



Wersja systemu operacyjnego: Android 15 lub nowsza

Odzyskiwanie danych Nokia/HMD

DB Workplace Mobile

DB Systel GmbH | 15 sierpnia 2026 r.

Spis treści

1 Czynności wymagane przed renovacją	4
1.1 Utwórz kopię zapasową danych	4
1.2 Aplikacja do uwierzytelniania – opcjonalnie	4
1.3 Tworzenie tymczasowej legitymacji pracownika DB (TAP) – tryb ekspercki	4
2 Rozpocznij przywracanie: zresetuj smartfon/tablet	8
2.1 Samodzielne resetowanie smartfona/tabletu	8
2.2 Zresetuj smartfon/tablet za pomocą aplikacji IT ServiceDesk	9
3 Ponowna konfiguracja w usłudze Microsoft Intune	10
3.1 Wybór języka	10
3.2 Konfiguracja Wi-Fi	11
3.3 Konfiguracja Wi-Fi w budynkach DB	12
4 Instalacja oprogramowania Nokia / HMD	13
4.1 Skonfiguruj profil służbowy	14
4.2 Konfiguracja blokady ekranu	15
4.3 Instalowanie aplikacji DB	16
4.4 Konto Google – nie jest wymagane	16
4.5 Aktywacja usług Google	17
4.6 Zakończenie konfiguracji – opcjonalnie	17
5 Aktywacja urządzenia – utworzenie tymczasowej legitymacji pracownika DB (TAP)	20
5.1 Utwórz tymczasową legitymację pracownika DB (TAP)	20
5.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika	24
6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)	26
6.1 Skonfiguruj dostęp do wszystkich aplikacji i stron internetowych DB	27
6.2 Aplikacje DB	28
7 Wymagane ustawienia	29
7.1 Sprawdź dostępność aktualizacji systemu operacyjnego	29
7.2 Outlook	30
7.2.1 Konfiguracja programu Outlook / Utworzenie konta e-mail / Konfiguracja szyfrowania wiadomości e-mail	30
7.2.2 Konfiguracja podpisu e-mailowego	31
7.2.3 Synchronizacja poczty e-mail – wszystkie wiadomości zawsze aktualne	33
7.3 Aplikacja MS Defender – należy ją uruchomić	33

7.3.1 Konfiguracja aplikacji MS Defender	33
7.3.2 Przyznanie uprawnień	35
7.4 DB M 365	37
7.5 Ponowne aktywowanie aplikacji Microsoft Authenticator dla uwierzytelniania	38

1 Czynności wymagane przed renovacją

Jeśli Twój służbowy smartfon lub tablet ma problemy, takie jak spowolnienie działania, zawieszanie się lub częste awarie, pomocne może być przywrócenie ustawień fabrycznych. Konieczne jest wykonanie następujących czynności:

1.1 Utwórz kopię zapasową danych

- **Utwórz kopię zapasową danych**

Aby to zrobić, wykonaj następujące czynności:

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

> Instrukcje dotyczące tworzenia kopii zapasowej danych znajdziesz pod adresem:

mobileworkplace.deutschebahn.com/mobile-daten-sichern

> Film instruktażowy znajdziesz pod adresem: db.de/mobile-videoanleitungen

1.2 Aplikacja Authenticator – opcjonalna

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

- Należy pamiętać, że aplikacja Authenticator nie może być używana podczas procesu odzyskiwania
- Nie są wymagane żadne dalsze kroki
- Po przywróceniu urządzenia aplikację należy ponownie aktywować; procedura ta została opisana w [rozdziale 7.5 Ponowna aktywacja aplikacji Microsoft Authenticator](#)
- Jeśli podczas procesu odzyskiwania konieczne jest użycie 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 \(MFA\)](#)

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

Po utworzeniu kopii zapasowej danych dostępne są dwie opcje:

Czy Twój iPhone/iPad nadal w pewnym stopniu działa? → Przejdź do tej sekcji

Czy Twój iPhone/iPad w ogóle nie działa?

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

Smartfon/tablet nadal działa częściowo:

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

Jeśli nadal masz zainstalowaną aplikację Welcome:

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

Jeśli nie masz zainstalowanej aplikacji Welcome:

- Wejdź na [stronę db.de/tap](https://db.de/tap) i wprowadź swoją nazwę użytkownika 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 z niego korzystać na wielu smartfonach/tabletach**

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

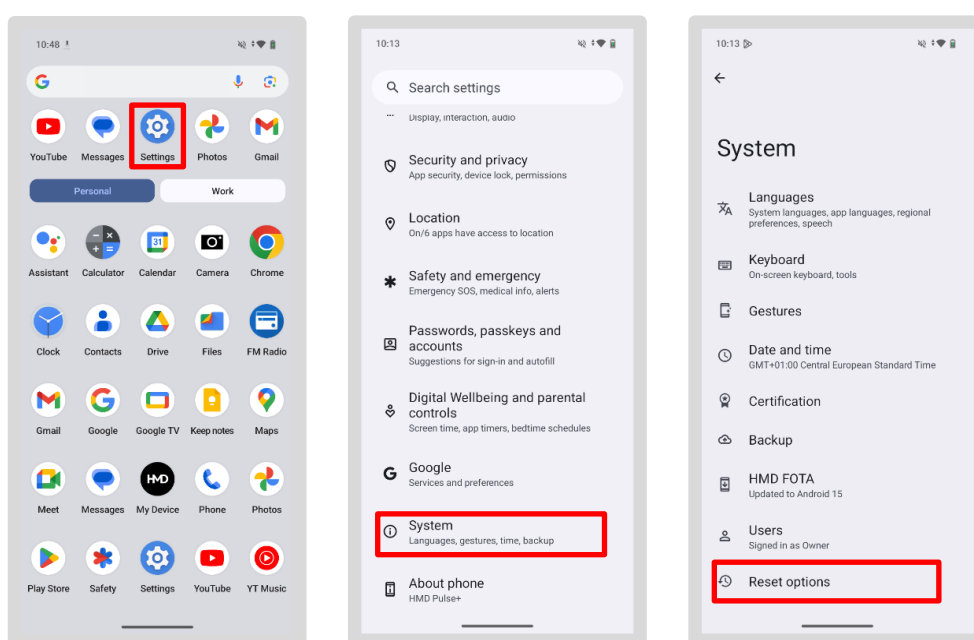
2 Rozpocznij odzyskiwanie: zresetuj smartfon/tablet

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

2.1 Samodzielne resetowanie smartfona/tabletu

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

- Przejdź do sekcji „Prywatne” na smartfonie lub tablecie
- Naciśnij aplikację „Ustawienia”
- Naciśnij „System”, a następnie „Opcje resetowania”
- Przewiń dalej w dół i dotknij opcji „Usuń wszystkie dane (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 „Usuń wszystkie dane”, wprowadź kod blokady ekranu (PIN lub hasło) i dotknij „Usuń wszystkie dane”
- Poczekać kilka minut; smartfon/tablet zresetuje się automatycznie

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

2.2 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:
- 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.

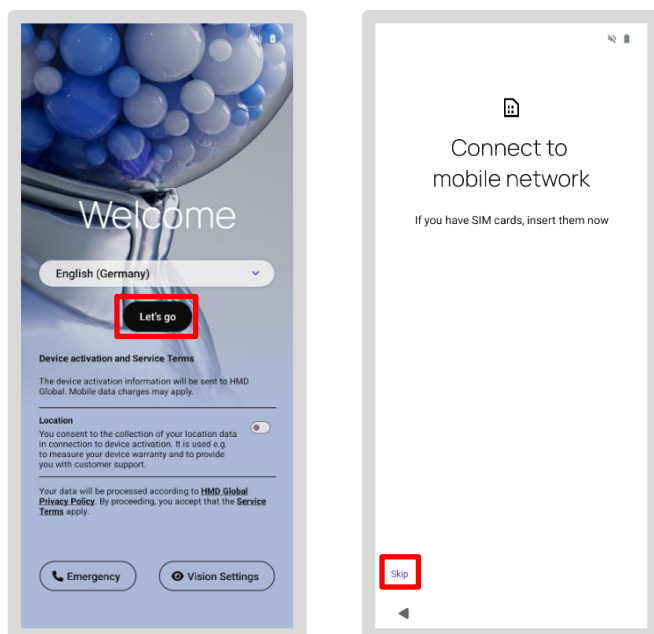
> Następnie przejdź do rozdziału 3: Ponowna konfiguracja w usłudze Microsoft Intune

3 Ponowna konfiguracja w usłudze Microsoft Intune

3.1 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 renovacji
- Sprawdź, czy wybrany jest żądany język. Jeśli nie, zmień go
- Następnie dotknij *opcji „Zacznijmy”*
- Jeśli w smartfonie/tablecie znajduje się karta SIM, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie
- Na następnym ekranie dotknij *„Pomiń”*



3.2 Skonfiguruj Wi-Fi

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

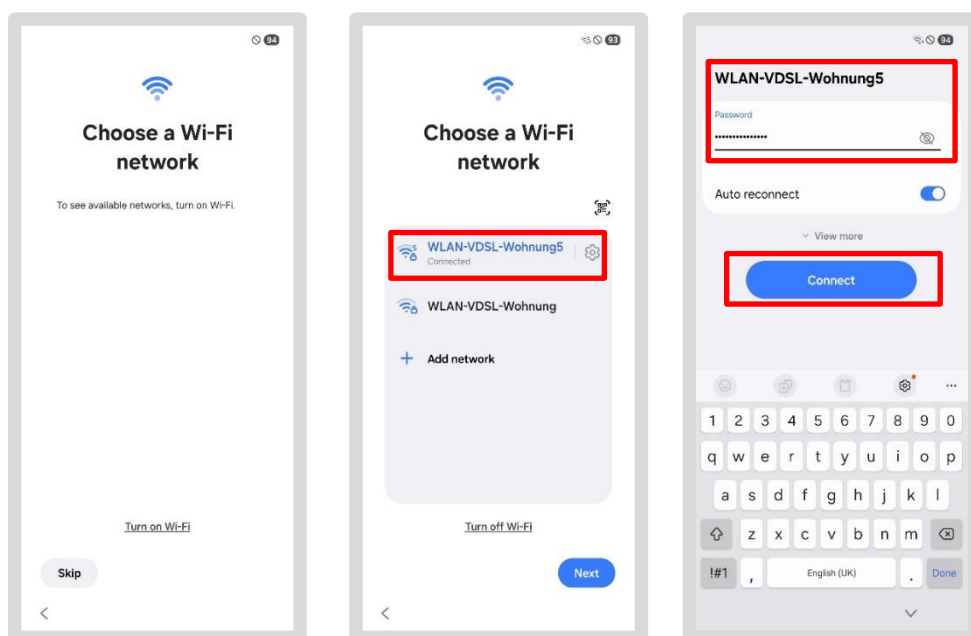
- Korzystaj z **mobilnego internetu**, o ile w smartfonie/tablecie znajduje się karta SIM (może to wiązać się z opłatami!)
- Skonfiguruj hotspot przy użyciu swojego smartfona/tabletu

lub

- Skorzystaj z hotspotu na smartfonie DB kolegi
- Skorzystaj z własnej 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 naciśnij „Połącz”
- Jeśli pojawi się drugi monit, dotknij „Kontynuuj”



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

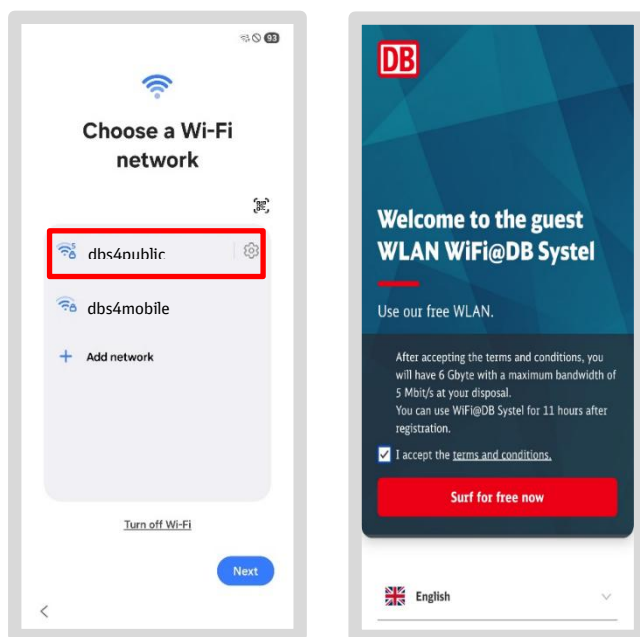
> Przejdź do rozdziału 4: Logowanie do DB za pomocą telefonu Nokia

3.3 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”



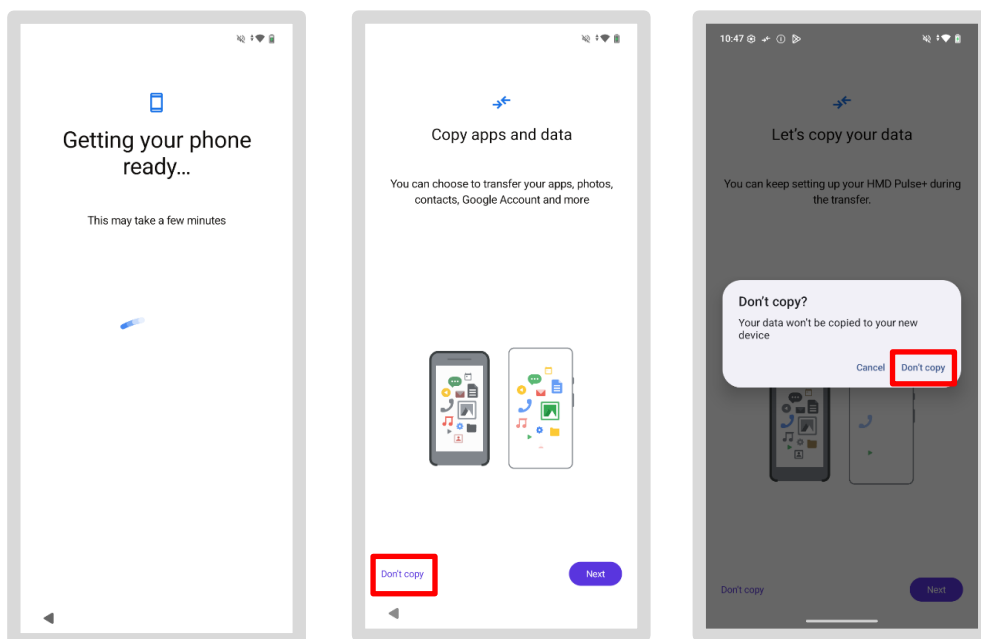
Gdy tylko smartfon/tablet połączy się z siecią Wi-Fi, rozpocznie się nawiązywanie połączenia z siecią DB.

> Przejdź do [rozdziału 4: Instalacja urządzeń Nokia/HMD](#)

4 Instalacja urządzeń Nokia / HMD

W następnym kroku smartfon/tablet DB musi zostać ponownie podłączony do sieci DB (a konkretnie do Enterprise Mobility Management, w skrócie EMM). Ponieważ informacje ulegają zmianie, poczekaj, 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
- Jeśli na tym etapie pojawi się monit o skopiowanie aplikacji i danych, najpierw dotknij *opcji „Nie kopiuj”*, a jeśli monit pojawi się ponownie, dotknij jeszcze raz opcji „Nie kopiuj”

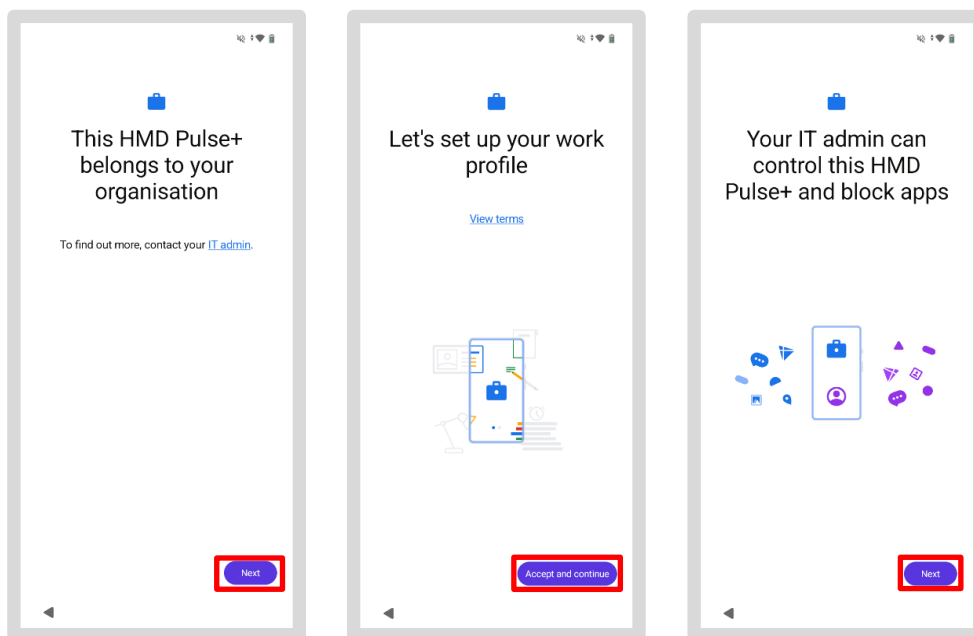


- Czasami smartfon/tablet zapisał również profil służbowy,
> Przejdź bezpośrednio do sekcji 4.4 Konto Google – nie jest to konieczne

4.1 Skonfiguruj profil służbowy

Profil służbowy jest wymagany, aby zapewnić przypisanie aplikacji służbowych do smartfona/tabletu. Należy go skonfigurować tutaj:

- Trwa konfiguracja smartfona/tabletu
- Potwierdź poniższy komunikat, *dotykając przycisku „Dalej”*
- Potwierdź wyświetlone ekrany, wybierając opcje „Akceptuj i kontynuuj” oraz „Kontynuuj”



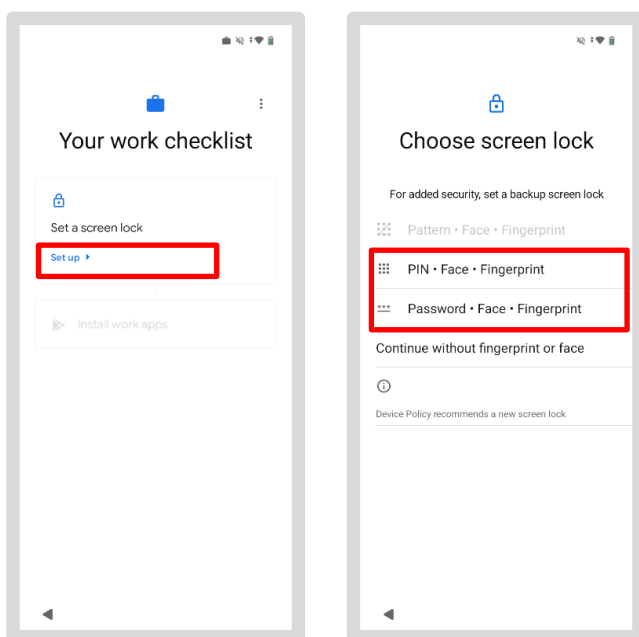
- Aktualizacja smartfona/tabletu może chwilę potrwać, a w niektórych przypadkach nawet dość długo – prosimy o cierpliwość!
- Trwa instalacja wymaganych aplikacji

> Przejdź do sekcji 4.2: Konfiguracja blokady ekranu

4.2 Konfiguracja blokady ekranu

W następnym kroku skonfigurujesz blokadę ekranu dla swojego smartfona/tabletu. Jest to obowiązkowe w DB ze względów ochrony danych i zapewnia niezawodną ochronę Twoich danych.

- Naciśnij „Skonfiguruj”
- Wybierz opcję, która najbardziej Ci odpowiada. Naciśnij jedną z dwóch opcji (kod PIN lub hasło), a następnie ustaw własną, osobistą blokadę ekranu
- Upewnij się, że nowe hasło to nowa 6-cyfrowa kombinacja

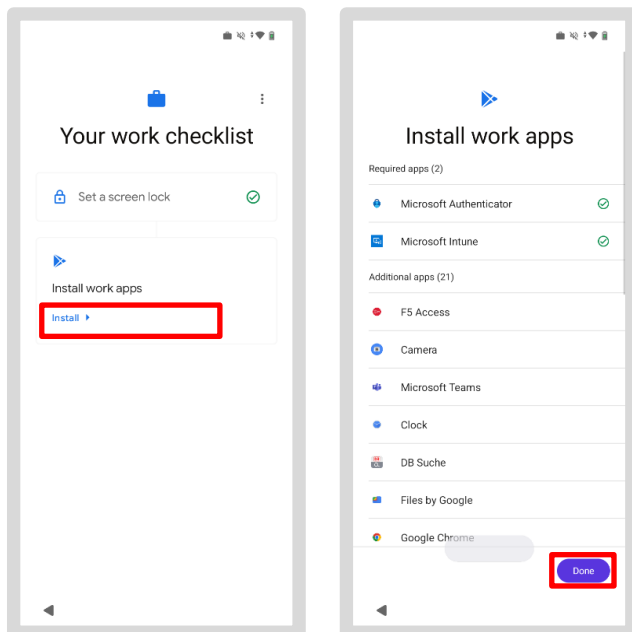


- Zapoznaj się z informacjami dotyczącymi prywatności i użytkowania zawartymi w przewodniku po pierwszej konfiguracji
 - Naciśnij „Dalej”, a następnie „Potwierdź” po dwukrotnym wprowadzeniu informacji
 - Jeśli pojawi się ekran „Konta prywatne”, dotknij „Później” po wyświetleniu monitu
- > Przejdź do sekcji 4.3 Instalowanie aplikacji bazodanowych

4.3 Instalowanie aplikacji DB

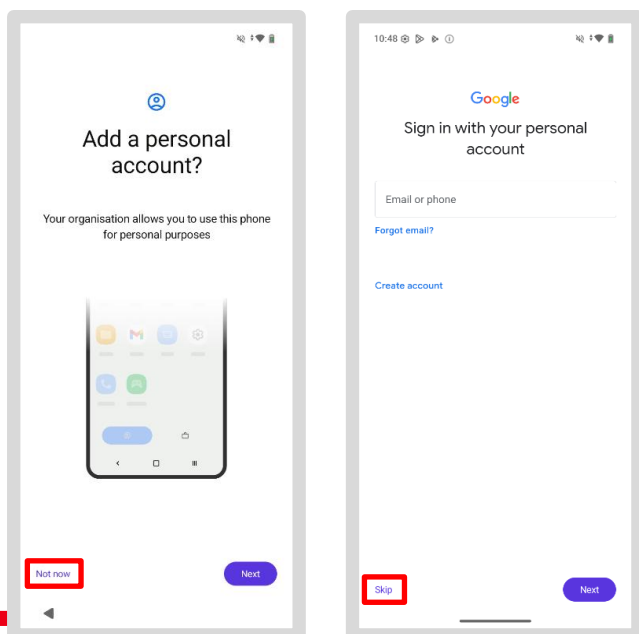
W następnym kroku wszystkie aplikacje DB zostaną ponownie zainstalowane na smartfonie/tablecie DB.

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



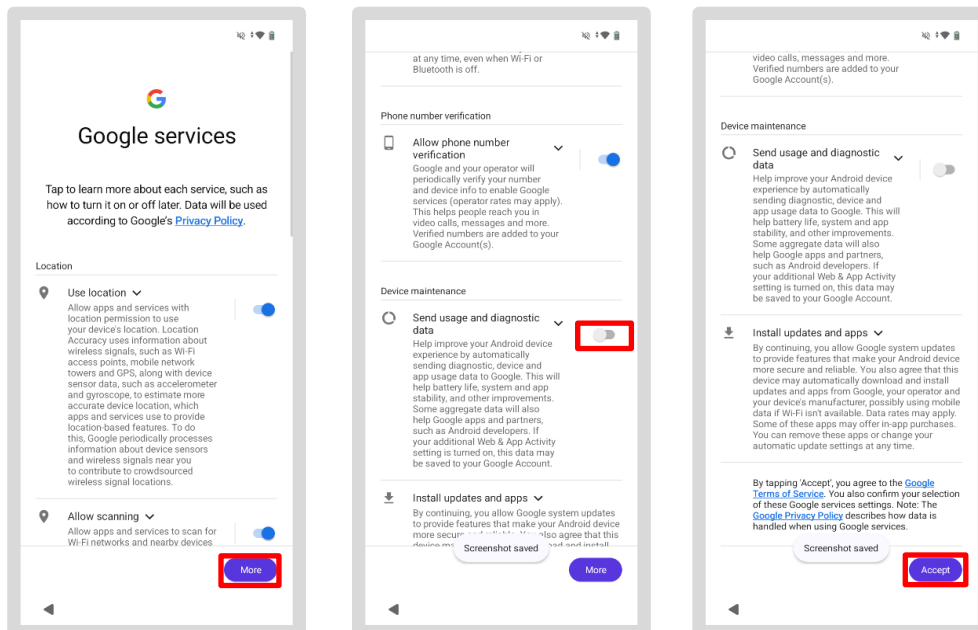
4.4 Konto Google – nie jest wymagane

- Zostaniesz poproszony o podanie osobistego konta Google
- Naciśnij „Później”. Do korzystania ze smartfona lub tabletu DB **nie** jest wymagane **żadne osobiste** konto Google!
- W razie potrzeby możesz to zrobić później
- W następnym kroku dotknij „Pomiń”



4.5 Włącz usługę Google

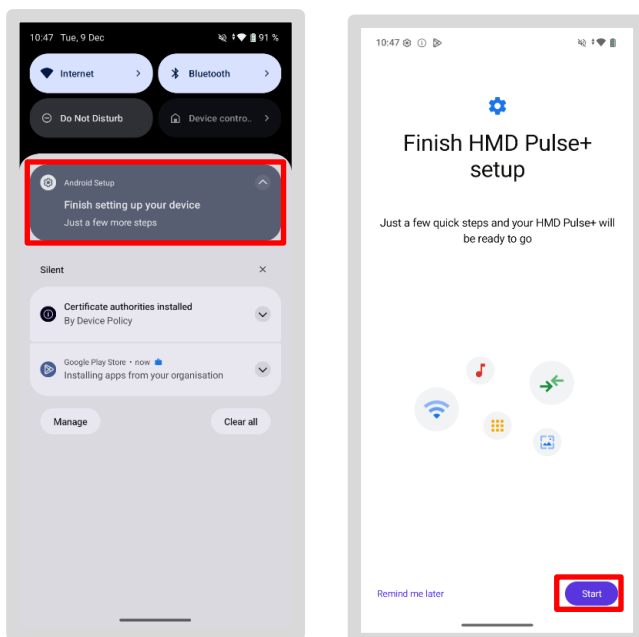
- W sekcji usług Google dotknij „Więcej”
- W sekcji „Wysyłaj dane dotyczące użytkowania i diagnostyki”: wyłącz tę funkcję!
- Przewiń w dół, a następnie dotknij „Akceptuj”



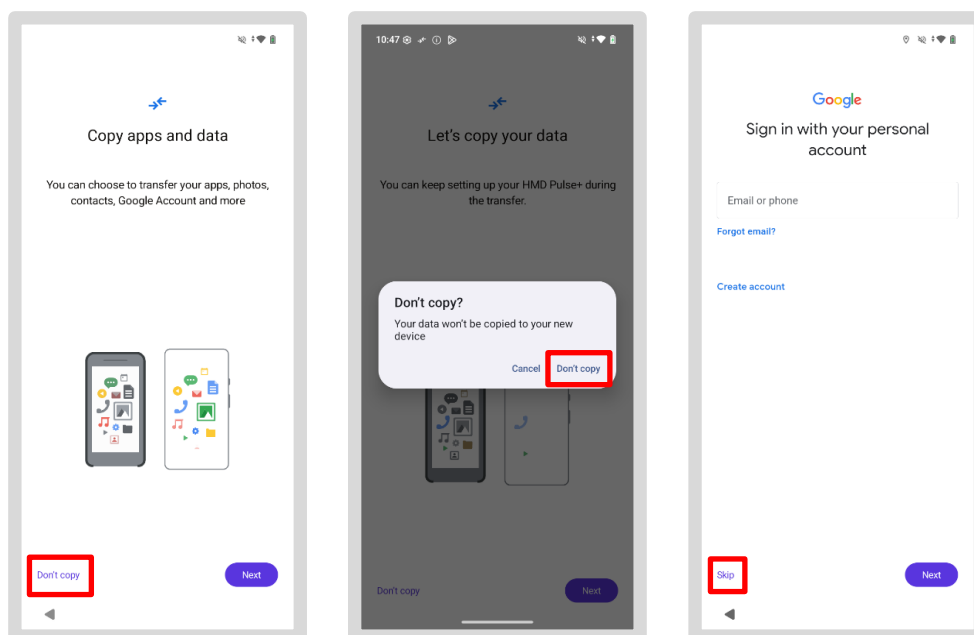
> Następnie przejdź do sekcji 4.6 Zakończ konfigurację – opcjonalnie

4.6 Zakończ konfigurację – opcjonalnie

- Przesuń palcem w dół po ekranie i dotknij opcji „Zakończ konfigurację”
- Naciśnij „Rozpocznij” i poczekaj
- Gdy pojawi się pytanie, czy chcesz skopiować aplikacje i dane, dotknij „Nie kopiuj”

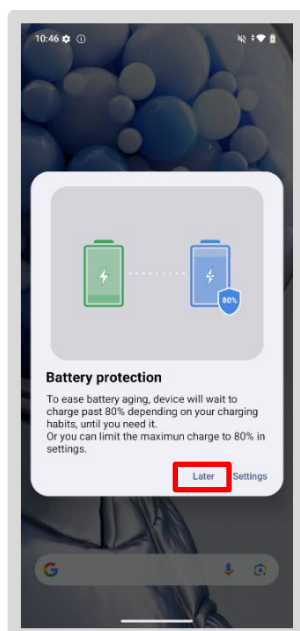


- Gdy pojawi się pytanie o konto osobiste, dotknij „*Pomiń*”
- **Nie** musisz logować się do aplikacji DB za pomocą swojego konta osobistego!



Następnie zostaniesz przeniesiony z powrotem do ekranu głównego:

- Jeśli w tym momencie pojawi się monit o dostęp do ustawień oszczędzania baterii, najpierw dotknij „*Później*”
- To ustawienie możesz zmienić w dowolnym momencie później



- Przesuń palcem w dół od góry ekranu, aby sprawdzić w powiadomieniach, czy jakieś aplikacje są nadal pobierane lub instalowane

- Dotknij powiadomienia, aby sprawdzić, ile aplikacji pozostało do zainstalowania
- Poczekaj chwilę, aż wszystkie aplikacje zostaną zainstalowane

Uwaga: jeśli smartfon/tablet nie działa zgodnie z opisem lub nie wyświetla ekranów pokazanych w niniejszej instrukcji, zresetuj go ponownie. Aby to zrobić, przejdź do Rozdziału 2: Rozpocznij odzyskiwanie: 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 5: Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB

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

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

- Ważna tymczasowa legitymacja pracownika DB (TAP)
- Twoja nazwa użytkownika DB i hasło DB
- *Aplikacja Intune*

Jeśli utworzyłeś już legitymację pracownika DB:

- > Przejdź do rozdziału 6: Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB
- > W przeciwnym razie przejdź do rozdziału 5.1: Utwórz tymczasową legitymację pracownika DB (TAP)

Dla Twojej informacji:

Użytkownik DB to konto użytkownika dla wszystkich pracowników w ramach Grupy DB. Składa się ono z wybranego przez Ciebie hasła oraz automatycznie wygenerowanej nazwy logowania.

- > **Hasło** do konta **DB User** można zresetować na stronie db.de/passwort
- > Instrukcje dotyczące **zmiany hasła** znajdziesz w sekcji „Zmiana hasła użytkownika bazy danych”
- > Informacje o tym, **jak uzyskać nazwę użytkownika bazy danych**, znajdziesz w sekcji „Wymagania wstępne: Użytkownik bazy danych”
- > **Nazwę użytkownika bazy danych** można znaleźć w systemie *DeBI* pod adresem: db.de/debi

5.1 Utwórz tymczasową legitymację pracownika DB (TAP)

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

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

Opcja 1:

Posiadasz **drugi smartfon/tablet** lub komputer w 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 5.2 Utwórz tymczasową legitymację pracownika DB dla współpracownika

Opcja 3 – Tryb ekspercki:

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

- > Rozdział 6 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)

Uwaga: Twoja karta TAP jest ważna tylko przez 60 minut i można jej używać na wielu smartfonach/tabletach!

Jeśli nadal masz zainstalowaną aplikację Welcome:

- otwórz aplikację „Welcome” i dotknij opcji „Pomoc”
- Następnie kliknij „Tymczasową legitymację 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 serwisu DB
- Wybierz opcję „Dla siebie” i naciśnij niebieski przycisk
- Teraz wybierz opcję „DB Workplace Mobile”
- Zostanie wyświetlona tymczasowa legitymacja pracownika DB (TAP)
- Jest on ważny przez 60 minut i można go używać na wielu smartfonach/tabletach

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen. It includes a 'Register' section with a red box around the 'DB User Anmeldenname' field (containing 'Max Mustermann') and the 'DB User Password' field. The right screenshot shows the 'Create a Temporary Access Pass (TAP) - Person selection' screen. It has a red box around the 'For myself' radio button and another red box around the blue arrow button at the bottom right.

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

Uwaga: Będziesz go potrzebować później podczas konfiguracji aplikacji Intune!

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen with a red box around the 'DB Workplace Mobile' option. The right screenshot shows the 'Create a Temporary Access Pass (TAP)' screen with a red box around the generated TAP code 'y&r3%9=cg2u#'. Below the code, it says '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.' At the bottom, there are two buttons: 'Start a new session' and 'To the homepage'.

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

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

Ważne!

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

> Przejdź teraz na stronę

5.2 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 serwisu DB
- Wprowadź swoją nazwę użytkownika DB i hasło DB

The image shows two screenshots of the DB Workplace mobile app interface. The left screenshot is titled 'Create a Temporary Access Pass (TAP)' and shows options to create a TAP for 'yourself' or 'an employee from the same company (see EVI)'. The right screenshot is titled 'Create a Temporary Access Pass (TAP) - Person selection' and shows a search for 'Max Mustermann' with a list of results. The selected user's details are shown: DB User: Max Mustermann, Name: Max Mustermann, E-mail: max.mustermann@db-systel.de, Department: IT, Company: DB Systel GmbH. A checkbox 'I confirm that I have established the employee's identity.' is checked.

- Wybierz opcję „Dla innego pracownika DB” i kliknij niebieski przycisk
- Wybierz właściwą osobę i potwierdź jej tożsamość
- Przekaż kontrolę w aplikacji Teams współpracownikowi (współpracownikom) (jeśli pracujesz zdalnie za pośrednictwem aplikacji Teams)

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 można ją używać na wielu smartfonach/tabletach**
- Przywróć kontrolę nad ekranem, jeśli korzystałeś z aplikacji Teams
- 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=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 skonfigurowania i aktywacji urządzenia w aplikacji Intune
 - Twój współpracownik może teraz aktywować swój smartfon lub tablet w aplikacji Intune
- > Przejdź bezpośrednio do rozdziału 6: Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)

Ważne!

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

Wprowadź **tymczasową legitymację pracownika DB (TAP)** w aplikacji *Intune*.

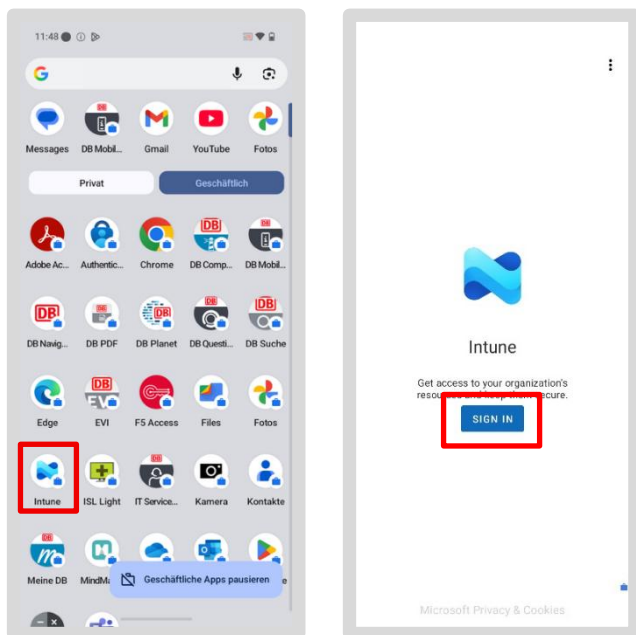
> Przejdź teraz na stronę

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

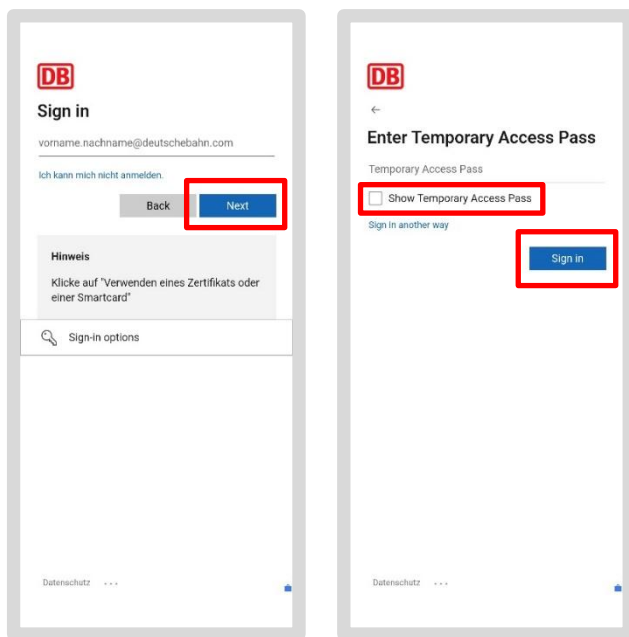
> **Uwaga:** Sprawdź, czy utworzyłeś i otrzymałeś tymczasową legitymację pracownika DB (TAP), zgodnie z opisem w rozdziale 5: Aktywacja urządzenia – utworzenie tymczasowej legitymacji pracownika DB (TAP)!

> **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 „Dalej”
- **Wskazówka:** 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 5: Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)
- > W przeciwnym razie przejdź do rozdziału 6.1: Konfiguracja dostępu do wszystkich aplikacji i stron internetowych bazy danych

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.

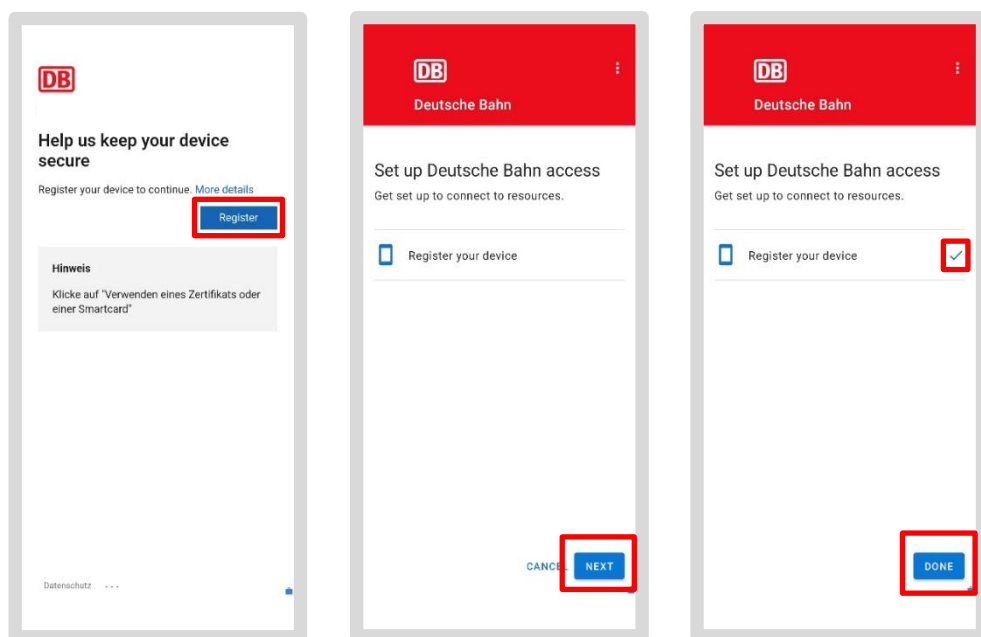
6.1 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB

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 pojawi się, aktywacja nie została zakończona

- Otwórz ponownie aplikację Intune i wykonaj krok po kroku czynności opisane w rozdziale 6. „Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)”



Uwaga:

Po rejestracji poczekaj od 5 minut do 1 godziny

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

6.2 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 aplikacja *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 dostępna jest aplikacja „DB MOBIL”, która zawiera wszystkie informacje, przydatne linki i dane dotyczące smartfona/tabletu DB.

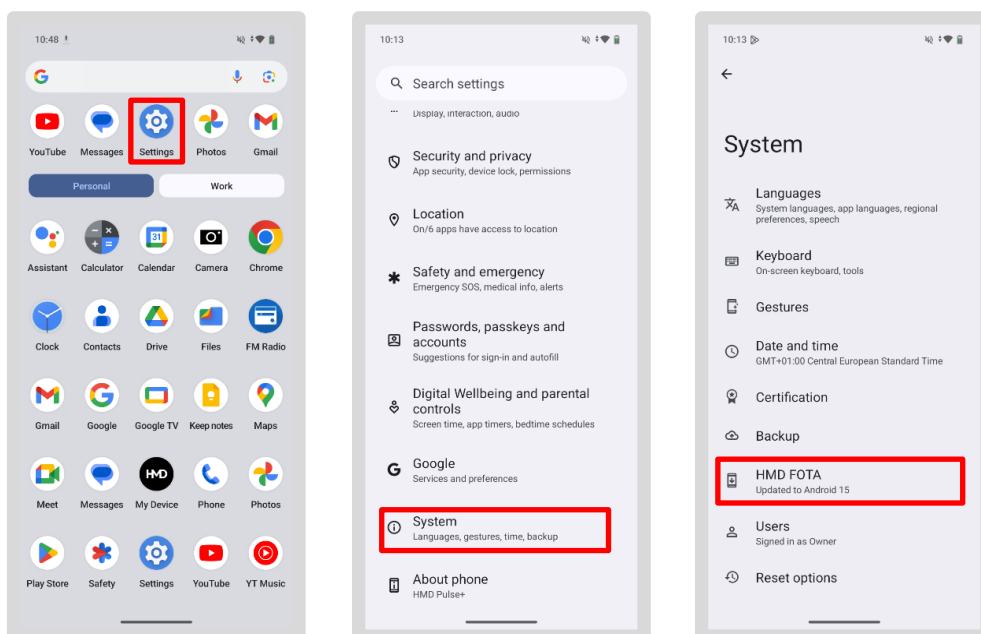
7 Wymagane ustawienia

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

7.1 Sprawdź dostępność aktualizacji systemu operacyjnego

Na smartfonie/tablecie przejdź do sekcji „Osobiste”/„Prywatne”

- Naciśnij aplikację „Ustawienia”
- Następnie przewiń w dół i wybierz „System”
- Teraz dotknij „HMD FOTA”
- Zostanie wyświetlona informacja, czy aktualizacja jest dostępna oraz jaki to rodzaj aktualizacji
- Zainstaluj wszystkie oczekujące aktualizacje, dotykając opcji „Zainstaluj aktualizację”

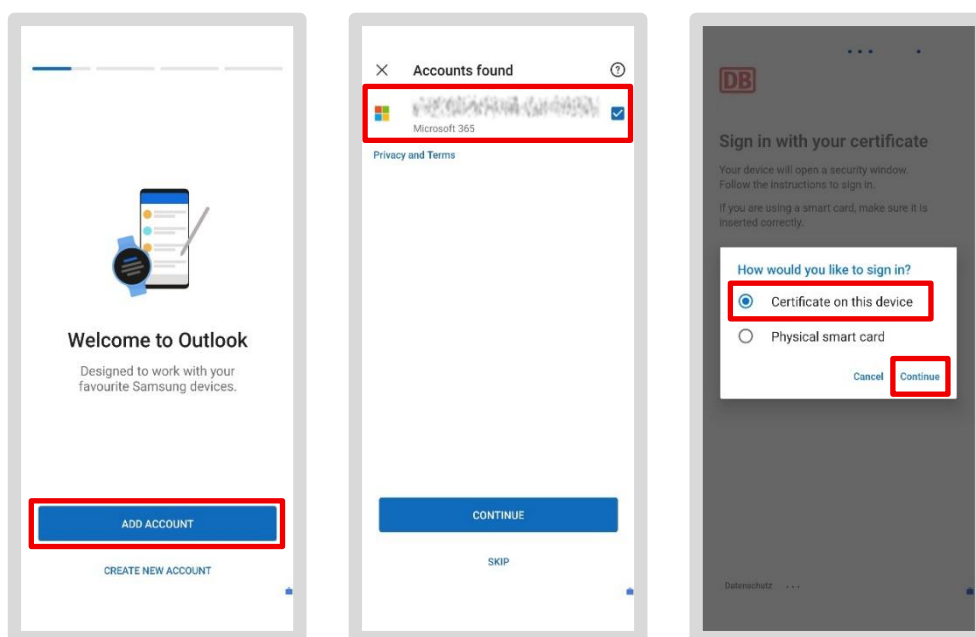


7.2 Outlook

7.2.1 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 5.1 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 wybranie certyfikatu

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

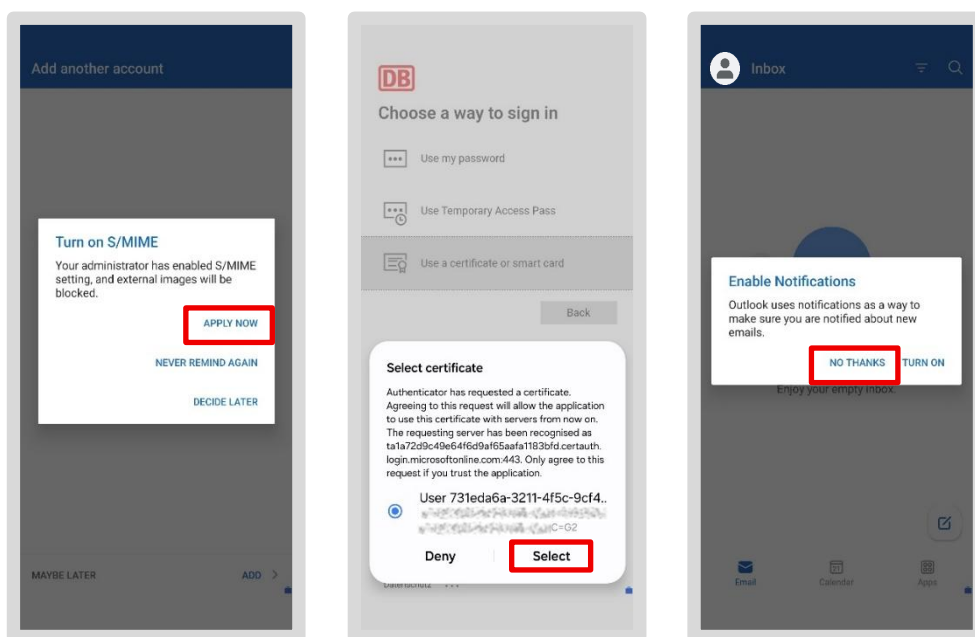
- W tym celu DB udostępnia szyfrowanie S/MIME
- Naciśnij „Zastosuj teraz”, gdy pojawi się pytanie, czy chcesz aktywować S/MIME

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, wybierz opcję „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

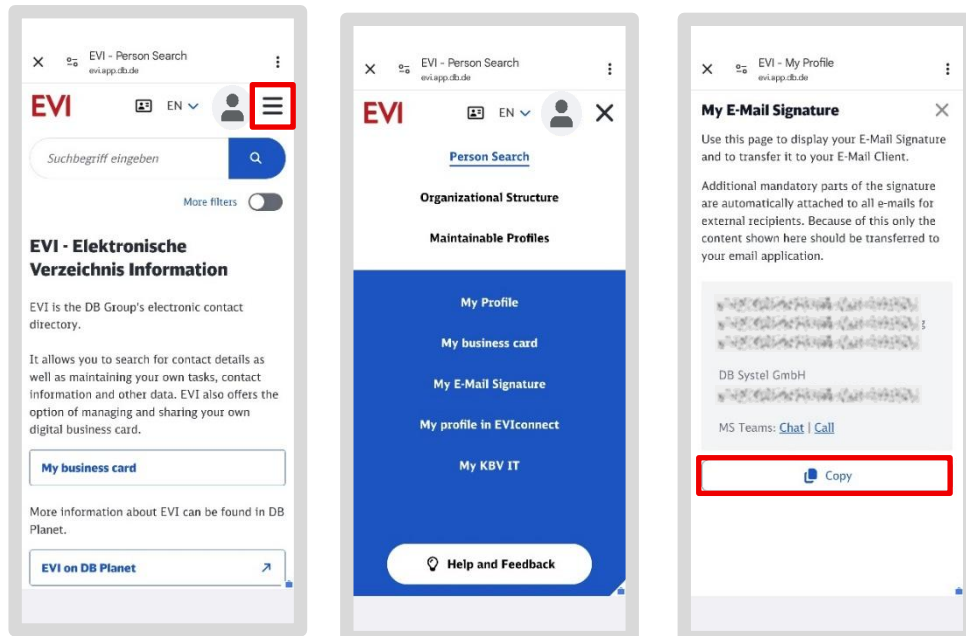
Android 16: Na smartfonach/tabletach z systemem Android 16 krok aktywacji S/MIME może zostać pominięty. W takim przypadku musisz zakończyć konfigurację aplikacji Outlook i ponownie ją uruchomić! Pojawi się wtedy monit o aktywację.

7.2.2 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”.

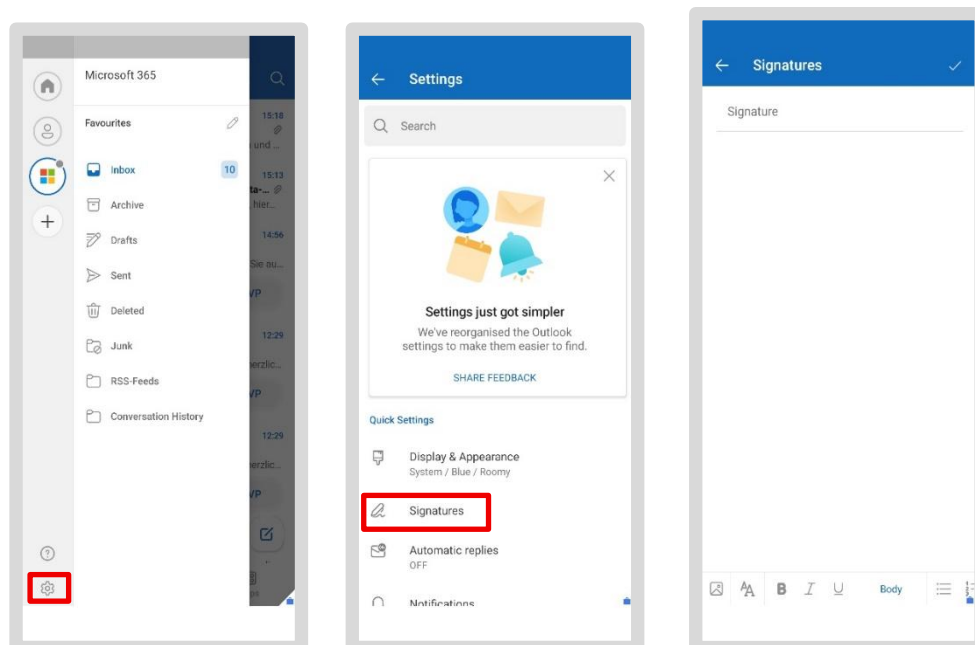
Oto jak pobrać podpis e-mailowy z EVI:

- 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.

7.2.3 Synchronizacja wiadomości e-mail – wszystkie wiadomości zawsze aktualne

Wszystkie Twoje wiadomości e-mail są automatycznie archiwizowane w *aplikacji Outlook* i synchronizowane z połączonym kontem Office. Oznacza to, że niezależnie od tego, z jakiego iPhone’a/iPada korzystasz lub czy logujesz się za pomocą iPhone’a/iPada, czy też komputera BKU/Basic Workplace, zawsze masz dostęp do aktualnych danych.

7.3 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.

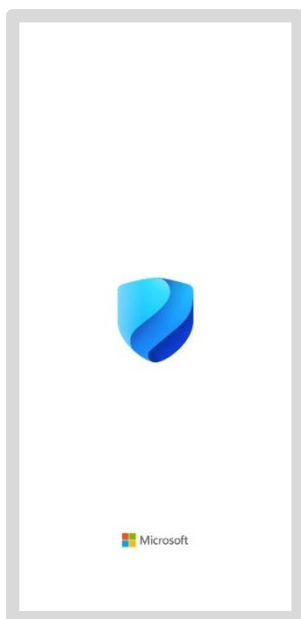
Ze względu na dużą różnorodność smartfonów i tabletów DB mogą występować niewielkie różnice w opisie poszczególnych kroków.

7.3.1 Konfiguracja aplikacji MS Defender

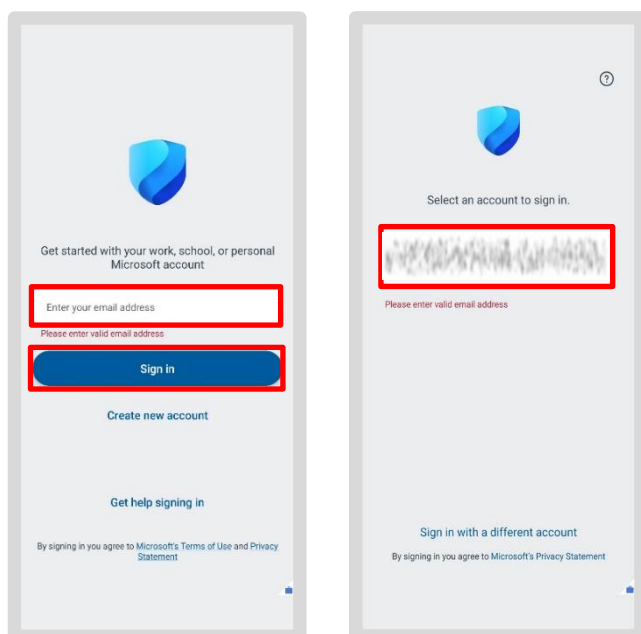
Aby skonfigurować aplikację MS Defender na smartfonie/tablecie, należy wykonać następujące czynności:

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

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

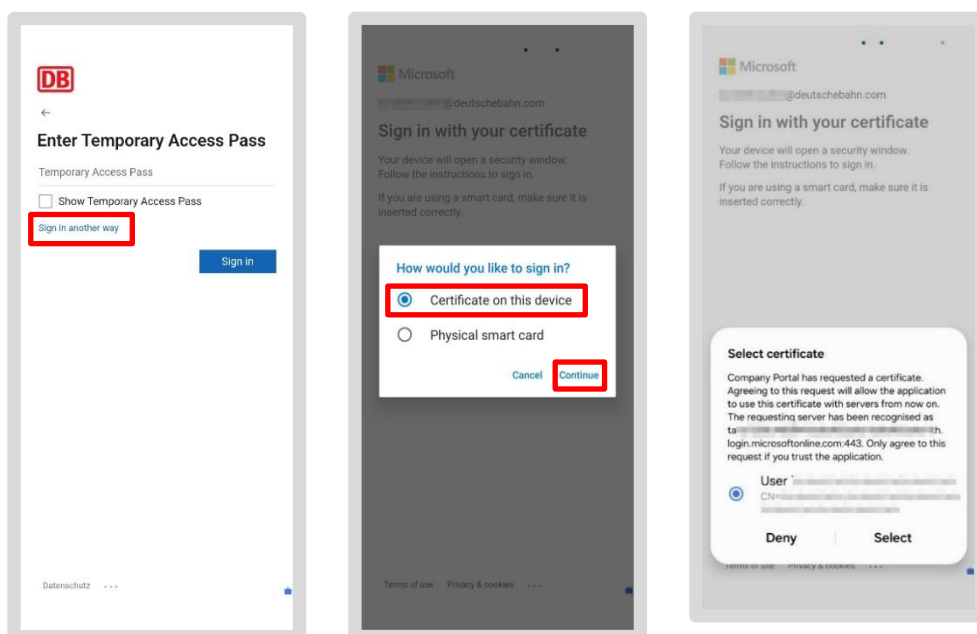


- Zostaniesz poproszony o podanie służbowego adresu e-mail
- Naciśnij przycisk „Zaloguj się” lub aplikacja automatycznie przeniesie Cię do następnego ekranu, na którym wyświetli się Twój adres e-mail
- Dotknij swojego służbowego adresu e-mail



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

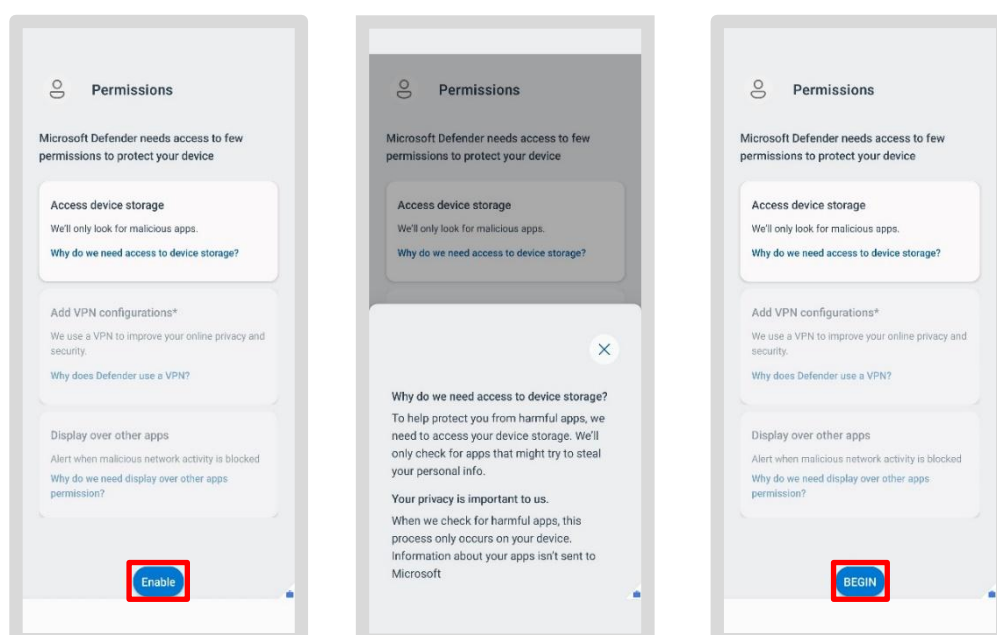
- Naciśnij „Zaloguj się w inny sposób”
- Gdy pojawi się monit, dotknij opcji „*Certyfikat na tym urządzeniu*”, a następnie dotknij „Kontynuuj”
- Wybierz certyfikat



7.3.2 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 „Rozpocznij”
- Otworzy się aplikacja „*Ustawienia*” na smartfonie/tablecie

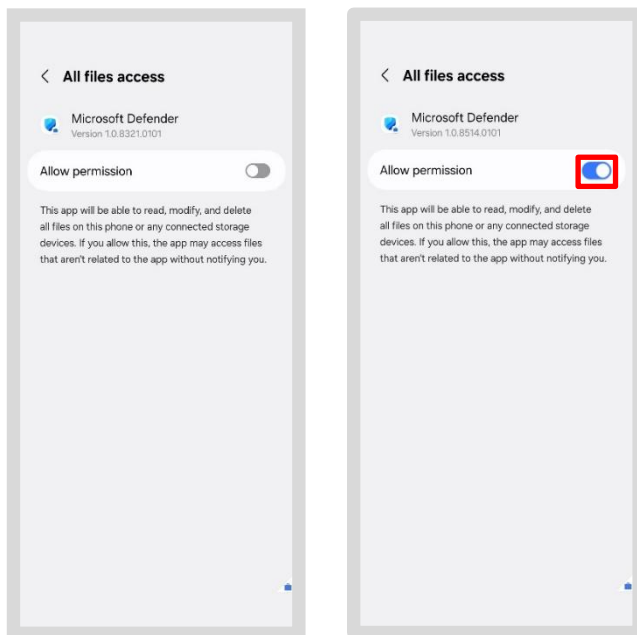


Informacje ogólne dotyczące uprawnień:

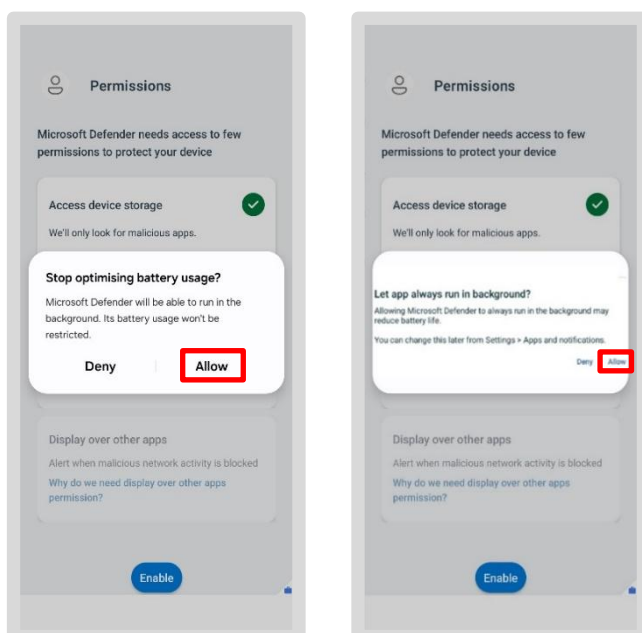
Uprawnienia te są niezbędne do prawidłowego działania aplikacji oraz zapewnienia bezpieczeństwa urządzenia.

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

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



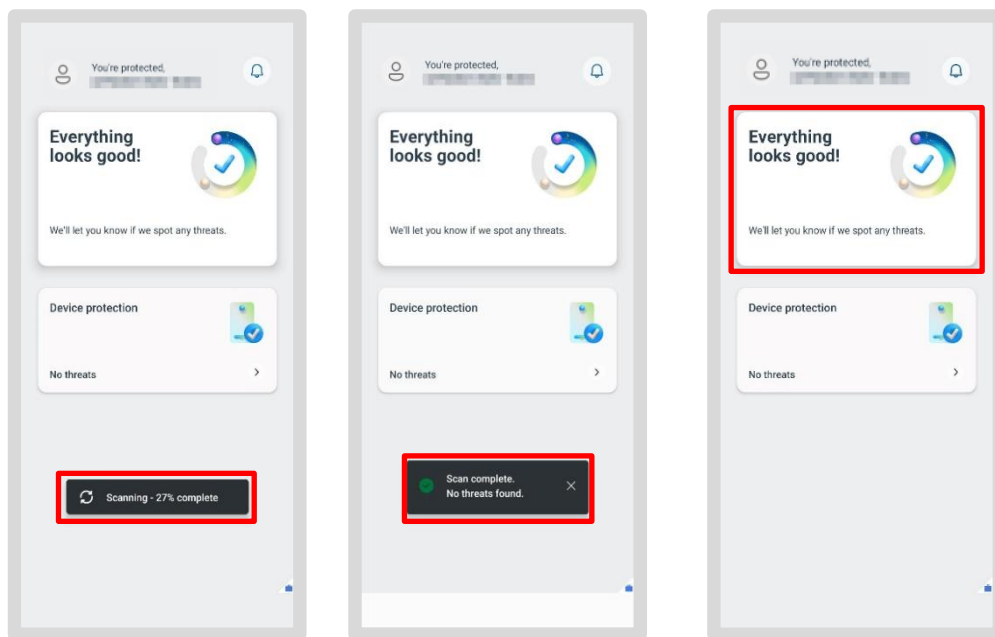
- W przypadku wszystkich kolejnych monitów dotknij „Zezwól”



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 do ekranu głównego 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.

7.4 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



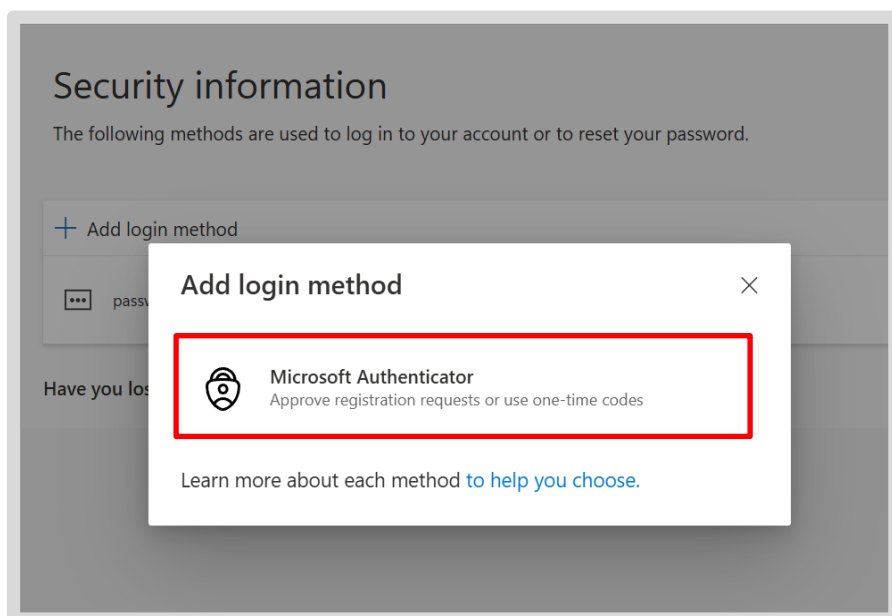
- Następnie dotknij „Zainstaluj”. Aplikacja zostanie pobrana i pojawi się w sekcji „Praca/Biznes”
- Po otwarciu pliku aplikacja uruchomi się automatycznie

Uwaga: w danym momencie można otworzyć tylko jeden plik. Nie ma możliwości, na przykład, jednoczesnego otwarcia kilku plików Word.

7.5 Ponowna aktywacja aplikacji do uwierzytelniania Microsoft Authenticator

Jeśli korzystałeś z aplikacji Authenticator do uwierzytelniania, postępuj w następujący sposób:

- 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, dotknij przycisku „Przewodnik po konfiguracji uwierzytelniania wieloskładnikowego” i postępuj zgodnie z podanymi instrukcjami
- Następnie możesz używać aplikacji Microsoft Authenticator do uwierzytelniania na smartfonie/tablecie
- Jeśli korzystałeś z **aplikacji Authenticator do uwierzytelniania na stronach internetowych lub w narzędziach**, ponownie włącz ją na tych stronach

Wskazówka: Jeśli po odzyskaniu dostępu masz trudności z ponownym aktywowaniem połączeń w aplikacji Authenticator, skorzystaj z opcji samoobsługi: „Zresetuj 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 usłudze OneDrive i zaimportować je z powrotem, znajdziesz w przewodniku konfiguracji w sekcji „Tworzenie kopii zapasowej kontaktów w usłudze OneDrive”

> Szczegółowy przewodnik konfiguracji znajdziesz na stronie db.de/mobile-setup