DB Systel

Betriebssystem-Version ab Android 15

Migration Nokia/HMD
DB Workplace Mobile

DB Systel GmbH | 04.06.2026

Inhaltsverzeichnis

1 Der Ablauf der Migration auf einen Blick

Der gesamte Prozess der Migration auf DB Workplace Mobile hier zusammengefasst:

Planung Migration

- **Sobald du eine E-Mail erhalten hast:**
  Buche einen Termin im PME-Tool
  > siehe Kapitel 2.1 Termin für Migration buchen

Technische Migrationsvorbereitung

- **Erinnerungs-E-Mail** kurz vor dem Termin, dass die Migration starten kann

Persönliche Migrationsvorbereitung

- **Sichere deine Daten**
  > siehe Kapitel 2.2 Daten sichern
- Falls du die Authenticator App nutzt
  > siehe Kapitel 2.3 Authenticator App - optional
- **Führe ein Systemupdate durch** – überprüfe dies in den Systemeinstellungen

Migration auf DB Workplace Mobile

- **Setze** das Smartphone/Tablet **zurück**
  > siehe Kapitel 3 Start Migration: Smartphone/Tablet zurücksetzen
- **Erstell und notiere** den befristeten Zugriffspass (TAP)
  > siehe Kapitel 6 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen
- **Aktiviere** das Smartphone/Tablet in *Microsoft Intune*
  > siehe Kapitel 7 Gerät in der DB aktivieren

Wichtig!

Dein Smartphone/Tablet ist noch nicht mit dem DB Management (Intune) verbunden.

Gibt den **befristeten Zugriffspass (TAP)** in der *Intune App* ein.

Outlook oder Teams sind dafür die falschen Apps!

Folge dieser Anleitung Schritt-für-Schritt!

2 Notwendige Schritte vor der Migration

2.1 Termin für Migration buchen

- **Buche im PME-Tool** db.de/pme **einen Termin für die Migration, sobald du per E-Mail dazu aufgefordert wirst:**
    - Kannst du das nicht selbst tun, lass dies deinen Kostenstellenverantwortlichen oder Bestellberechtigten buchen. Der Termin ist Montag bis Freitag für den Folgewochentag (Mo-Fr) bis 12 Uhr buchbar.
- **Falls du den Migrationstermin nicht einhalten kannst**: Ist eine Terminstornierung bis 12 Uhr am Vortag (Mo-Fr) möglich!
    - **Ab dem gebuchten Tag** der Migration hast du **28 Tage Zeit** dein Smartphone/Tablet zu migrieren. Der letzte mögliche Tag wird in PME angezeigt. Danach wird dein Gerät automatisch gelöscht und auf den DB Workplace Mobile mit *Microsoft Intune* migriert.

2.2 Daten sichern

> **Hinweis:** Eine Video-Anleitung findest du unter db.de/mobile-videoanleitung

- **Sichere deine Daten**, sobald du eine Terminbestätigung per E-Mail für die Migration erhalten hast

  Führe dazu folgende Schritte durch:

  a) Sichere deine dienstlichen Daten und Einstellungen

  b) Sichere deine privaten Daten und Einstellungen

  Falls vorhanden:

  c) Entferne dein Samsung- oder Google-Konto von deinem Smartphone/Tablet

  d) Entferne alle Speicherkarten aus dem Smartphone/Tablet

> Eine Anleitung zur Datensicherung findest du unter Anleitung - Daten sichern

2.3 Authenticator App – optional

Hinweis: Diese Information betrifft nur Nutzer, die die Authenticator App aktiv für bspw. administrative Zugänge mit dem sogenannten 2er Account oder für die Multifaktor-Authentifizierung z.B. für VPN bei einem Basic Workplace MAC nutzen.

- Beachte, dass während der Migration die *Authenticator App* nicht genutzt werden kann
- Es sind keine weiteren Schritte notwendig
- Nach der Migration muss die App erneut aktiviert werden, das wird in Kapitel 8.5 Microsoft Authenticator App wieder aktivieren beschrieben
- Ist es notwendig, dass du während der Migration die Authenticator App nutzen musst, so nimm ein weiteres Smartphone/Tablet, um dieses mit der Authenticator App zu verbinden. Hierzu folge der Schritt-für-Schritt Anleitung zur Einrichtung der Multi-Faktor-Authentifizierung (MFA)

2.4 Erstellen eines befristeten Zugriffspass (TAP) - Expertenmodus

Wenn du nur ein DB Smartphone/Tablet besitzt und ohne fremde Hilfe dein Gerät zurücksetzen kannst, dann erstelle dir vor dem Zurücksetzen den befristeten Zugriffspass (TAP).

> Springe dafür in Kapitel 6.1 Befristeten Zugriffspass (TAP) erstellen

- Setze dann dein Gerät zurück

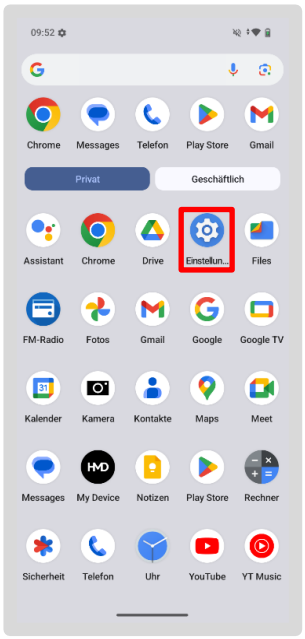
3 Start Migration: Smartphone/Tablet zurücksetzen

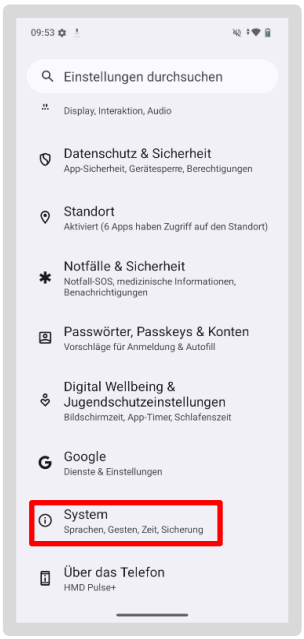
Hinweis: Die nachfolgenden Screens können je nach Gerätemodell des Smartphones/Tablets eine andere Darstellung haben.

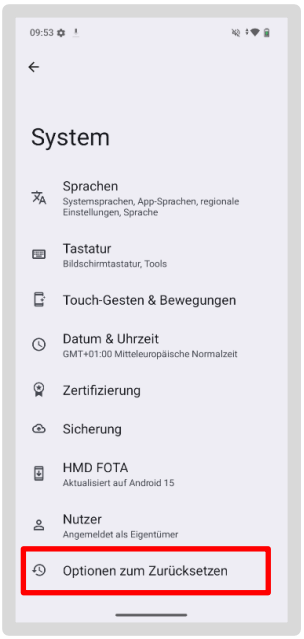
3.1 Smartphone/Tablet selbst zurücksetzen

> **Hinweis:** Eine Video-Anleitung findest du unter db.de/mobile-videoanleitung

- Gehe auf deinem Smartphone/Tablet in den Bereich „Privat“
- Tippe auf die *App Einstellungen*
- Tippe auf „System“ und dann auf „Optionen zum Zurücksetzen“
- Scrolle weiter nach unten und tippe auf „Alle Daten löschen (auf Werkseinstellungen zurücksetzen)“







- Du siehst einen Hinweis, was durch das Zurücksetzen gelöscht wird
- Überprüfe, ob du deine dienstlichen Daten (Anleitung: Daten sichern) gesichert hast
- Tippe anschließend den Button „Alle Daten löschen“, gib deine Bildschirmsperre (PIN oder Passwort) ein und tippe auf „Alle Daten löschen“
- Warte einige Minuten ab, dein Smartphone/Tablet wird automatisch zurückgesetzt

> Gehe dann zu Kapitel 4 Erneut einrichten

3.2 Smartphone/Tablet über die IT ServiceDesk App zurücksetzen

Sollte dein Smartphone/Tablet nicht mehr funktionieren, dann wähle diesen Schritt:

- Öffne die IT ServiceDesk App und gib unter „Neues Serviceanliegen“ deinen Auftrag für das Zurücksetzen deines Smartphones/Tablets ein
- Falls du die App nicht öffnen kannst, wähle diese Nummer:
- IT ServiceDesk Migrations-Hotline (Mo-Fr 7:00-18:00)
    - Intern: Tel. 9833-8699
    - Extern: Tel. 0361 430 8699
- IT ServiceDesk
    - Intern: Tel. 91-5555
    - Extern: Tel. 0361 430 8200
    - Hier den Menüpunkt 0 wählen
- IT ServiceDesk DB Cargo

Tel. 91 7777 (internal)

Tel. 00800 327 978 35 (external)

    - Hier den Menüpunkt 0 wählen

- Wenn andere Dinge auftauchen, so überlege Dir schon vorab:
    - An **welcher Stelle traten Probleme** auf?
    - **Definiere die Fehlerstelle**; um dir schneller Support zu liefern
    - **Bei Zertifikatsproblemen**: Warte im Anschluss an die Registrierung **von 5 Minuten bis 24 Stunden** bis alle Informationen und Zertifikate auf das Smartphone/Tablet übertragen wurden.

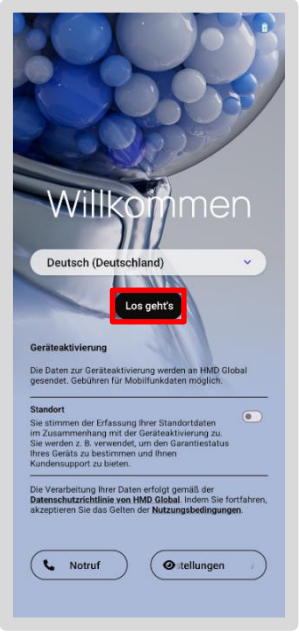
> Gehe dann zu Kapitel 4 Erneut einrichten

4 Erneut einrichten

4.1 Sprache auswählen

> **Hinweis:** Eine Video-Anleitung findest du unter db.de/mobile-videoanleitung

- Halte dein Tablet im **Hochformat**, um die Screens in der gleichen Darstellung zu erhalten, wie sie in der Anleitung dargestellt sind
- Schalte dein Smartphone/Tablet ein
- Achte darauf, dass dein Smartphone/Tablet während der Migration entweder an die Stromversorgung angeschlossen ist oder einen hohen Akkustand hat
- Prüfe, ob die gewünschte Sprache ausgewählt ist. Falls nicht, passe sie an
- Tippe dann auf „Los geht‘s“
- Falls eine SIM-Karte in deinem Smartphone/Tablet eingelegt ist, folge den Schritten auf dem Screen
- Tippe beim nächsten Screen auf „Überspringen“



4.2 WLAN einrichten

Wähle zum Einrichten deines WLANs eine dieser Möglichkeiten:

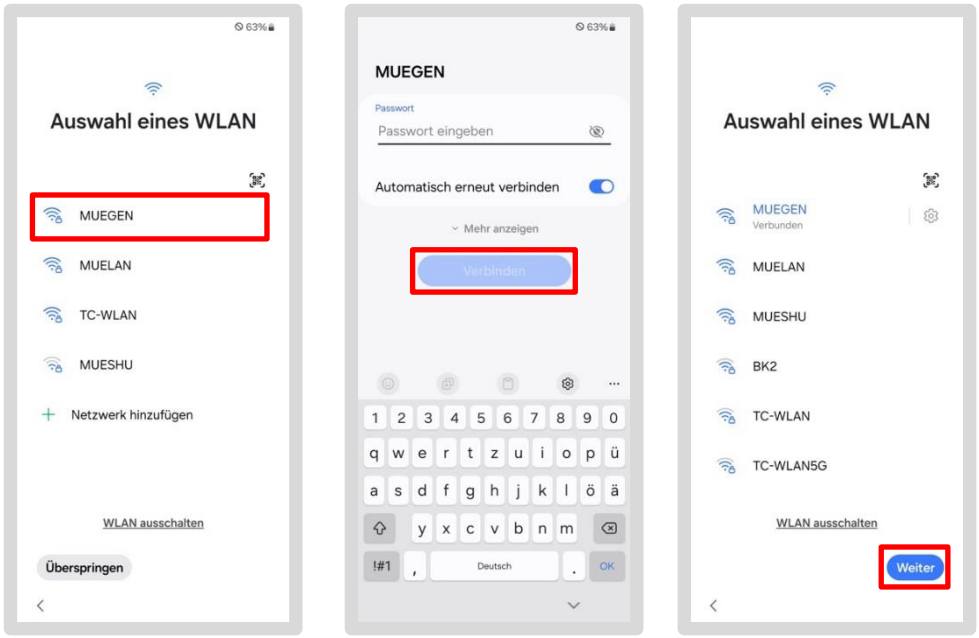
- Nutze deine **mobilen Daten**, sofern eine SIM Karte in deinem Smartphone/Tablet vorhanden ist (das könnte unter Umständen kostenpflichtig sein!)
- Richte einen Hotspot mit deinem privaten Smartphone/Tablet ein

oder

- Nutze einen Hotspot aus dem DB Smartphone deines/er Kollegen:in
- Nutze dein privates WLAN, sofern du im Homeoffice arbeitest

Bei der Auswahl eines anderen WLANs gehe so vor:

- Tippe auf das auszuwählende WLAN
- Gib deine persönlichen Anmeldedaten ein und tippe auf „Verbinden“
- Bei einer zweiten Anfrage tippe auf „Weiter“



Sobald dein Smartphone/Tablet mit dem WLAN verbunden ist, startet die Verknüpfung mit dem DB Netzwerk.

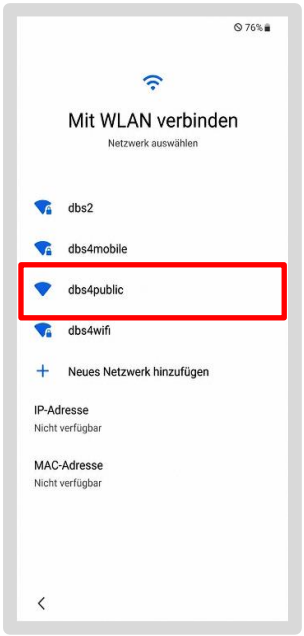
> Gehe zu Kapitel 5 Nokia/HMD installieren

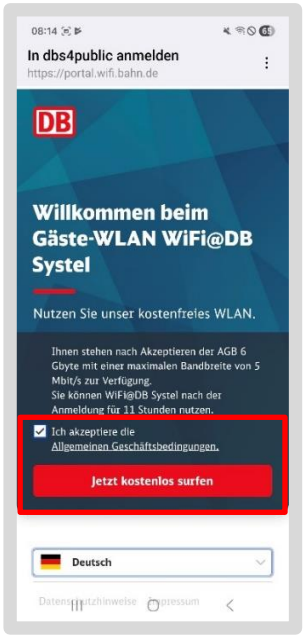
4.3 WLAN einrichten im DB Gebäude

Da das WLAN „dbs4public“ in den DB Gebäuden nicht immer zufriedenstellend funktioniert, empfehlen wir die Auswahl eines der Schritte, die in Kapitel 3.2 WLAN einrichten vorgestellt werden.

Wenn du dich in einem **DB Gebäude** befindest und das WLAN „dbs4public“ nutzen möchtest, gehe so vor:

- Tippe auf das WLAN „dbs4public“
- Es öffnet sich ein Dialog, akzeptiere die AGB
- Tippe auf „Jetzt kostenlos surfen“
- Tippe auf „Schließen“





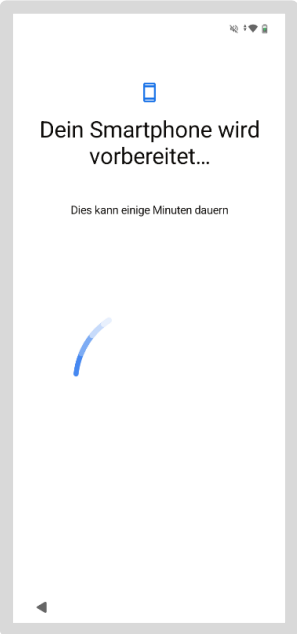
Sobald dein Smartphone/Tablet mit dem WLAN verbunden ist, startet die Verknüpfung mit dem DB Netzwerk.

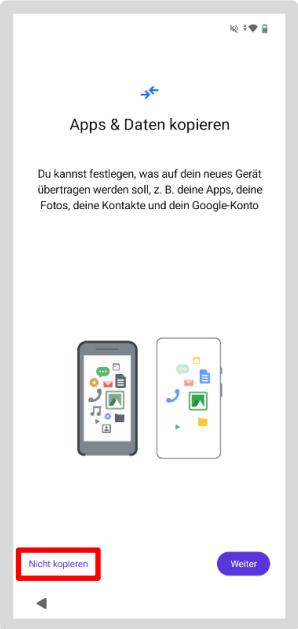
> Gehe zu Kapitel 5 Nokia/HMD installieren

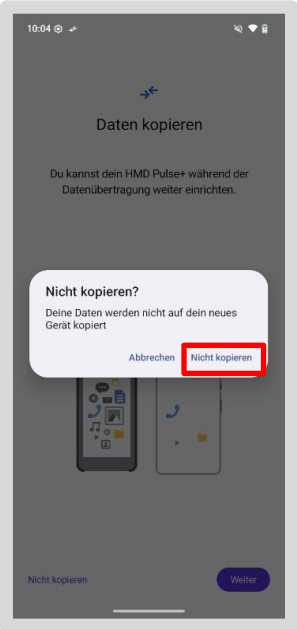
5 Nokia/HMD installieren

Im nächsten Schritt muss dein DB Smartphone/Tablet wieder mit dem DB Management (genauer im Enterprise Mobility Management, kurz EMM) verknüpft werden. Warte bei den wechselnden Informationen, bis eine Anweisung erscheint. Je nach Netzverbindung, rauschen oder wechseln die Screens durch.

- Halte dein Tablet im **Hochformat**, wenn du es bis hier im Querformat gehalten hast
- Es wechseln nun einzelne Screens durch
- Sollte bereits an dieser Stelle eine Abfrage zum Kopieren von Apps & Daten erscheinen, tippe zunächst auf „Nicht kopieren“ und bei erneuter Abfrage nochmals auf „Nicht kopieren“



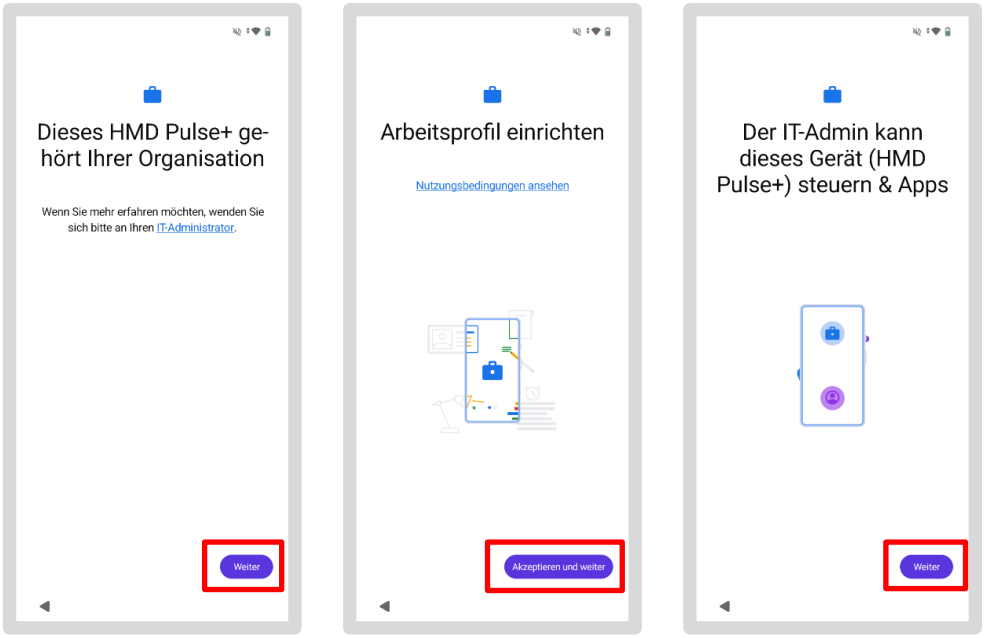




5.1 Arbeitsprofil einrichten

Damit die dienstlichen Apps auf deinem Smartphone/Tablet zugeordnet werden, braucht es ein Arbeitsprofil. Das muss hier eingerichtet werden:

- Das Smartphone/Tablet wird nun eingerichtet
- Bestätige die folgende Abfrage mit „Weiter“
- Bestätige den folgenden Screens mit „Akzeptieren & weiter“ und „weiter“



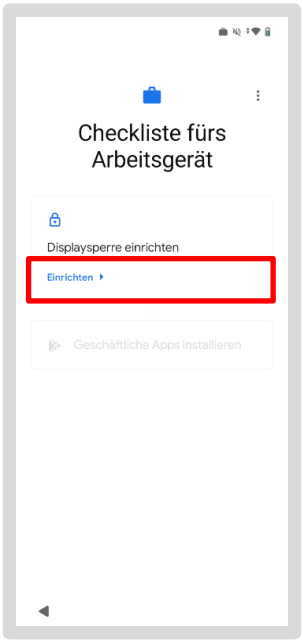
- Die Aktualisierung des Smartphones/Tablets kann etwas oder auch teilweise sehr lange dauern, gedulde dich hier!
- Die erforderlichen Apps werden installiert

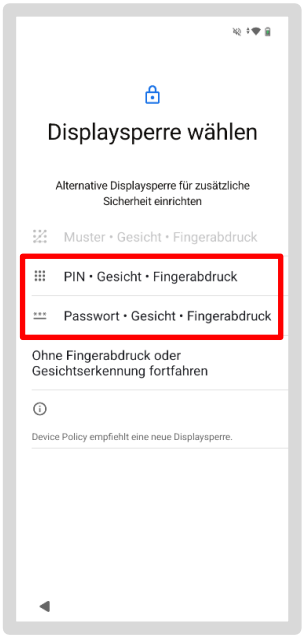
> Gehe zu Kapitel 5.2 Bildschirmsperre festlegen

5.2 Bildschirmsperre festlegen

Im nächsten Schritt richtest du die Bildschirmsperre für dein Smartphone/Tablet ein. Diese ist bei der DB aus Datenschutzgründen verpflichtend und schützt deine Daten zuverlässig.

- Tippe auf „Einrichten“
- Wähle selbst, was für dich die beste Option ist. Tippe auf eine der zwei Optionen (PIN oder Passwort) und lege dann deine eigene, persönliche Bildschirmsperre fest
- Achte darauf, dass das neue Passwort eine neue Zahlenkombination aus 6 Ziffern hat





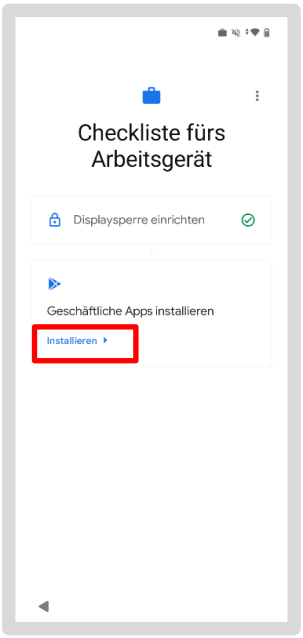
- Achte auf die Datenschutz- und Nutzungshinweise in der Anleitung Ersteinrichtung
- Bestätige mit „Weiter“ und dann bei zweimaligem Eingeben mit „Bestätigen“
- Falls der Screen „Private Konten“ kommt: Tippe bei der Abfrage auf „Später“

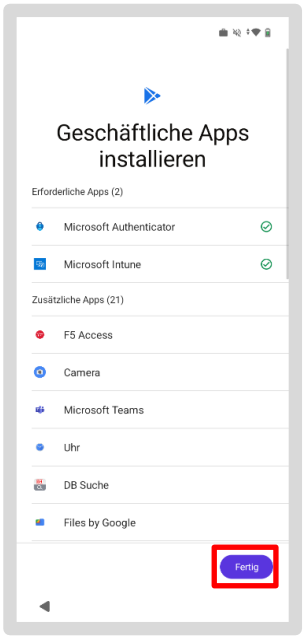
> Gehe zu Kapitel 5.3 DB Apps installieren

5.3 DB Apps installieren

Im nächsten Schritt werden für dein DB Smartphone/Tablet wieder alle DB Apps installiert.

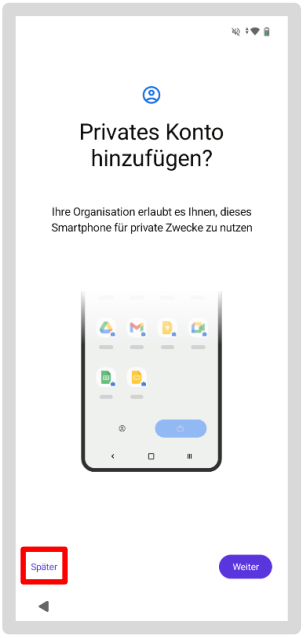
- Tippe auf „Installieren“
- Scrolle nach unten und tippe auf „Fertig“

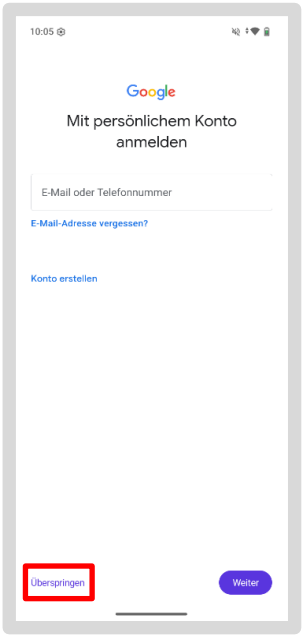




5.4 Google Konto – nicht notwendig

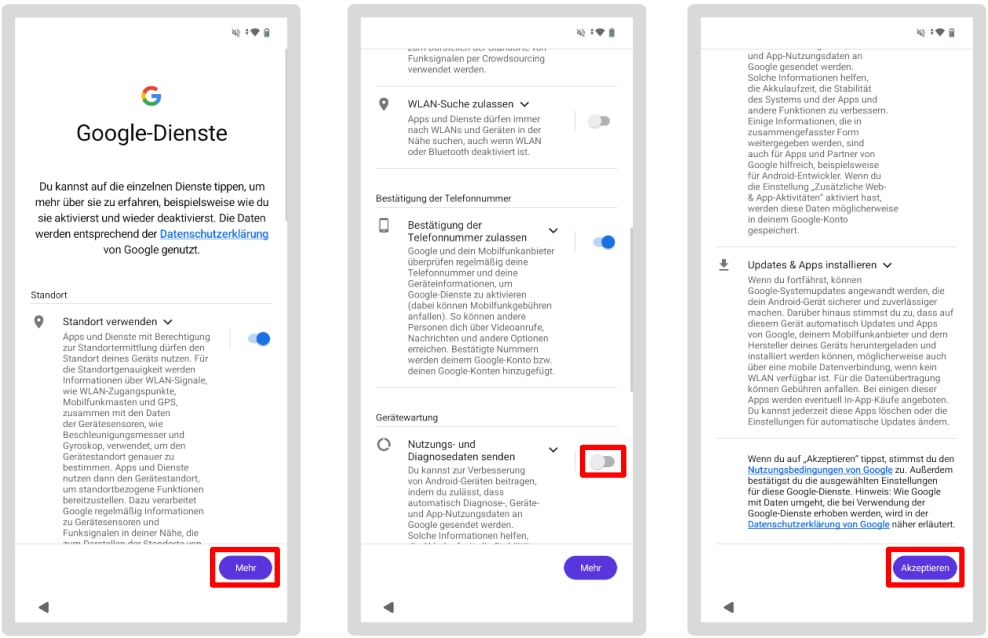
- Es kommt die Abfrage für ein privates Google Konto
- Tippe auf „Später“. Für dein DB Smartphone/Tablet wird **kein privates** Google Konto benötigt!
- Bei Bedarf kannst du dies später nachholen
- Tippe deshalb im nächsten Schritt auf „Überspringen“





5.5 Google Dienst aktivieren

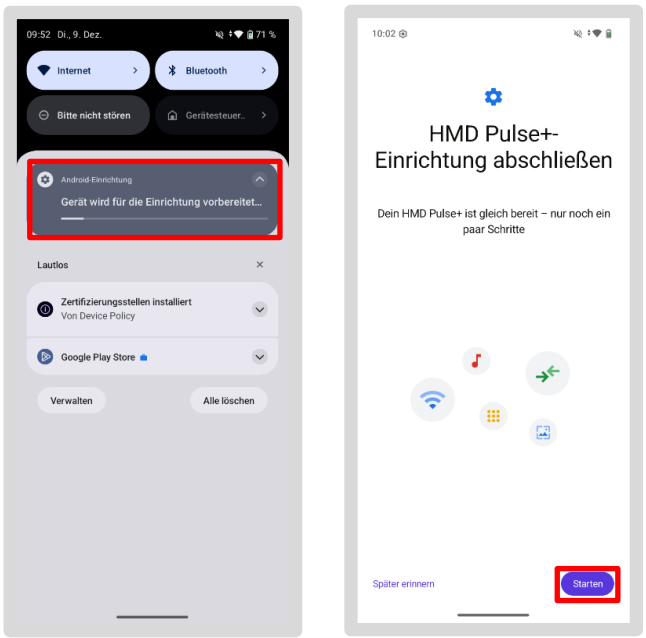
- Tippe auf „Mehr“ bei den Google Diensten
- Bei **Nutzungs- und Diagnosedaten senden:** Schalte die Funktion aus!
- Scrolle weiter und tippe dann auf „Akzeptieren“



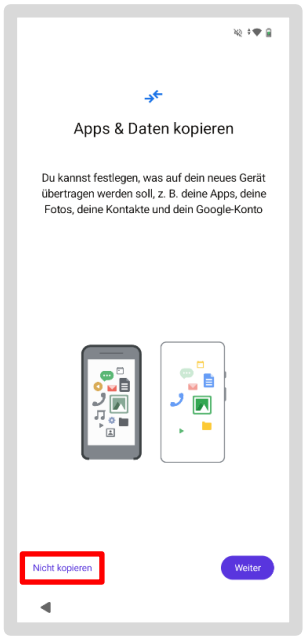
> gehe zu Kapitel 5.6 Einrichtung abschließen

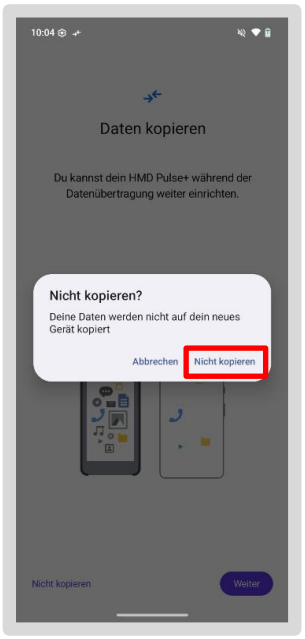
5.6 Einrichtung abschließen

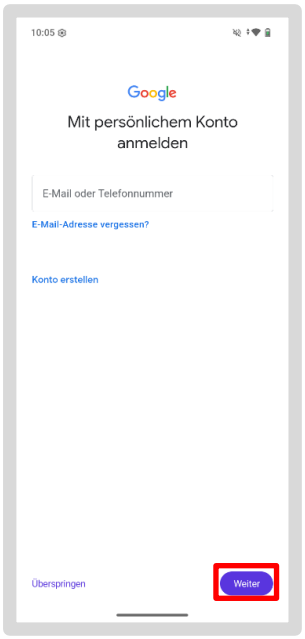
- Wische deinen Screen nach unten und tippe auf „Einrichtung abschließen“
- Tippe auf „Starten“ und warte
- Tippe bei der Abfrage zum Kopieren von Apps & Daten auf „Nicht kopieren“



- Tippe bei der Abfrage nach deinem persönlichen Konto auf „Überspringen“
- Mit deinem persönlichen Konto musst du dich **nicht** für die DB Apps anmelden!







Anschließend gelangst du wieder auf deinen Startbildschirm:

- Wenn du bereits an dieser Stelle zu den Einstellungen für den Batterieschutz aufgefordert wirst, tippe zunächst auf „Später“
- Diese Einstellung kannst du jederzeit noch nachträglich anpassen

- Wische von oben nach unten, um in den Benachrichtigungen zu sehen, ob noch Apps geladen oder installiert werden

- Tippe auf die Benachrichtigung, um zu sehen, wie viele Apps noch installiert werden müssen
- Warte hier eine Weile, bis alle Apps installiert sind

Hinweis: wenn dein Gerät sich nicht so verhält oder die Screens anzeigt, die hier in der Anleitung gezeigt werden, setze es nochmal zurück. Gehe dafür zu Kapitel 3 Start Migration: dein Smartphone/Tablet zurücksetzen

Wichtig!

Dein Smartphone/Tablet ist noch nicht mit dem
DB Management (Intune) verbunden.

Gibt den **befristeten Zugriffspass (TAP)**
in der *Intune App* ein.

Folge dafür der Schritt-für-Schritt-Anleitung in
> Kapitel 6 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen

6 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen

Um dein Smartphone/Tablet im DB-Management einzurichten, brauchst du diese Dinge:

- Einen gültigen befristeten Zugriffspass (TAP) - db.de/tap
- deinen DB User Name und DB User Passwort
- die *Intune App*

Nur zur Info:

Der DB User ist das Benutzerkonto für alle Mitarbeitenden im DB Konzern. Er besteht aus einem selbst gewählten Passwort und einem automatisch generierten Anmeldenamen.

> Dein **DB-User-Passwort** kannst du unter db.de/passwort zurücksetzen

> Eine Anleitung zum **Passwort ändern**, findest du in DB User Passwort ändern

> **Wie du deinen DB User erhältst** findest du in Vorbedingung: DB User

> Deinen **DB User Name** findest du in DeBI unter: db.de/debi

6.1 Befristeten Zugriffspass (TAP) erstellen

> **Hinweis:** Eine Video-Anleitung findest du unter db.de/mobile-videoanleitung

Um den befristeten Zugriffspass (TAP) zu erstellen, gibt es mehrere Varianten:

Variante 1:

Du besitzt **ein zweites Smartphone/Tablet** oder einen BKU/ Basic-Workplace Rechner, der schon im DB Management angemeldet ist. Bleibe in diesem Fall in dem aktuellen Kapitel und fahre auf der nächsten Seite fort.

Variante 2:

Ein/e Kollege/in aus dem gleichen Unternehmen (wie DB Vertrieb oder DB Fernverkehr) unterstützt dich sofern er/sie ein DB Smartphone/Tablet (oder iPhone/iPad) oder ein BKU/Basic Workplace Rechner besitzt. Gehe hier zu:

> Kapitel 6.2 Befristeten Zugriffspass für eine(n) Kollegen:in erstellen

Variante 3 - Expertenmodus:

Du besitzt **nur ein Smartphone/Tablet** und konntest es noch so weit nutzen, dass du dir bereits vor dem Zurücksetzen einen befristeten Zugriffspass (Tap) erstellt hast. Notiere dir deinen Zugriffspass und gehe zu:

> Kapitel 3 Start Migration: Smartphone/Tablet zurücksetzen

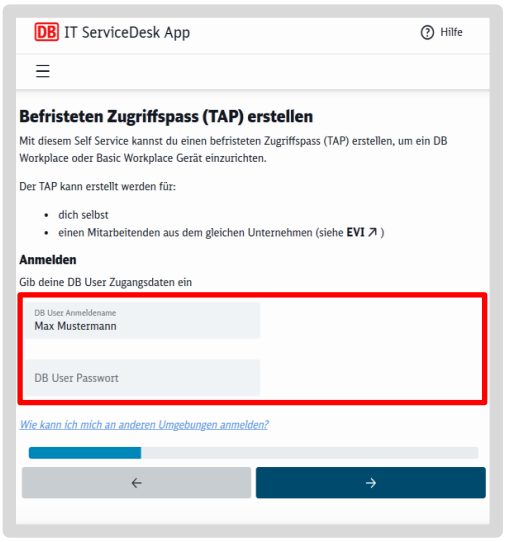
Beachte: Dein Tap ist nur 60 Minuten und für mehrere Smartphones/Tablets gültig!

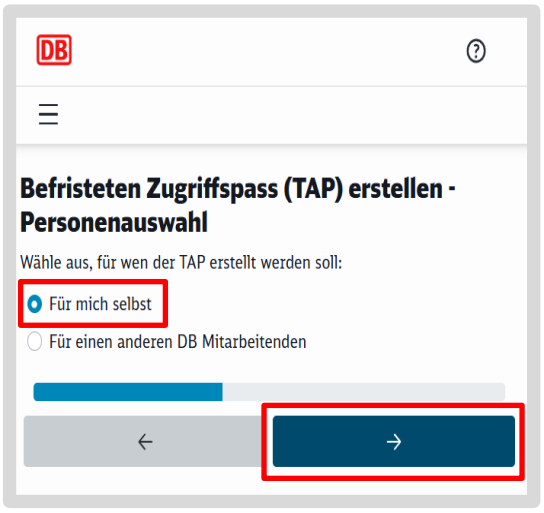
Wenn du die Willkommen App noch installiert hast:

- öffne die *Willkommen App* und tippe auf „Hilfe“
- Klicke anschließend auf „Befristeten Zugriffspass (TAP)“, um diesen zu erstellen

Wenn du die Willkommen App nicht installiert hast:

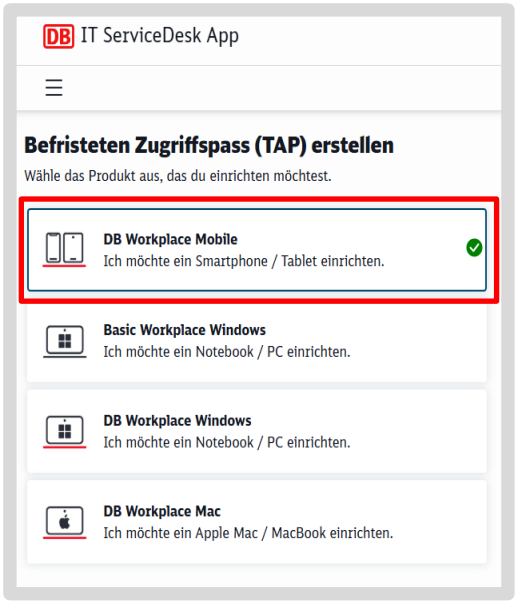
- Öffne deinen Standardbrowser
- Gehe auf db.de/tap und gib deinen DB User Namen und dein DB User Passwort ein
- Wähle „Für mich selbst“ aus und tippe auf den blauen Button
- Wähle nun „DB Workplace Mobile“ aus
- Danach wird dir der befristete Zugriffspass (TAP) angezeigt
- Dieser ist nun 60 Minuten und für mehrere Smartphones/Tablets gültig

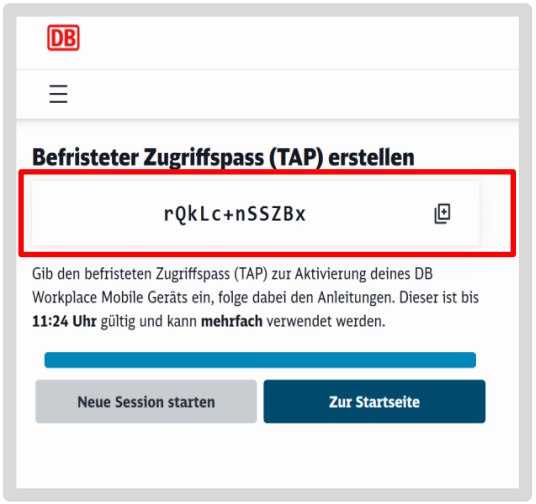




- Notiere dir den befristeten Zugriffspass (TAP) auf einen Zettel oder Notizheft

Beachte: Du brauchst ihn später bei der Einrichtung in der **Intune App!**





Wichtig!
Der **TAP** darf nur in der **Intune App** eingegeben werden, selbst wenn du in einer anderen DB App oder auf einem anderen Gerät danach gefragt wirst.

- Notiere dir den befristeten Zugriffspass (TAP) auf einen Zettel oder Notizheft
- Du brauchst ihn später bei der Einrichtung und Aktivierung in der *Intune App*
- Du kannst jetzt dein Smartphone/Tablet in der *Intune App* aktivieren

> Gehe direkt weiter zu Kapitel 7 Gerät in der DB aktivieren

Wichtig!

Dein Smartphone/Tablet ist noch nicht mit dem DB Management (Intune) verbunden.

Gibt den **befristeten Zugriffspass (TAP)** in der *Intune App* ein.

Folge dafür der Schritt-für-Schritt-Anleitung in
> Kapitel 7 Gerät in der DB aktivieren

6.2 Befristeten Zugriffspass für eine(n) Kollegen:in erstellen

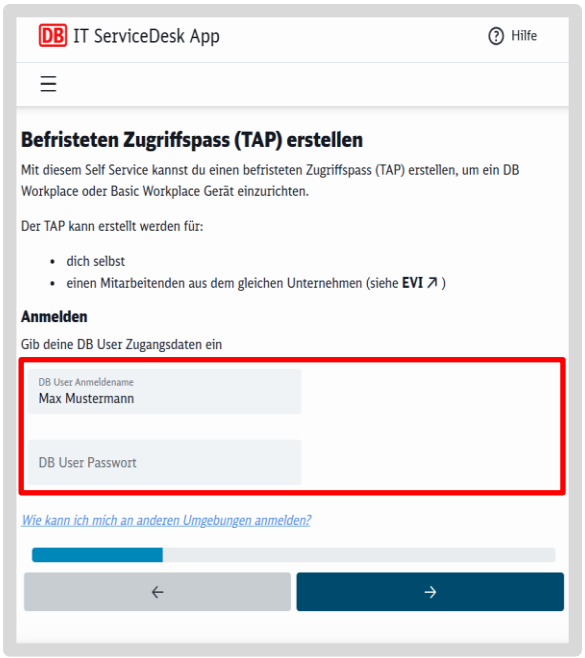
Um für eine(n) Kollegen:in einen TAP zu erstellen befolge folgende Anweisungen:

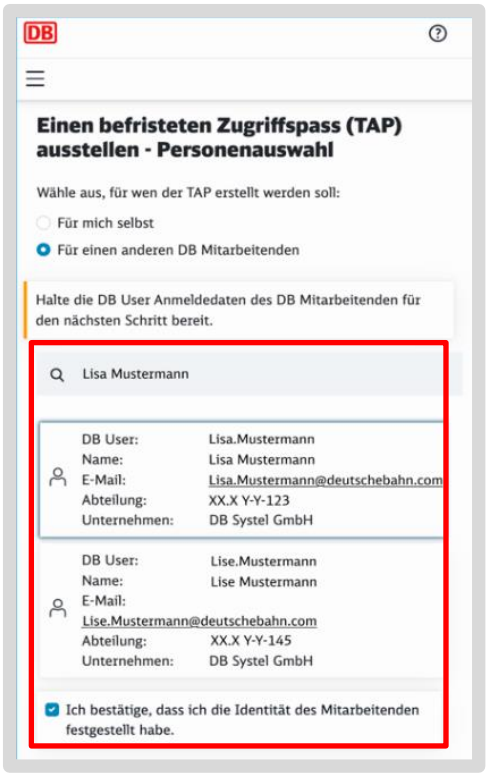
Wenn du die Willkommen App noch installiert hast:

- öffne die *Willkommen App* und tippe auf „Hilfe“
- Klicke anschließend auf „Befristeten Zugriffspass (TAP)“, um diesen zu erstellen

Wenn du einen DB Workplace Windows oder Mac besitzt:

- Öffne den Standardbrowser
- Gehe auf db.de/tap und gib deinen DB User Namen und dein DB User Passwort ein
- Gib deinen DB User Namen und dein DB User Passwort ein
- Wähle „Für einen anderen DB Mitarbeiter“ aus und tippe auf den blauen Button

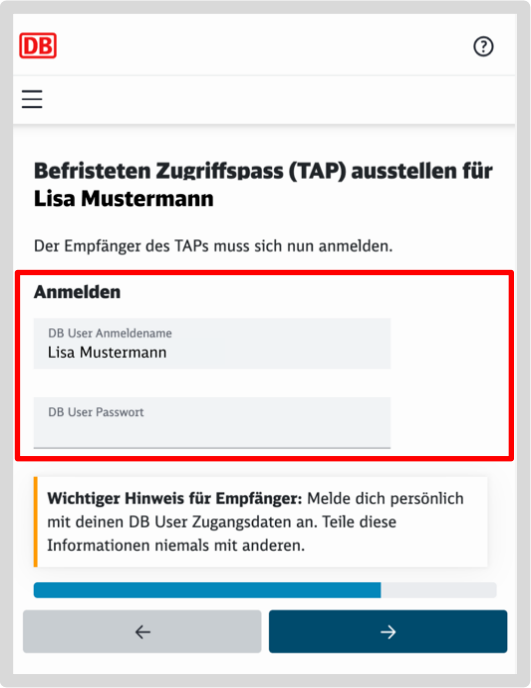


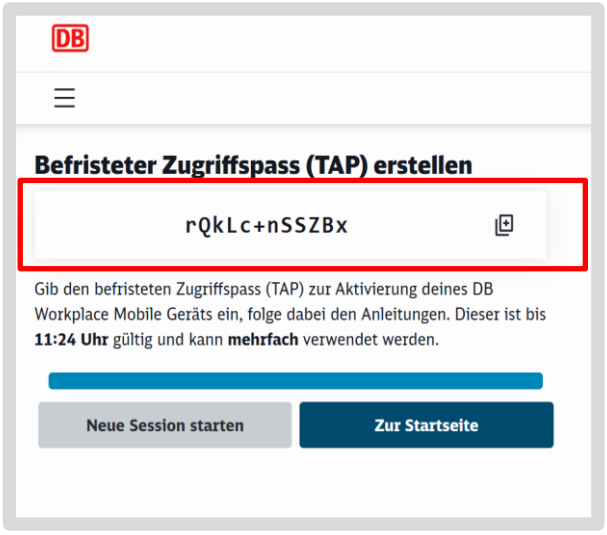


- Wähle die richtige Person aus und bestätige die Identität
- Gib die Steuerung in Teams an den/die Kollege:in (wenn remote über Teams gearbeitet wird)

oder

- Lass die/den Kollege:in an den Rechner
- Die/den DB Kollege:in gibt das DB User Passwort ein
- Danach wird der Zugriffspass angezeigt, **dieser ist 60 Minuten und für mehrere Smartphones/Tablets gültig**
- Hole die Bildschirmsteuerung wieder zurück, falls du Teams genutzt hast
- Notiere den befristeten Zugriffspass auf einen Zettel oder Notizheft





- Du brauchst ihn später zur Einrichtung und Aktivierung in der *Intune App*
- Der/die Kollegen:in kann jetzt sein Smartphone/Tablet in der *Intune App* aktivieren

> Gehe direkt weiter zu Kapitel 7 Gerät in der DB aktivieren

Wichtig!

Dein Smartphone/Tablet ist noch nicht mit dem DB Management (Intune) verbunden.

Gibt den **befristeten Zugriffspass (TAP)** in der *Intune App* ein.

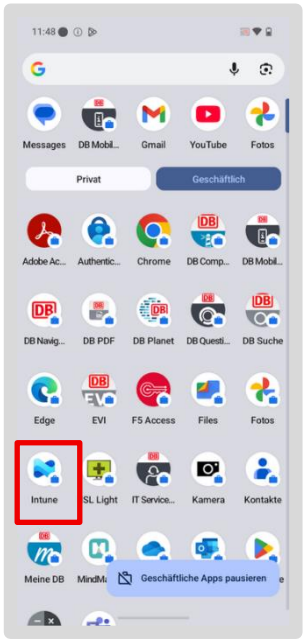
Folge dafür der Schritt-für-Schritt-Anleitung in
> Kapitel 7 Gerät in der DB aktivieren

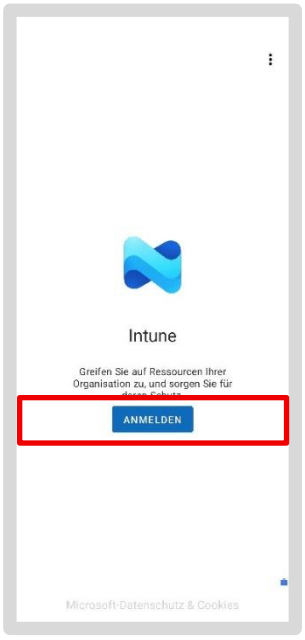
7 Gerät in der DB aktivieren

> **Beachte**: Prüfe, ob du einen befristeten Zugriffspass (TAP) wie in Kapitel 6 Befristeten Zugriffspass (TAP) erstellen beschrieben und erhalten hast!

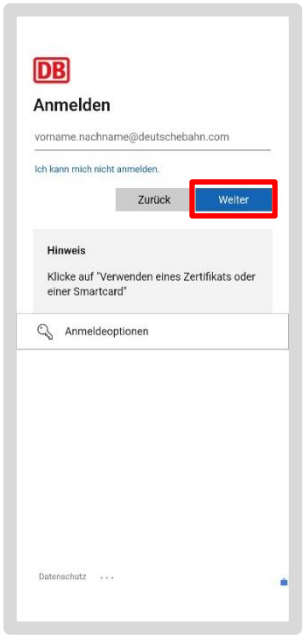
> **Hinweis:** Eine Video-Anleitung findest du unter db.de/mobile-videoanleitung

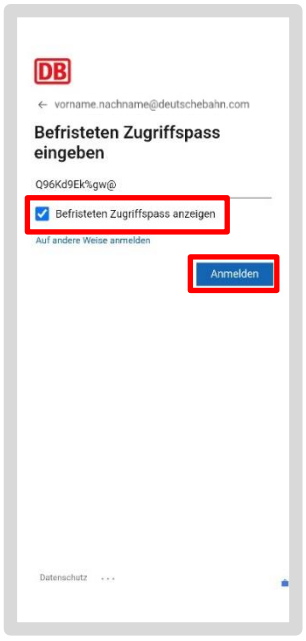
- Öffne die *App Intune*
- Tippe dann auf den Button „Anmelden“





- Gib deine **DB User E-Mail-Adresse** ein (Nicht: DB User) und tippe auf „Weiter“
- **Tipp:** Setze den Haken bei „Befristeten Zugriffspass anzeigen“
- Gib deinen befristeten Zugriffspass ein und tippe auf „Anmelden“





Wenn du eine Fehlermeldung erhältst:

- Erstelle dir einen neuen befristeten Zugriffspass und wiederhole die Anmeldung, wie in Kapitel 6 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen beschrieben

> Ansonsten gehe zu Kapitel 7.1 Zugriff auf alle DB Apps und Webseiten einrichten

Hinweis: Solange der befristete Zugriffspass (TAP) gültig ist (innerhalb der 60 Minuten) und du z.B. Outlook, Teams oder die IT ServiceDesk App öffnest, wirst du nach dem befristeten Zugriffspass gefragt, tippe deinen notierten befristeten Zugriffspass auch hier ein.

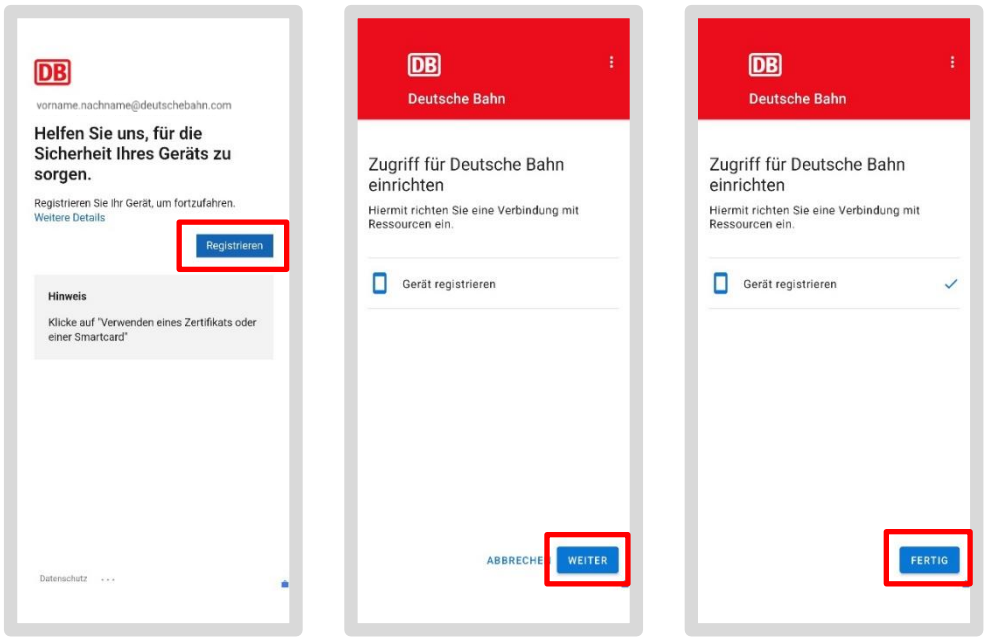
7.1 Zugriff auf alle DB Apps und Webseiten einrichten

Nun wird der Zugriff auf das DB Management (Intune) eingerichtet:

- Tippe auf „Registrieren“ und dann auf „Weiter“
- Wenn der Haken bei „Gerät registrieren“ erscheint, tippe auf den Button „Fertig“

Beachte: Wenn der Button „Fertig“ nicht erscheint, ist die Aktivierung nicht abgeschlossen

- Öffne nochmal die *Intune App* und gehe nochmal die Schritte ab dem Kapitel 6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP) Schritt für Schritt durch



Hinweis:

Warte im Anschluss an die Registrierung von 5 Minuten bis 1 Stunde

bis alle Informationen und Zertifikate auf das Smartphone/Tablet übertragen wurden. Danach kannst du deine Apps wie Outlook, Teams, etc. nutzen.

7.2 DB Apps

Beachte: Die Bereitstellung der Zertifikate kann ***5* Minuten bis 24 Stunden** dauern. Erst danach kannst du deine Apps wie Outlook, Teams, etc. nutzen.

Nach Abschluss der Einrichtung laden sich die DB Apps, wie z.B Outlook-App oder Teams-App automatisch herunter.

Deine unternehmensspezifischen bzw. geschäftsfeldspezifischen Apps werden danach geladen.

Weitere DB Apps kannst du aus dem dienstlichen Google Play Store (die App mit dem Koffersymbol) im Bereich „Geschäftlich“ herunterladen.

Die **Willkommen App** ist **nicht mehr** auf dem DB Smartphone/Tablet, dafür gibt es die **App DB Mobile Info** mit allen Informationen, nützlichen Links und Daten rund um dein DB Smartphone/Tablet.

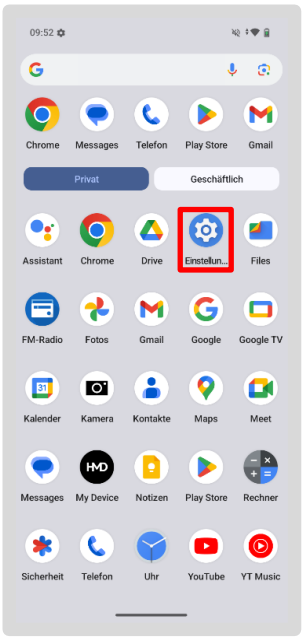
8 Notwendige Einstellungen

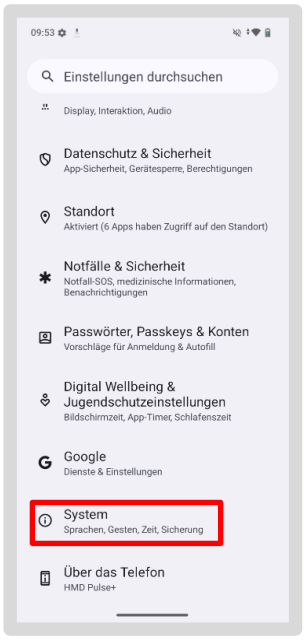
Beachte: Die Bereitstellung der Zertifikate kann **5 Minuten bis 24 Stunden** dauern. Erst danach kannst du deine Apps wie Outlook, Teams, etc. nutzen.

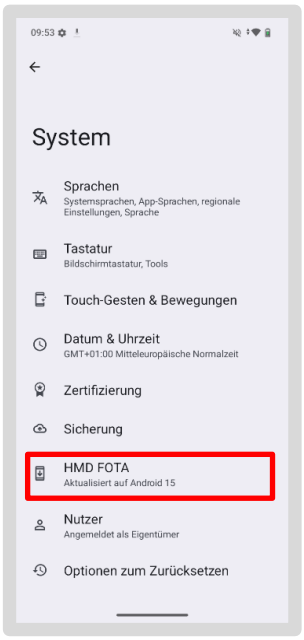
8.1 Nach Betriebssystem Updates suchen

Gehe auf deinem Smartphone/Tablet in den Bereich „Persönlich“/“Privat“

- Tippe auf die App „Einstellungen“
- Scrolle dann nach unten und wähle „System“
- Tippe nun auf „HMD FOTA“
- Dort steht, ob und was für ein Update angeboten wird
- Führe anstehende Updates durch, tippe dafür auf „Update installieren“





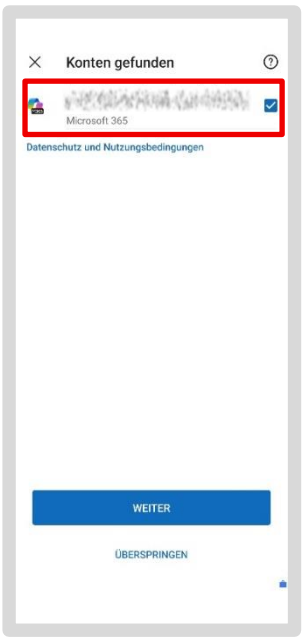


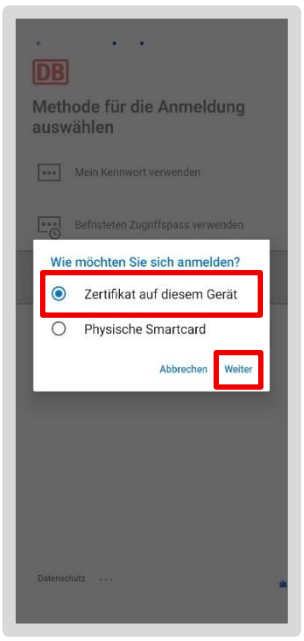
8.2 Outlook

8.2.1 Outlook einrichten/E-Mail-Konto erstellen/E-Mail-Verschlüsselung einrichten

> **Hinweis:** Eine Video-Anleitung findest du unter db.de/mobile-videoanleitung

- Gehe in deinem Bereich „Arbeit/Geschäftlich“ und tippe dort auf die App „Outlook“
- Dein E-Mail-Konto sollte bereits automatisch hinterlegt sein – tippe dann auf „Konto hinzufügen“
- Wähle im nächsten Schritt deine E-Mail-Adresse aus und tippe auf „Weiter“





Bei der Abfrage nach der Anmeldung kann es sein, dass du nach einem TAP gefragt wirst:

- Falls dein befristeter Zugriffspass noch gültig ist, gib diesen hier ein oder erstelle dir einen neuen, wie in Kapitel 6.1 Befristeten Zugriffspass (TAP) erstellen beschrieben
- Alternativ: wähle unter „andere Anmeldeoption wählen“ die Option „Zertifikat auf diesem Gerät“ aus
- Tippe auf „Auswählen“ bei der Zertifikatsabfrage

Sofern du besonders schützenswerte Daten (z.B. Personaldaten) per E-Mail versenden möchtest, musst du zusätzlich den Inhalt der E-Mail verschlüsseln

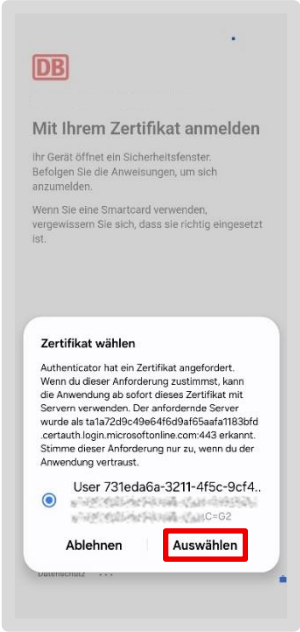
- Die DB stellt dafür die sogenannte S/MIME-Verschlüsselung zur Verfügung
- Tippe auf „Jetzt übernehmen“ bei der Abfrage, ob du S/MIME aktivieren möchtest

Danach kommt die Zertifikatsabfrage. Das für dich gültige Zertifikat erkennst du so:

- Erste Zeile: "**User** ds2232… (dann Zahlen und Buchstaben)
- Zweite Zeile: „**CN**- **DB User Namen**“ z.B. LisaMustermann 89sd7es0ßwd (dann Zahlen und Buchstaben)
- Wähle den Textschnipsel aus und tippe auf „Auswählen“

Dein E-Mail-Konto wird nun eingerichtet:

- Tippe auf „Vielleicht später“ bei der Abfrage für ein weiteres Konto hinzufügen
- Und „Nein Danke“ bei Benachrichtigung aktivieren



- Deine E-Mails werden nun geladen (dieser Prozess kann einige Minuten dauern)
- Anschließend kannst du wieder E-Mails lesen und schreiben

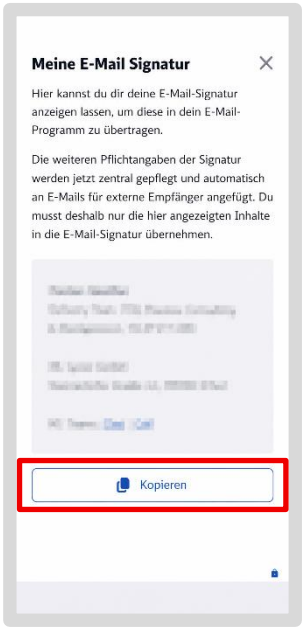
Android 16: Bei Geräten mit Android 16 kann es vorkommen, dass der Schritt zur Aktivierung von S/MIME übersprungen wird. In diesem Fall muss die Einrichtung von Outlook abgeschlossen und die App neu gestartet werden! Anschließend erscheint die Abfrage zur Aktivierung.

8.2.2 E-Mail Signatur einrichten

Eine E-Mail Signatur ist ein verpflichtender Bestandteil der dienstlichen Kommunikation. Sie steht am Ende einer E-Mail und muss laut Gesetz bestimmte Informationen enthalten, wie z.B. den Firmennamen und den offiziellen Sitz deines DB-Unternehmens. Den Text für deine E-Mail Signatur findest du im zentralen Telefonbuch der DB, dem sogenannten „EVI“.

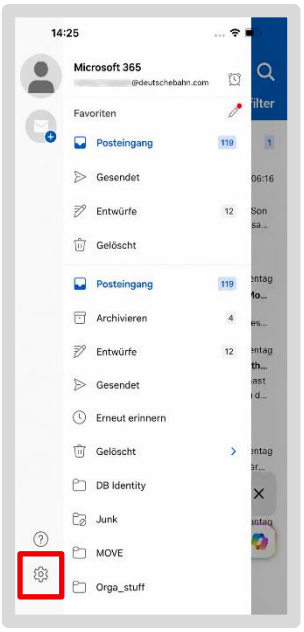
So bekommst du deine E-Mail Signatur aus EVI:

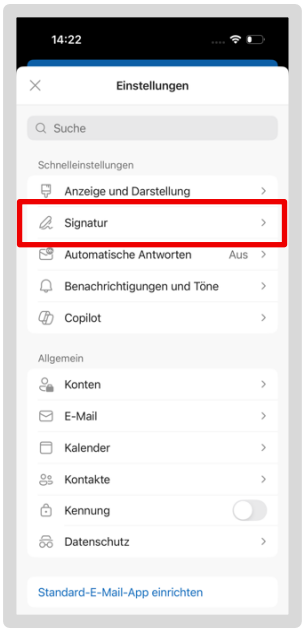
- Öffne die EVI App
- Tippe oben rechts auf die drei Striche neben deinem Profilbild
- Tippe dann auf „Meine E-Mail-Signatur“
- Im grauen Feld steht deine persönliche Signatur. Kopiere sie, indem du unten auf das Feld „Kopieren“ tippst



Füge die Signatur in Outlook ein:

- Öffne die Outlook App
- Tippe links oben auf dein Profilbild und dann links unten auf das Zahnrad
- Tippe nun auf „Signatur“





- Es öffnet sich ein Feld für die Signatur. Falls dort bereits ein Eintrag steht, lösche diesen
- Tippe nun lange auf das Feld, bis das „Einfügen“-Feld auftaucht und tippe darauf
- Deine kopierte Signatur aus dem EVI wird eingefügt

Schließe das Fenster – deine Signatur wird nun bei allen E-Mails, die du schreibst, automatisch eingefügt

Hinweis: Falls du mehrere E-Mail-Konten eingerichtet hast, kannst du über den Schieberegler „Signatur pro Konto“ für jedes Konto eine eigene Signatur einrichten. Ansonsten wird die hinterlegte Signatur für alle deine E-Mail-Konten verwendet.

8.2.3 Die E-Mail Synchronisierung – Alle E-Mails immer auf dem aktuellen Stand

Alle deine E-Mails werden in der Outlook App automatisch gesichert und mit deinem verbundenen Office-Konto synchronisiert. Das bedeutet, egal von welchem iPhone/iPad, ob iPhone/iPad oder BKU-Rechner/Basic Workplace Rechner, du dich anmeldest, du bist immer auf dem aktuellen Stand.

8.3 MS Defender App – Öffnen notwendig

Nach dem Aktivieren von Outlook und Teams aktiviere die App „Microsoft Defender for Endpoint Mobile“ (kurz MS Defender App) auf deinem Smartphone/Tablet. Die App schützt vor Cyberangriffen und scannt vorhandene Apps auf schädliche Software. Damit der Schutz aktiv ist öffne einmal die App.

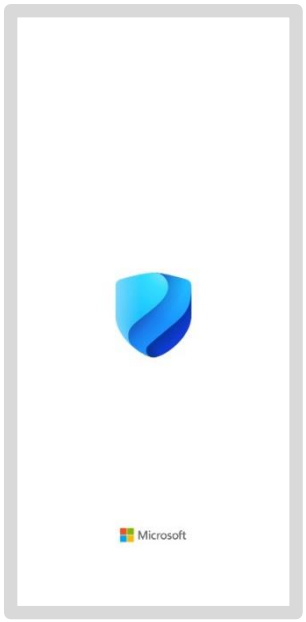
Aufgrund der Vielzahl unterschiedlicher DB Smartphones/Tablets kann es bei einzelnen Schritten zu geringfügigen Abweichungen in der Beschreibung kommen.

8.3.1 MS Defender App einrichten

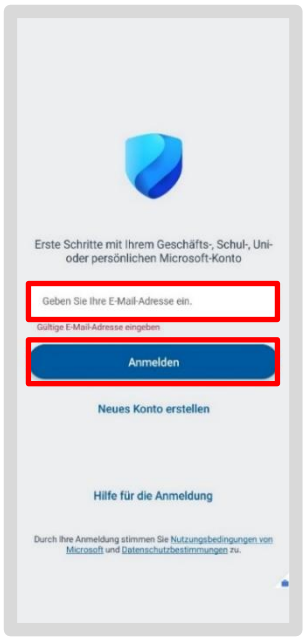
Um die MS Defender App auf deinem Smartphone/Tablet einzurichten, musst du folgende Schritte durchführen:

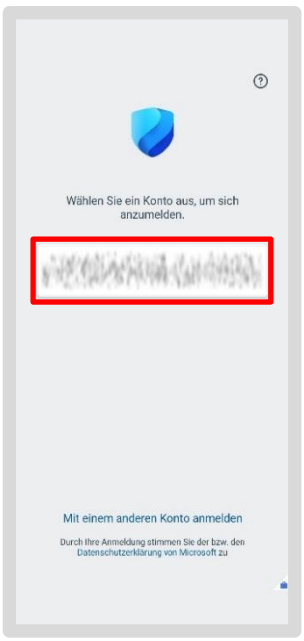
- Gehe in den Bereich Arbeit/Geschäftlich und öffne den „DB Google Play Store“
- Suche nach der App Microsoft Defender: Antivirus und tippe auf „installieren“

- Tippe auf das App Icon der MS Defender App, um die App zu öffnen



- Du wirst nach deiner dienstlichen E-Mail-Adresse gefragt
- Tippe auf den Button „Anmelden“ oder die App leitet dich automatisch auf den nächsten Screen, hier wird deine E-Mail-Adresse angezeigt
- Tippe auf Deine dienstliche E-Mail-Adresse

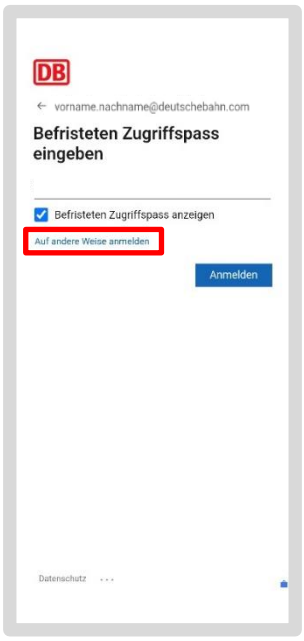


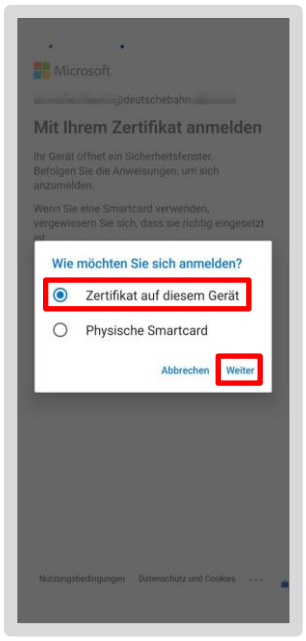


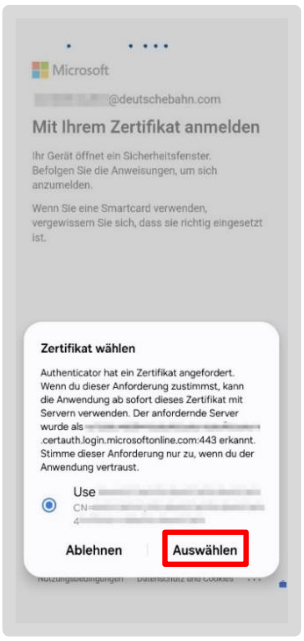
Wenn du innerhalb von einer Stunde dein Smartphone/Tablet mit der *Intune App* aktiviert hast, kann es sein, dass du hier nochmal aufgefordert wirst dein befristeten Zugriffpass einzugeben.

- Tippe auf „Auf andere Weise anmelden“

- Tippe bei der Abfrage auf „Zertifikat auf diesem Gerät“ und tippe auf „Weiter“
- Wähle das Zertifikat aus



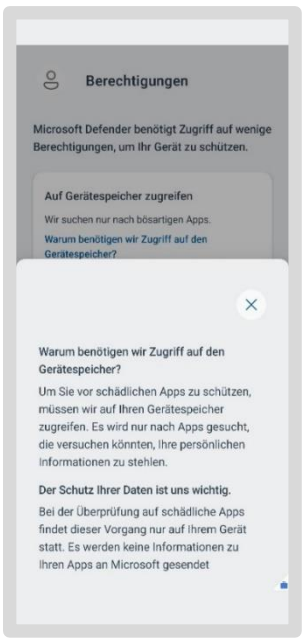


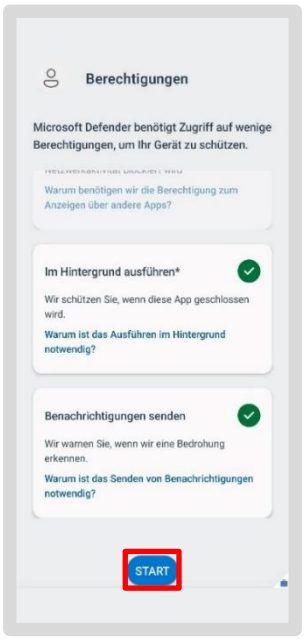


8.3.2 Berechtigungen vergeben

Die App fragt dich nun nach notwendigen Berechtigungen. An dieser Stelle können die Screens in einer Abweichenden Reihenfolge zur Anleitung auftreten. Sofern dein erster Screen mit dem abgebildeten übereinstimmt:

- Tippe auf „Aktivieren“
- Tippe anschließend auf „Start“
- Es öffnet sich die App Einstellungen deines Smartphones/Tablets



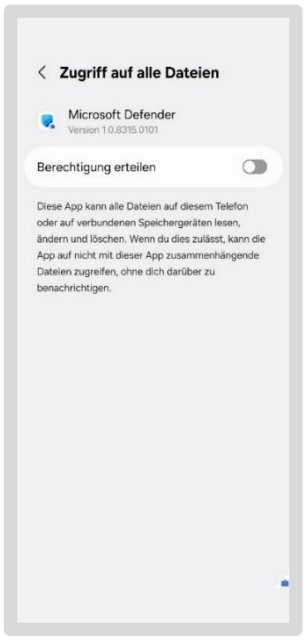


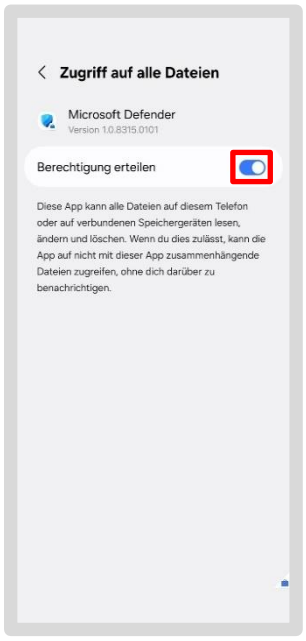
Hintergrundinfo Berechtigungen:

Diese Berechtigungen sind erforderlich, damit die Anwendung einwandfrei funktioniert und die Sicherheit auf deinem Gerät gewährleistet ist.

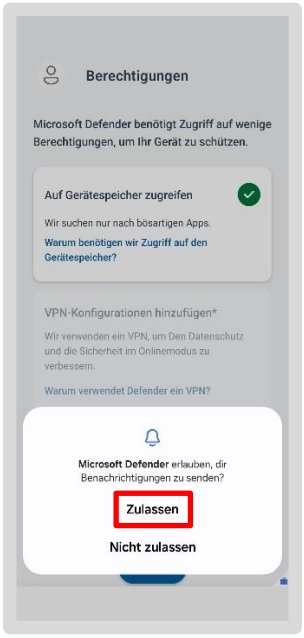
Zu den einzelnen Berechtigungen kannst du dir jeweils ein Infofenster anzeigen lassen (z. B. durch Klick auf „Warum benötigen wir Zugriff auf den Gerätespeicher?“). Einige Elemente sind jedoch nicht auswählbar (sie sind ausgegraut, wie z. B. „VPN-Konfiguration hinzufügen“) oder bereits aktiviert (grüner Haken, wie z. B. „Im Hintergrund ausführen“), da diese systemseitig vorgegeben sind.

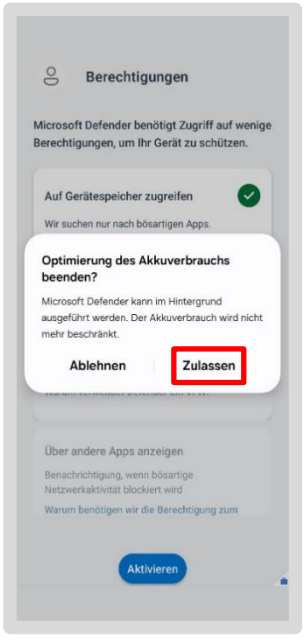
- Schiebe nun den Schieberegler nach rechts, um die Berechtigung zu erteilen
- Tippe bei der anschließenden Abfrage auf „Zulassen“

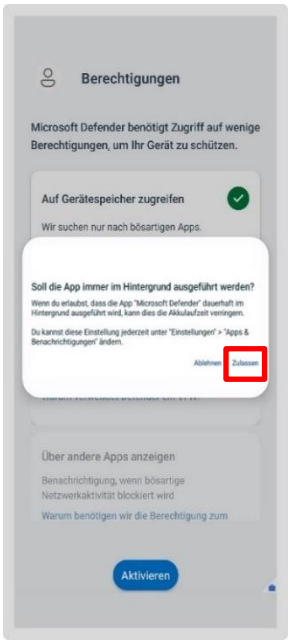




- Tippe bei allen folgenden Abfragen jeweils auf „Zulassen“



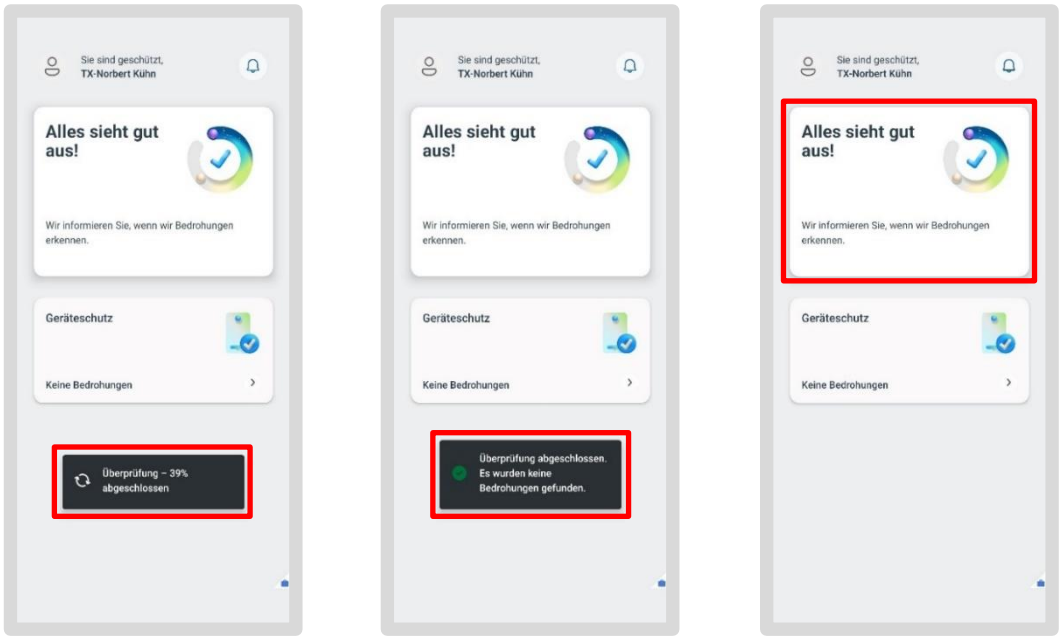




Beachte: Es wird je nach Gerätetyp nach anderen Berechtigungen gefragt! Dadurch kommt gegebenenfalls nur eine der abgebildeten Abfragen.

Anschließend landest du auf der Startseite der MS Defender App. Sofort wird automatisch eine Überprüfung nach Schadsoftware für dein Smartphone/Tablet durchgeführt. Während der Überprüfung werden Zwischenschritte angezeigt.

Das Ergebnis wird auf der Startseite schriftlich angezeigt. Wenn ein grüner Haken sichtbar ist, ist keine Schadsoftware erkannt.



Du hast die Ersteinrichtung erfolgreich beendet! Das Gerät ist jetzt gegen Schadsoftware geschützt.

8.4 DB M 365

Auch auf deinem Smartphone/Tablet kannst du Word-, Excel-, PowerPoint-Dateien oder PDF-Dateien öffnen und lesen. Lade dir dafür einmalig die entsprechenden Apps herunter:

- Öffne den DB Google Play Store
- Suche nach der jeweiligen App über die Suchleiste, zum Beispiel Word, Excel, PowerPoint oder den PDF Reader

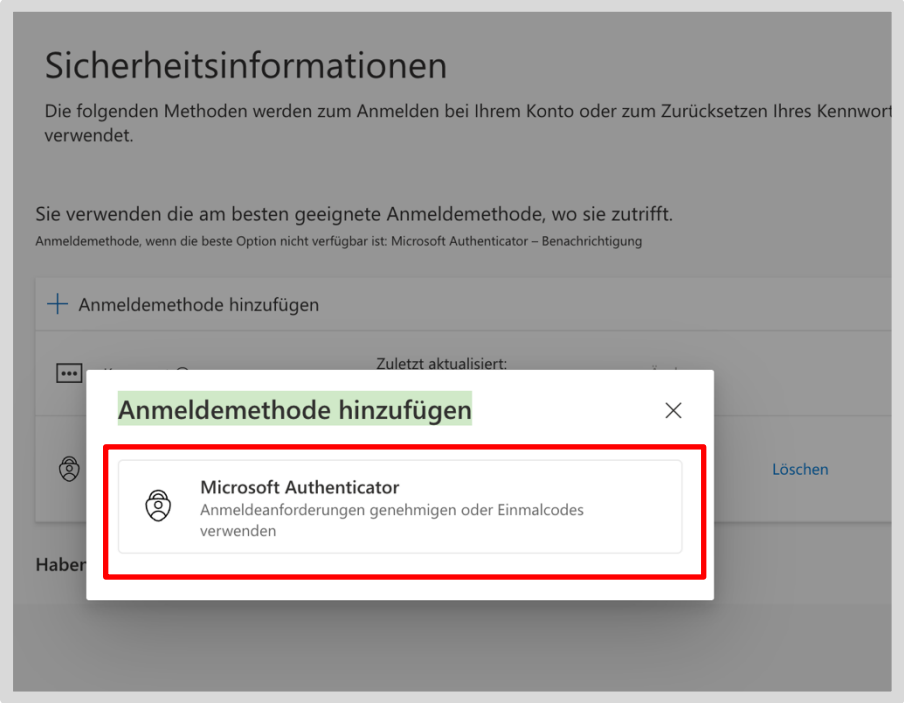
- Tippe anschließend auf „Installieren“. Die App wird nun heruntergeladen und erscheint in deinem Bereich „Arbeit/Geschäftlich“
- Wenn du nun eine Datei öffnest, öffnet sich die App automatisch

Beachte: Du kannst immer nur eine Datei auf einmal öffnen. Es ist als bspw. nicht möglich mehrere Word-Dateien gleichzeitig zu öffnen.

8.5 Microsoft Authenticator App wieder aktivieren

Wenn du die Authenticator-App genutzt hast, gehe wie folgt vor:

- Tippe auf db.de/authenticator auf deinem BKU oder Basic Workplace Rechner
- Tippe auf das „Plus-Icon“ und den Button „Anmeldemethode hinzufügen"
- Es öffnet sich ein Dialog, wähle "Microsoft Authenticator" aus



- Wechsle zu deinem Smartphone/Tablet und öffne die Microsoft Authenticator App
- Öffne diese Seite für eine Schritt-für-Schritt-Anleitung und tippe auf den Button „Anleitung zur Einrichtung der MFA“ und gehe die angegebenen Schritte durch
- Anschließend kannst du die Microsoft Authenticator App zur Authentifizierung auf deinem Smartphone/Tablet nutzen
- Hast du die **Authenticator-App für Webseiten oder Tools** genutzt, aktiviere die App nun wieder in den Webseiten

Tipp: Solltest du Schwierigkeiten haben, die Verbindungen in der Authenticator-App nach der Migration wieder zu aktivieren, nutze den Self Service: „Microsoft Authenticator App (MFA) zurücksetzen“: db.de/resetmfa und folge dann den Schritten.

Glückwunsch!

Du hast dein dienstliches Smartphone/Tablet erfolgreich migriert!

Mehr Informationen zu deinem Smartphone/Tablet findest du in der App: DB Mobile Info.

> Wie du deine Kontakte in OneDrive speichern und wieder importieren kannst findest du in der Anleitung Einrichtung unter Kontakte in OneDrive sichern

> Eine Langanleitung für die Einrichtung findest du unter db.de/mobile-setup