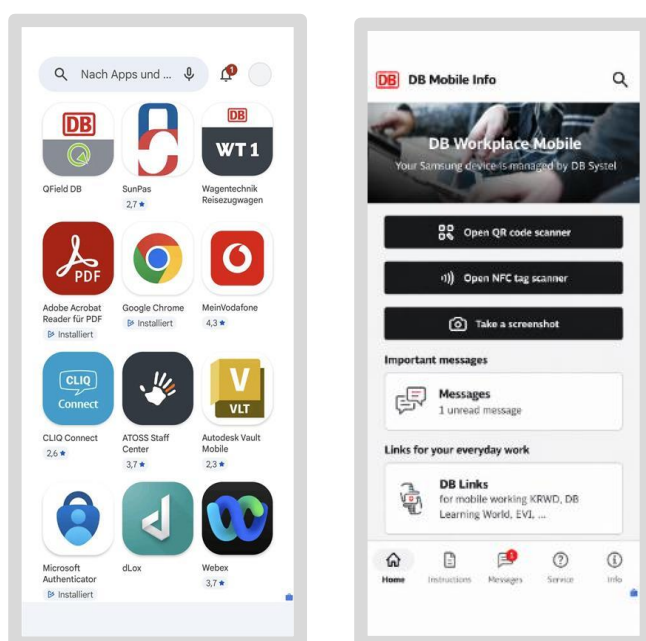
6.2 Aplikacje bazy danych

Uwaga: Przekazanie certyfikatów może **zająć od 5 minut do 24 godzin**. Dopiero wtedy możesz korzystać ze swoich aplikacji, takich jak *Outlook*, *Teams* itp.

Po zakończeniu konfiguracji automatycznie pobierane są aplikacje bazowe, takie jak *Outlook* czy *Teams*. Następnie ładowane są aplikacje specyficzne dla Twojej firmy lub firmy.

- Możesz pobrać inne aplikacje bazy danych z oficjalnego Google Play Store (aplikacji z symbolem walizki) w sekcji "Biznes"
- Jeśli używasz *ASES* lub *ATOSS Staff Center* jako narzędzia do śledzenia czasu, oto przewodnik po najważniejszych funkcjach:
 - > Centrum Personelu ATOSS – najważniejsze funkcje
- Jeśli używasz swojego Deutschlandticket w *DB Navigator*, możesz go ponownie aktywować w ten sposób:
 - > Czy mogę przenieść cyfrowy bilet na pracę Deutschland-Ticket na inny telefon komórkowy?

The **Aplikacja Welcome** jest już **nie** na smartfonie/tablecie DB, dla którego istnieje **App DB Mobile Info** zawiera wszystkie informacje, przydatne linki i dane dotyczące Twojego smartfona/tabletu z bazą danych.

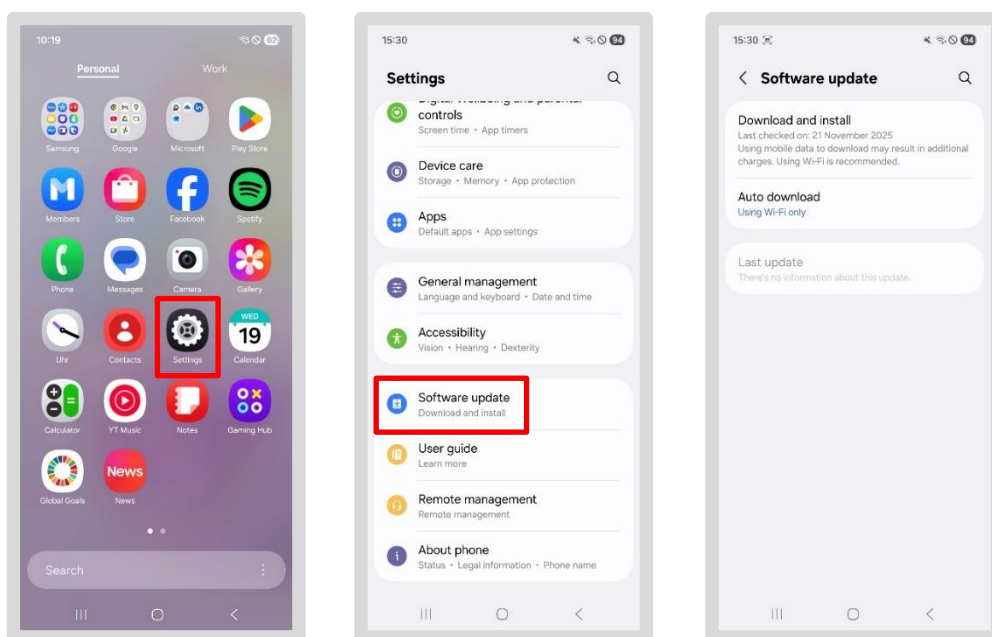


7 Niezbędne ustawienia

Uwaga: Zapewnienie certyfikatów może być **5 minut do 24 godzin**. Dopiero wtedy możesz korzystać z aplikacji takich jak *Perspektywy*, *Drużyny*, itd.

7.1 Instalacja aktualizacji systemu Android

- Na telefonie/tablecie przejdź do sekcji Prywatne
- Kliknij w aplikację *Ustawienia*
- Kliknij "Aktualizacja systemu" (pokazuje, czy dostępna jest aktualizacja)
- Wykonaj nadchodzące aktualizacje, klikając "Install Update"



7.2 Aplikacja MS Defender – wymagana aktywacja

Po aktywowaniu *Outlook* i *Teams* aktywuj aplikację "*Microsoft Defender for Endpoint Mobile*" (w skrócie *MS Defender App*) na swoim smartfonie/tablecie. Aplikacja chroni przed cyberatakami i skanuje istniejące aplikacje pod kątem złośliwego oprogramowania. Aby ochrona była aktywna, otwórz aplikację 1 raz.

Ze względu na dużą liczbę różnych smartfonów/tabletów z bazą danych, mogą występować drobne odchylenia w opisie poszczególnych kroków.

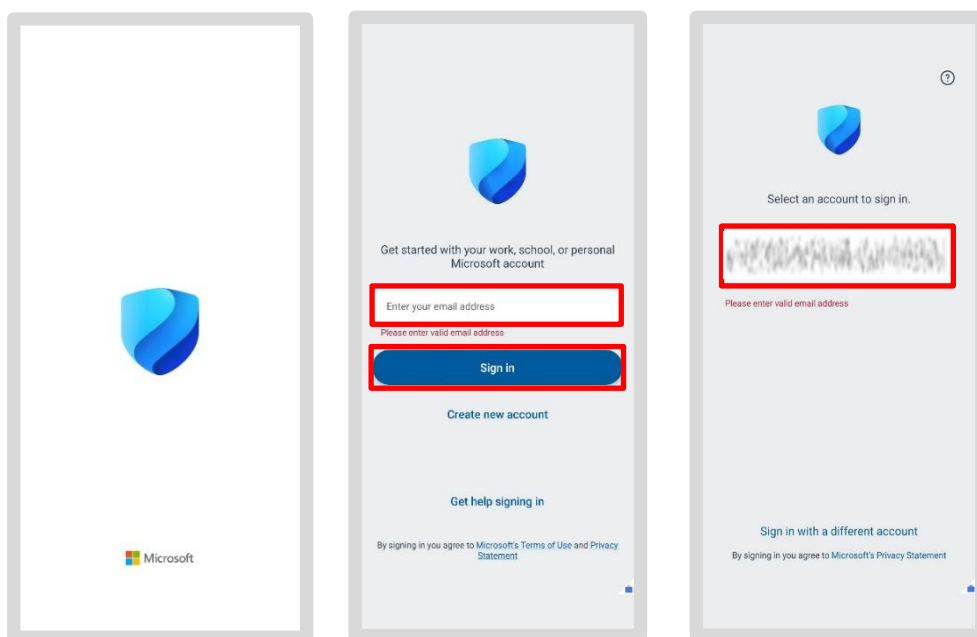
Ważne:

jeśli Twój iPhone/iPad ma **Defender nie włączony** Twój iPhone/iPad nie jest zgodny z odpowiednią bazą danych *Bezpieczna konfiguracja CSIRT* Polityka i wola **do 21 dni Być użytecznym w ograniczonym stopniu**.

Oznacza to: Aplikacje takie jak Teams, Outlook, OneDrive **Nie jest już użyteczny**.

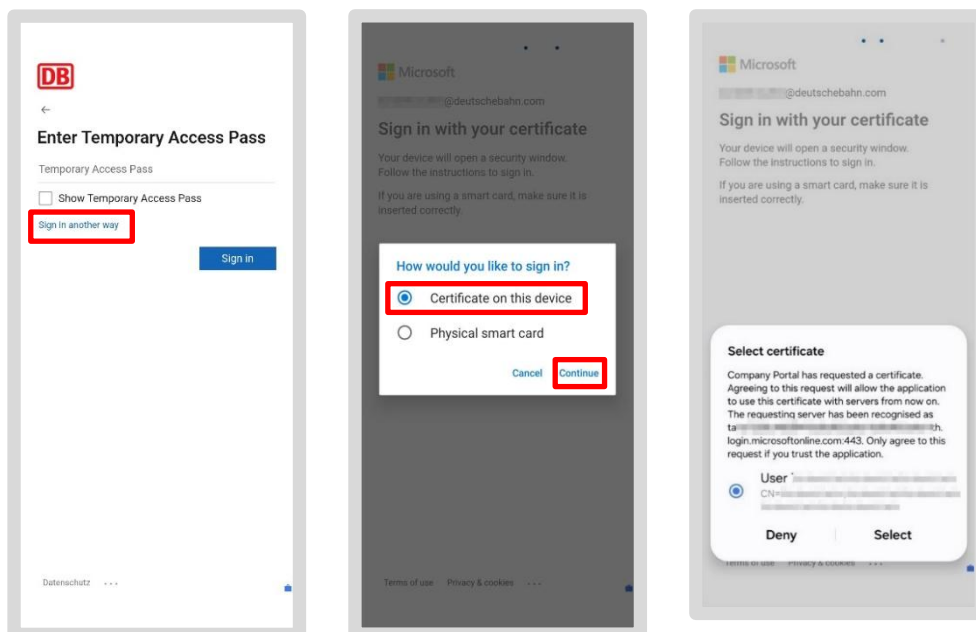
Konfiguracja aplikacji MS Defender:

- Przejdź do sekcji Praca/Biznes i otwórz "DB Google Play Store"
- Wyszukaj aplikację Microsoft Defender: Antivirus i kliknij Install
- Kliknij ikonę aplikacji w *aplikacji MS Defender*, aby otworzyć aplikację
- Poproszono Cię o podanie służbowego adresu e-mail
- Kliknij przycisk "Zaloguj się", albo aplikacja automatycznie przekieruje Cię na kolejny ekran, gdzie pojawi się Twój adres e-mail
- Podklikaj swój służbowy adres e-mail



Jeśli aktywujesz smartfon/tablet za pomocą aplikacji Intune w ciągu godziny, możesz zostać poproszony o ponowne wprowadzenie tymczasowej karty dostępu.

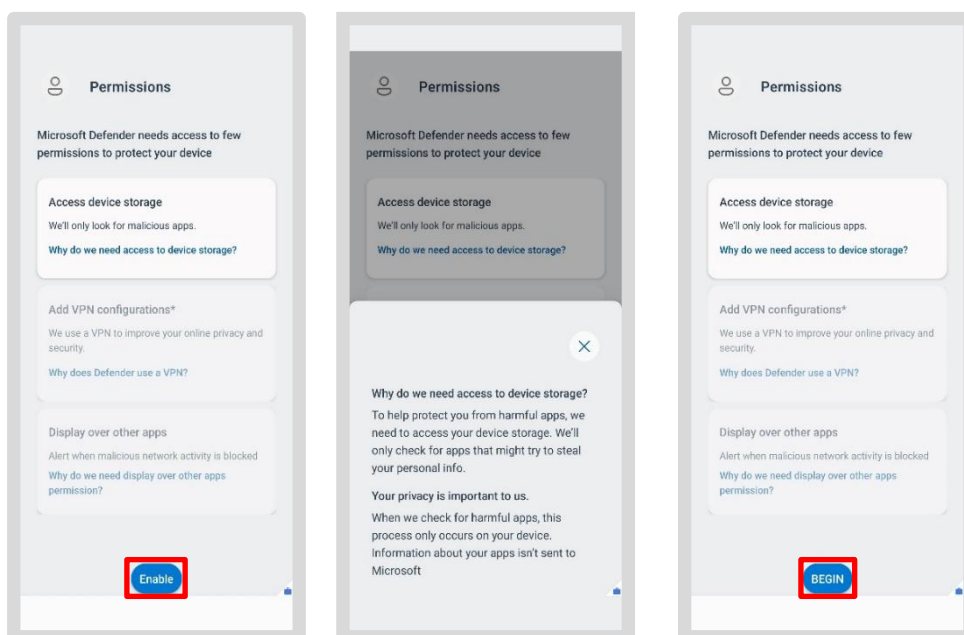
- Kliknij Zaloguj się w inny sposób
- Po pojawieniu się pytania kliknij Certyfikat na tym urządzeniu, a następnie kliknij Dalej
- Wybierz certyfikat



Przypisz uprawnienia:

Aplikacja poprosi Cię teraz o niezbędne uprawnienia. W tym momencie ekrany mogą pojawiać się w innej kolejności niż instrukcje. Jeśli Twój pierwszy ekran zgadza się z tym, który pokazujesz:

- Naciśnij Aktywuj
- Następnie naciśnij Start
- Aplikacja Ustawienia na Twoim smartfonie/tablecie się otworzy

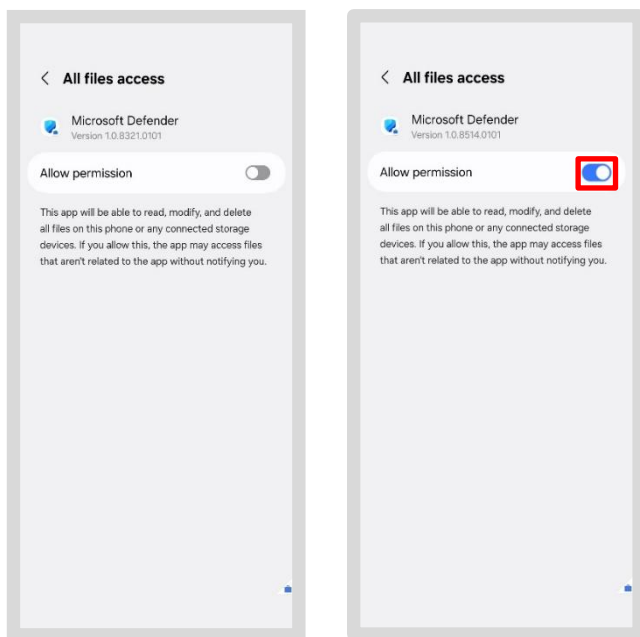


Informacje wstępne: Uprawnienia:

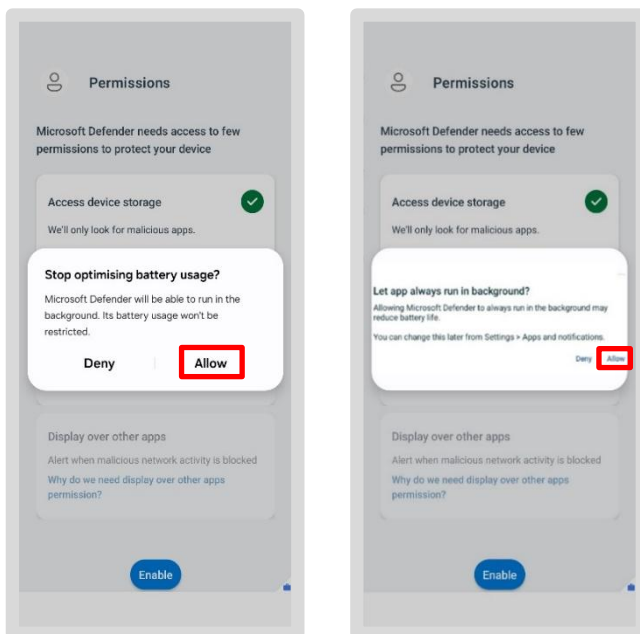
Te uprawnienia są wymagane, aby aplikacja działała poprawnie i zapewniała bezpieczeństwo urządzenia.

Możesz wyświetlić okno informacyjne dla każdego z indywidualnych uprawnień (np. klikając "Dlaczego potrzebujemy dostępu do pamięci na urządzeniu?"). Jednak niektóre elementy nie są wybieralne (są wyszarzone, np. "Dodaj konfigurację VPN") lub już aktywowane (zielony znacznik, np. "Uruchom w tle"), ponieważ są zdefiniowane przez system.

- Teraz przesunąć suwak w prawo, aby uzyskać zgodę
- Kliknij "Pozwól" w kolejnym promptie



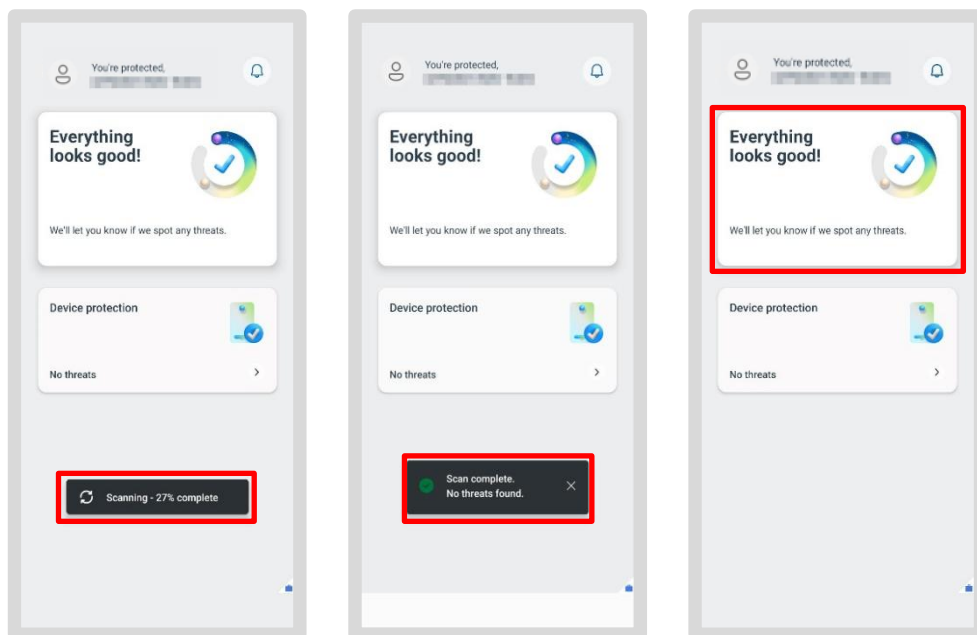
- Naciśnij Pozwól na każde z następujących zapytań



Uwaga: W zależności od typu urządzenia, będą wymagane różne autoryzacje! Może to skutkować tylko jednym z wyświetlanych żądań.

Następnie trafisz na stronę główną *aplikacji MS Defender*. Automatycznie przeprowadzi się sprawdzenie złośliwego oprogramowania na smartfonie/tablecie. Podczas sprawdzania będą wyświetlane kroki pośrednie.

Wynik jest wyświetlany na piśmie na stronie głównej. Jeśli widoczny jest zielony znaczek, nie wykryto żadnego złośliwego oprogramowania.



Smartfon/tablet jest teraz chroniony przed złośliwym oprogramowaniem.

7.3 Konfiguracja Outlooka / tworzenie konta e-mail / szyfrowanie poczty

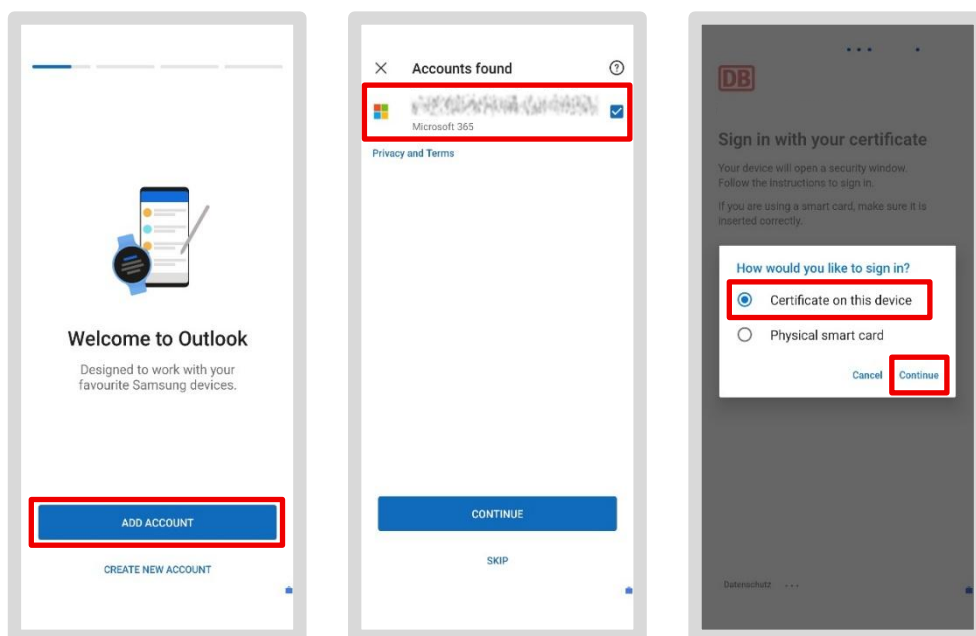
Dzięki Outlookowi możesz otrzymywać i wysyłać służbowe e-maile. Zanim zaczniesz, musisz ustawić kilka ustawień.

> Czy masz pytania dotyczące pisania i wysyłania e-maili? Na [ITfit](#) znajdziesz przydatne wskazówki i instrukcje, jak korzystać z *Outlooka*.

> Jesteś pracownikiem DB E&C: Masz pytania i/lub wystąpił błąd lub problemy z certyfikatami, to sprawdź [Pytania dotyczące bazy danych](#)

Aby skonfigurować Outlook:

- Przejdź do sekcji "Praca/Biznes" i kliknij w aplikację Outlook
- Twoje konto e-mail zostanie automatycznie zapisane – kliknij "Dodaj konto"
- W kolejnym kroku wybierz swój adres e-mail i kliknij "Następny"



Podczas rejestracji możesz zostać poproszony o TAP:

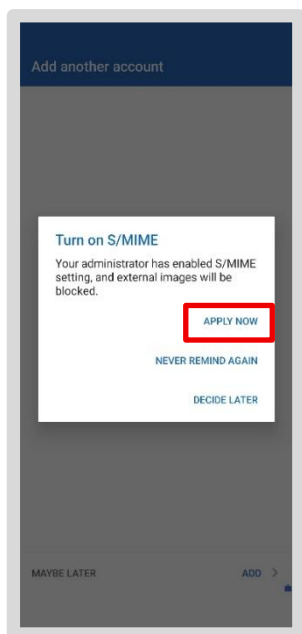
- Jeśli Twoja tymczasowa przepustka dostępu jest nadal ważna, wpisz ją tutaj
- > opisane w [rozdziale 5.2 Tworzenie tymczasowego dostępu \(TAP\)](#)

Alternatywnie:

- W sekcji "Wybierz inną opcję logowania" wybierz "Certyfikat na tym urządzeniu"
- Tap "Select" przy żądaniu certyfikatów

Jeśli chcesz przesłać szczególnie wrażliwe dane (np. dane osobowe) e-mailem, musisz również zaszyfrować treść e-maila. DB zapewnia tzw. szyfrowanie S/MIME w tym celu.

- Kliknij *Apply Now* przy następnym zapytaniu

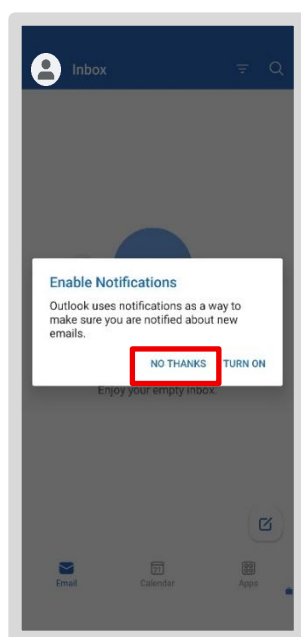
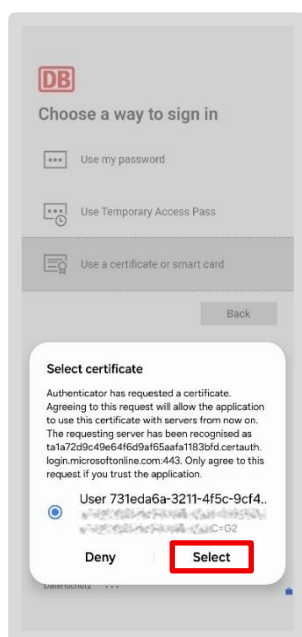


Następnie pojawia się wniosek o certyfikat. Możesz rozpoznać certyfikat ważny dla Ciebie w następujący sposób:

- Pierwsza linijka: "**Użytkownik** ds2232... (potem liczby i litery)"
- Druga linia: "**CN- DB User Name**" np. LisaMustermann 89sd7es0ßwd (wtedy liczby i litery)
- Wybierz fragment tekstu, a następnie kliknij Wybierz

Twoje konto e-mail zostanie teraz utworzone:

- Kliknij "Może później" podczas pytania o założenie innego konta
- oraz "Nie Dziękuję" Aktywuj po powiadomieniu



- Twoje e-maile zostaną teraz załadowane (ten proces może potrwać kilka minut)
- Wtedy możesz znów czytać i pisać e-maile

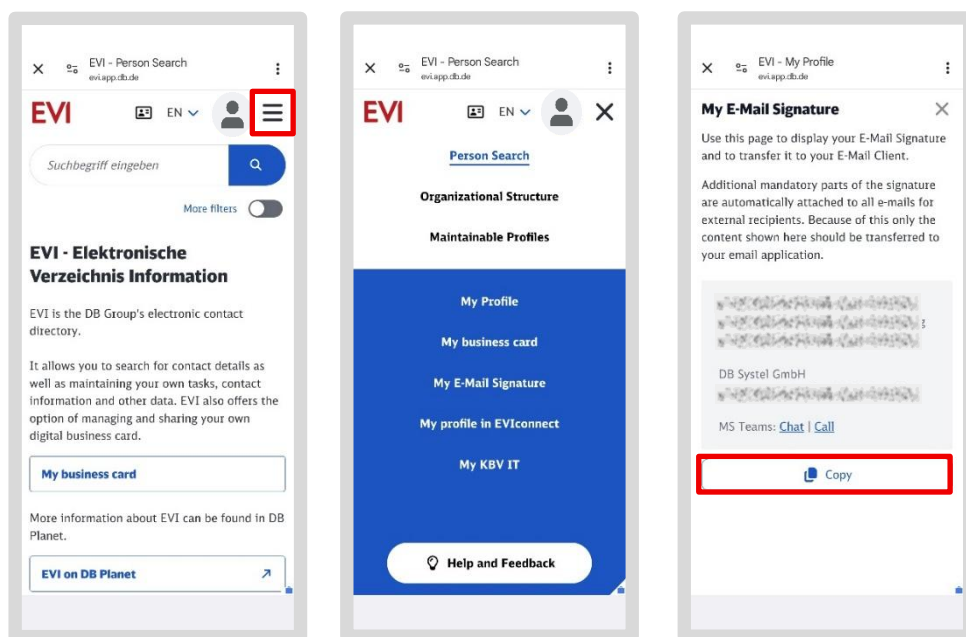
Android 16: W przypadku smartfonów/tabletów z Androidem 16 może się zdarzyć, że krok włączenia S/MIME zostanie pominięty. W takim przypadku konfiguracja *Perspektywy* i zrestartuj aplikację! Wtedy pojawi się komunikat aktywacyjny.

7.3.1 Outlook: Konfiguracja podpisu e-mailowego

Podpis e-maila jest obowiązkową częścią oficjalnej komunikacji. Znajduje się na końcu e-maila i zgodnie z prawem musi zawierać określone informacje, takie jak nazwa firmy oraz oficjalna siedziba Twojej firmy DB. Tekst podpisu e-mailowego znajdziesz w centralnej książce telefonicznej DB, tzw. "EVI".

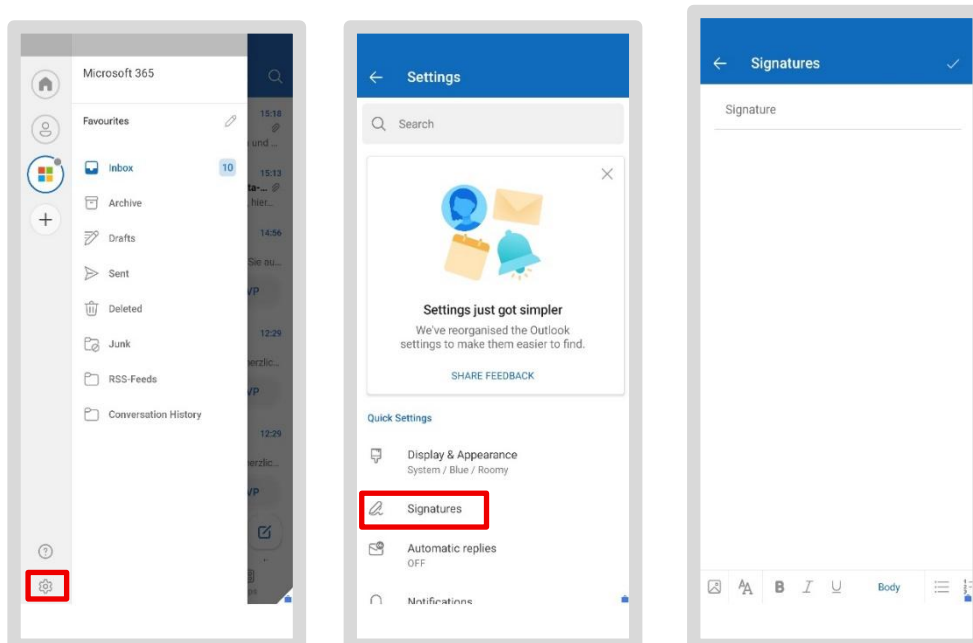
Tak właśnie otrzymujesz podpis e-mail z EVI:

- Otwórz aplikację EVI
- Stuknij trzy linie obok zdjęcia profilowego w prawym górnym rogu
- Następnie kliknij Mój podpis e-mail



Wklej podpis w Outlooku:

- Otwórz *aplikację Outlook*
- Stuknij zdjęcie profilowe w lewym górnym rogu, a potem kliknij w trybik na dole
- Teraz stuknij w "Podpis"



- Otworzy się pole na podpis. Jeśli już tam jest wpis, usuń go za pomocą
- Teraz długo stuknij w pole, aż pojawi się pole "Wstaw" i stuknij w nie
- Twój skopiowany podpis z *EVI* jest wstawiane

Zamknij okno – Twój podpis będzie automatycznie wstawiany do wszystkich nowych wiadomości

Uwaga: Jeśli założyłeś wiele kont e-mail, możesz użyć suwaka "*Podpis na konto*" Ustaw osobny podpis dla każdego konta. W przeciwnym razie podpis w systemie będzie używany dla wszystkich Twoich kont e-mail.

7.3.2 Outlook: Synchronizuj e-maile

Wszystkie Twoje e-maile są automatycznie kopiowane w *aplikacji Outlook* i synchronizowane z Twoim połączonym kontem Office. Oznacza to, że niezależnie od tego, na jakim urządzeniu logujesz się na smartfonie/tablecie czy komputerze BKU/Basic Workplace, jesteś zawsze na **bieżąco**.

7.3.3 Outlook: Utwórz nowe kontakty w

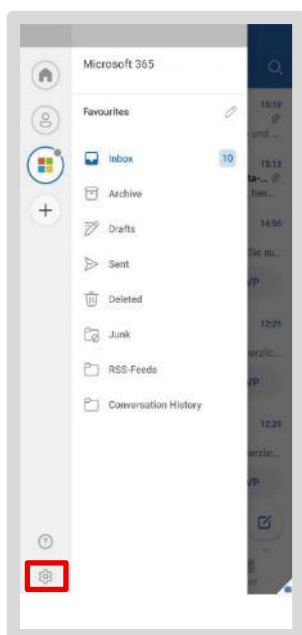
- Przejdź do sekcji Praca i otwórz aplikację Kontakty
- Kliknij "+", aby utworzyć nowy kontakt
- W lewym górnym rogu nad strzałką wybierz Outlook
- Nowy kontakt będzie *Perspektywy* zabezpieczone



7.3.4 Outlook: Synchronizacja kontaktów

Jeśli utworzysz nowy kontakt w sekcji "Praca/Biznes" na smartfonie/tablecie za pomocą aplikacji Kontakty, zaleca się umożliwienie synchronizacji z Outlookiem. Oto jak to zrobić:

- Otwórz *aplikację Outlook* w panelu Praca/Praca
- W aplikacji jest kółko z ikoną w lewym górnym rogu – stuknij
- Po lewej stronie otworzy się przegląd folderów pocztowych
- Wybierz bieżący w lewym dolnym rogu (ustawienia się otworzą)
- W sekcji Konta e-mail wybierz swoje konto Outlook. Następnie kliknij mały suwak obok Sync Contacts
- Następnie potwierdź prośbę o dostęp za pomocą "Zezwalaj"
- Po włączeniu synchronizacji wyjdź z *Aplikacja Outlook*



7.4 DB M 365

Możesz także otwierać i czytać pliki Word, Excel, PowerPoint lub PDF na swoim smartfonie/tablecie. Pobierz odpowiednie aplikacje raz:

- Otwórz bazę danych w Google Play Store
- Wyszukaj odpowiednią aplikację za pomocą paska wyszukiwania, na przykład Word, Excel, PowerPoint lub PDF Reader

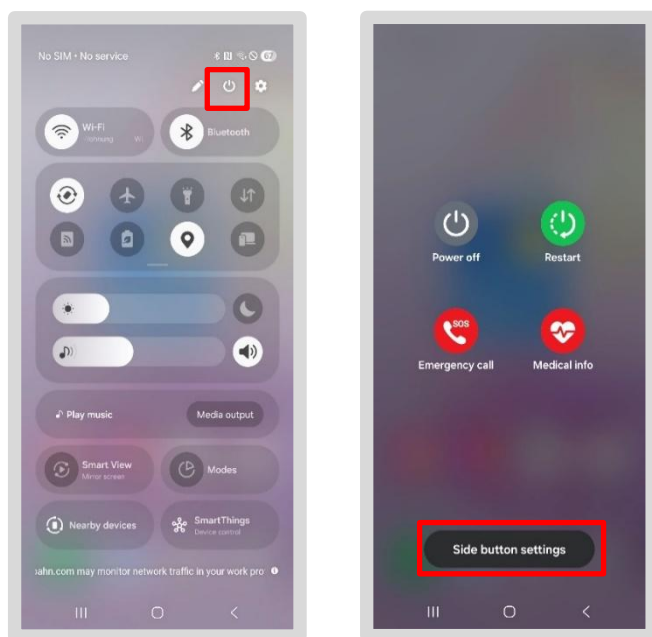


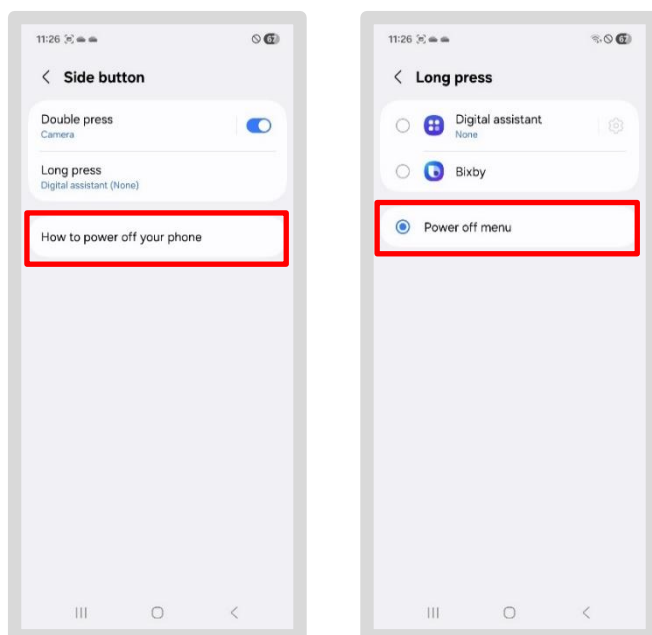
- Następnie kliknij "Install"
- Teraz, gdy otworzysz plik, aplikacja otwiera się automatycznie

Uwaga: Możesz otworzyć tylko jeden plik naraz. Np. nie jest możliwe otwarcie kilku plików Word jednocześnie.

7.5 Wyłącz przycisk Bixby

- Domyślnie uruchamia asystenta głosowego Bixby przycisk zasilania. Ze względów bezpieczeństwa należy go wyłączyć:
- Przesuń w dół od góry ekranu. Centrum sterowania się otworzy.
- Kliknij ikonę zasilania w prawym górnym rogu ikony ustawień
- Wybierz ustawienia klawiszy funkcyjnych
- Zmień funkcję w "Długi nacisk" do "Menu wyłączania"

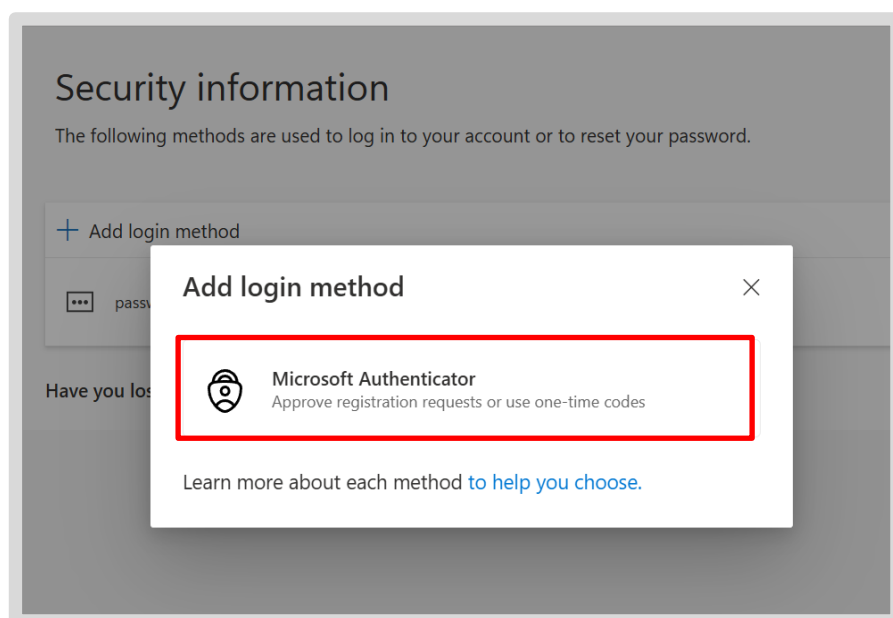




7.6 Ponownie włącz aplikację Microsoft Authenticator

Jeśli korzystałeś z aplikacji Authenticator, postępuj zgodnie z tymi krokami:

- Stuknij db.de/authenticator w kalkulatorze BKU lub Basic Workplace
- Kliknij ikonę "Plus" oraz przycisk "Dodaj metodę logowania"
- Otworzy się okno dialogowe, wybierz "Microsoft Authenticator"



- Przełącz się na telefon/tablet i otwórz *aplikację Microsoft Authenticator*
- Otwórz tę stronę, aby uzyskać instrukcje krok po kroku , stuknąć w przycisk "MFA setup guide" i przejść przez podane kroki

- Następnie możesz użyć *aplikacji Microsoft Authenticator* do uwierzytelniania na smartfonie/tablecie
- Jeśli używałeś **aplikacji Authenticator do stron internetowych lub narzędzi**, aktywuj aplikację ponownie na stronach

Wskazówka: Jeśli masz problem z reaktywacją połączeń w aplikacji Authenticator po odzyskaniu, użyj Self Service: Reset *Microsoft Authenticator App* (MFA): db.de/resetmfa, a następnie postępuj zgodnie z instrukcjami.

Gratulacje!

Udało Ci się przywrócić służbowy smartfon/tablet!

Więcej informacji o swoim smartfonie/tablecie znajdziesz w aplikacji: DB Mobile Info.

> Aby zapisać i ponownie zaimportować kontakty do OneDrive, zobacz poradnik konfiguracji poniżej [Zrób kopię zapasową kontaktów do OneDrive](#)

> Długi poradnik, jak to skonfigurować, znajdziesz pod db.de/mobile-setup