



Betriebssystem-Version ab Android 15

Wiederherstellung Samsung DB Workplace Mobile

DB System GmbH | 04.06.2026

Inhaltsverzeichnis

1 Notwendige Schritte vor der Wiederherstellung	4
1.1 Daten sichern	4
1.2 Authenticator App – optional	4
1.3 Erstellen eines befristeten Zugriffspass (TAP) - Expertenmodus	4
2 Start Wiederherstellung: Smartphone/Tablet zurücksetzen	7
2.1 Smartphone/Tablet selbst zurücksetzen	7
2.2 Smartphone/Tablet über die IT ServiceDesk App zurücksetzen	8
3 Erneut einrichten in Microsoft Intune	9
3.1 Sprache auswählen	9
3.2 Endbenutzer-Lizenzvereinbarung zustimmen	10
3.3 WLAN einrichten	11
3.4 WLAN einrichten im DB Gebäude	12
4 Samsung in der DB anmelden	13
4.1 Arbeitsprofil einrichten	14
4.2 Bildschirmsperre festlegen	15
4.3 DB Apps installieren	16
4.4 Google Konto – nicht notwendig	16
4.5 Google Dienst aktivieren	17
4.6 Automatische Installation DB Apps	18
5 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen	19
5.1 Befristeten Zugriffspass (TAP) erstellen	19
5.2 Befristeten Zugriffspass für eine(n) Kollegen:in erstellen	22
6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP)	24
6.1 Zugriff auf alle DB Apps und Webseiten einrichten	25
6.2 DB Apps	26
7 Notwendige Einstellungen	27
7.1 Nach Betriebssystem Updates suchen	27
7.2 Outlook	28
7.2.1 E-Mail Signatur einrichten	29
7.2.2 Die E-Mail Synchronisierung – Alle E-Mails immer auf dem aktuellen Stand	31
7.3 MS Defender App – Öffnen notwendig	31
7.3.1 MS Defender App einrichten	31

7.3.2 Berechtigungen vergeben	33
7.4 DB M 365	35
7.5 Bixby-Taste ausschalten	36
7.6 Microsoft Authenticator App wieder aktivieren	37



1 Notwendige Schritte vor der Wiederherstellung

Wenn dein dienstliches Smartphone/Tablet Probleme wie langsame Leistung, Einfrieren oder häufiges Abstürzen aufweist, ist ein Zurücksetzen auf die Werkseinstellungen hilfreich. Diese Schritte sind notwendig:

1.1 Daten sichern

- **Sichere deine Daten**

Führe dazu folgende Schritte durch:

- a) Sichere deine dienstlichen Daten und Einstellungen
- b) Sichere deine privaten Daten und Einstellungen

> Eine Anleitung zur Datensicherung findest du unter:

mobileworkplace.deutschebahn.com/mobile-daten-sichern

> Eine Video-Anleitung findest du unter: db.de/mobile-videoanleitungen

1.2 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 Wiederherstellung die *Authenticator App* nicht genutzt werden kann
- Es sind keine weiteren Schritte notwendig
- Nach der Wiederherstellung muss die App erneut aktiviert werden, das wird in [Kapitel 7.6 Microsoft Authenticator App wieder aktivieren](#) beschrieben
- Ist es notwendig, dass du während der Wiederherstellung 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 \(MFA\)](#)

1.3 Erstellen eines befristeten Zugriffspass (TAP) - Expertenmodus

Nachdem du deine Daten gesichert hast, gibt es zwei Möglichkeiten:

Dein Smartphone/Tablet funktioniert noch teilweise, gehe zur nächsten Seite

Dein Smartphone/Tablet funktioniert überhaupt nicht mehr, gehe weiter zu

> [Kapitel 2.2 Smartphone/Tablet über die IT ServiceDesk App zurücksetzen](#)

Smartphone/Tablet funktioniert noch teilweise:

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

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:

- 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**

IT ServiceDesk App

Befristeten Zugriffspass (TAP) erstellen

Mit diesem Self Service kannst du einen befristeten Zugriffspass (TAP) erstellen, um ein DB Workplace oder Basic Workplace Gerät einzurichten.

Der TAP kann erstellt werden für:

- dich selbst
- einen Mitarbeitenden aus dem gleichen Unternehmen (siehe [EVI](#))

Anmelden

Gib deine DB User Zugangsdaten ein

DB User Anmeldename
Max Mustermann

DB User Passwort

[Wie kann ich mich an anderen Umgebungen anmelden?](#)

DB

Befristeten Zugriffspass (TAP) erstellen - Personenauswahl

Wähle aus, für wen der TAP erstellt werden soll:

Für mich selbst

Für einen anderen DB Mitarbeitenden

IT ServiceDesk App

Befristeten Zugriffspass (TAP) erstellen

Wähle das Produkt aus, das du einrichten möchtest.

DB Workplace Mobile
Ich möchte ein Smartphone / Tablet einrichten.

Basic Workplace Windows
Ich möchte ein Notebook / PC einrichten.

DB Workplace Windows
Ich möchte ein Notebook / PC einrichten.

DB Workplace Mac
Ich möchte ein Apple Mac / MacBook einrichten.

DB

Befristeter Zugriffspass (TAP) erstellen

rQkLc+nSSZBx

Gib den befristeten Zugriffspass (TAP) zur Aktivierung deines DB Workplace Mobile Geräts ein, folge dabei den Anleitungen. Dieser ist bis **11:24 Uhr** gültig und kann **mehrfach** verwendet werden.

Neue Session starten

Zur Startseite

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 beim Anmelden, nachdem du dein Smartphone/Tablet zurückgesetzt hast
 - Du hast **nun 60 Minuten Zeit** um dein Smartphone/Tablet zurückzusetzen
- > Gehe direkt zu [Kapitel 2.1 Smartphone/Tablet selbst zurücksetzen](#)

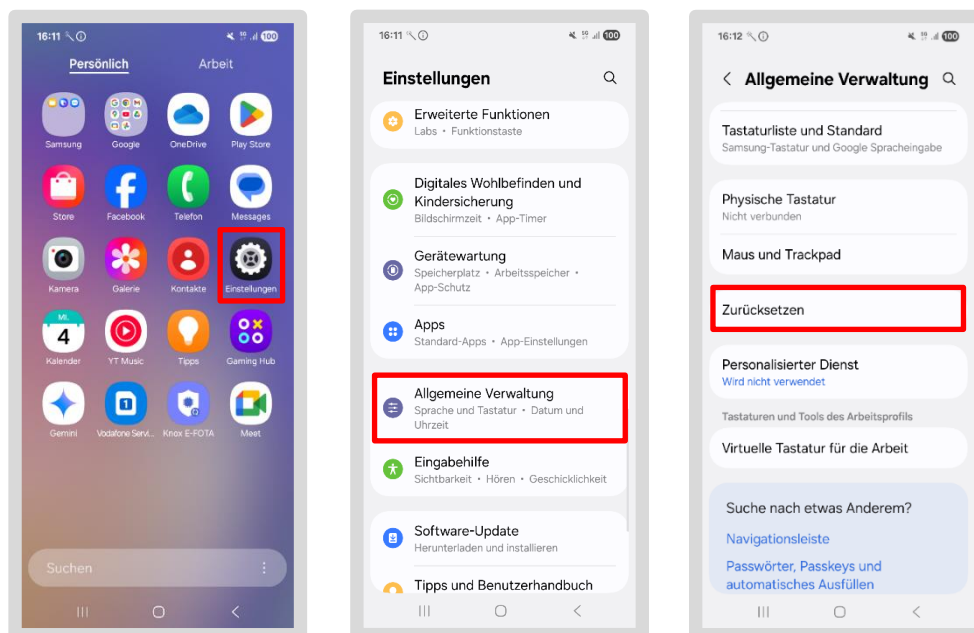
2 Start Wiederherstellung: Smartphone/Tablet zurücksetzen

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

2.1 Smartphone/Tablet selbst zurücksetzen

> **Hinweis:** Eine Video-Anleitung findest du unter [db.de/mobile-videoanleitung](https://www.db.de/mobile-videoanleitung)

- Gehe auf deinem Smartphone/Tablet in den Bereich „Persönlich“
- Tippe auf die App „Einstellungen“
- Tippe auf „Allgemeine Verwaltung“
- Scrolle weiter nach unten und tippe auf „Zurücksetzen“



- Wähle dann „Reset auf Werkseinstellungen“
- 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 „Zurücksetzen“, gib deine Bildschirmsperre ein und im Weiteren auf „Alles löschen“
- Warte einige Minuten ab, dein Gerät wird automatisch zurückgesetzt

> Gehe dann zu [Kapitel 3 Erneut einrichten in Microsoft Intune](#)

2.2 Smartphone/Tablet über die IT ServiceDesk App zurücksetzen

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

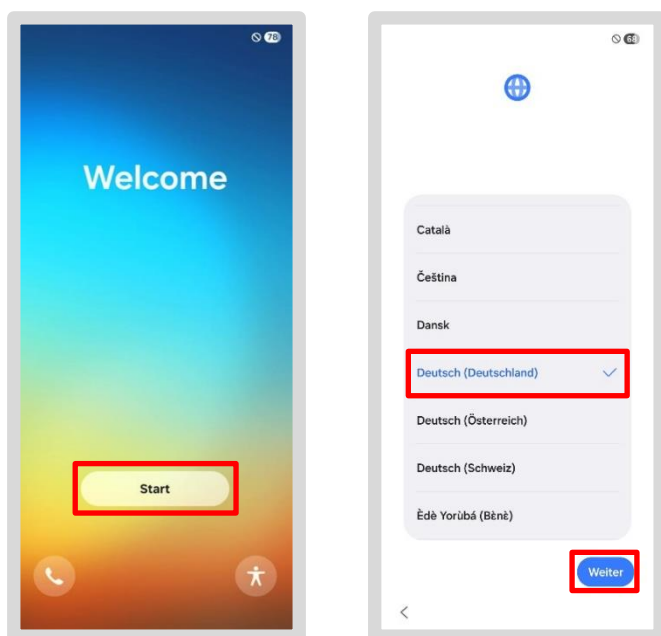
- Öffne die IT ServiceDesk App und gib unter „Neues Serviceanliegen“ deinen Auftrag für das Zurücksetzen deines Smartphones/Tablets ein
 - Falls du die App nicht öffnen kannst, wähle diese Nummer:
 - IT ServiceDesk
 - Intern: Tel. 91-5555
 - Extern: Tel. 0361 430 8200
 - Hier den Menüpunkt 0 wählen
 - 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 3 Erneut einrichten in Microsoft Intune

3 Erneut einrichten in Microsoft Intune

3.1 Sprache auswählen

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

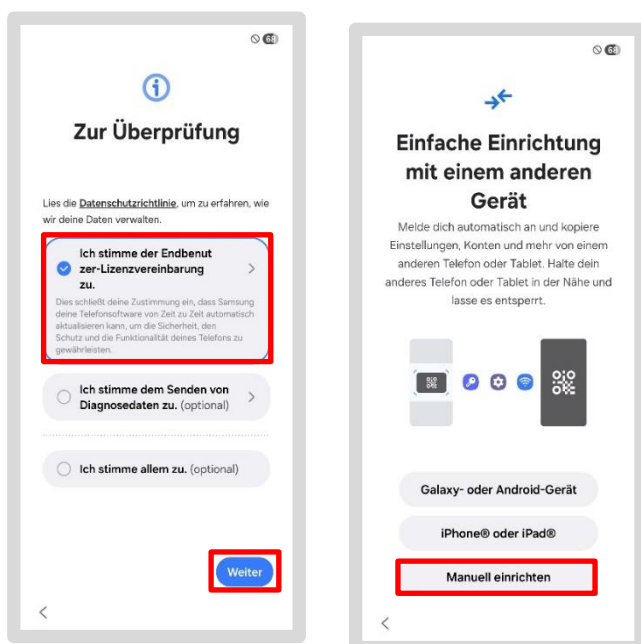
- Halte dein Tablet im **Hochformat**, um die Screens in der gleichen Darstellung zu erhalten, wie sie in der Anleitung dargestellt sind
- Schalte dein Smartphone/Tablet ein
- Achte darauf, dass dein Smartphone/Tablet während der Wiederherstellung entweder an die Stromversorgung angeschlossen ist oder einen hohen Akkustand hat
- Tippe auf „Start“
- Wähle auf dem nächsten Screen die für dich gewünschte Sprache in der Auswahl aus und tippe auf „Weiter“



> Gehe weiter zu [Kapitel 3.2 Endbenutzer-Lizenzvereinbarung zustimmen](#)

3.2 Endbenutzer-Lizenzvereinbarung zustimmen

- Tippe **nur** auf „Ich stimme der Endbenutzer-Lizenzvereinbarung zu“ und dann auf „Weiter“
- Tippe bei der „Einrichtung mit einem anderen Gerät“ auf „Manuell einrichten“



> Gehe weiter zu Kapitel 3.3 WLAN einrichten

3.3 WLAN einrichten

Wähle zum Einrichten deines WLANs eine dieser Möglichkeiten:

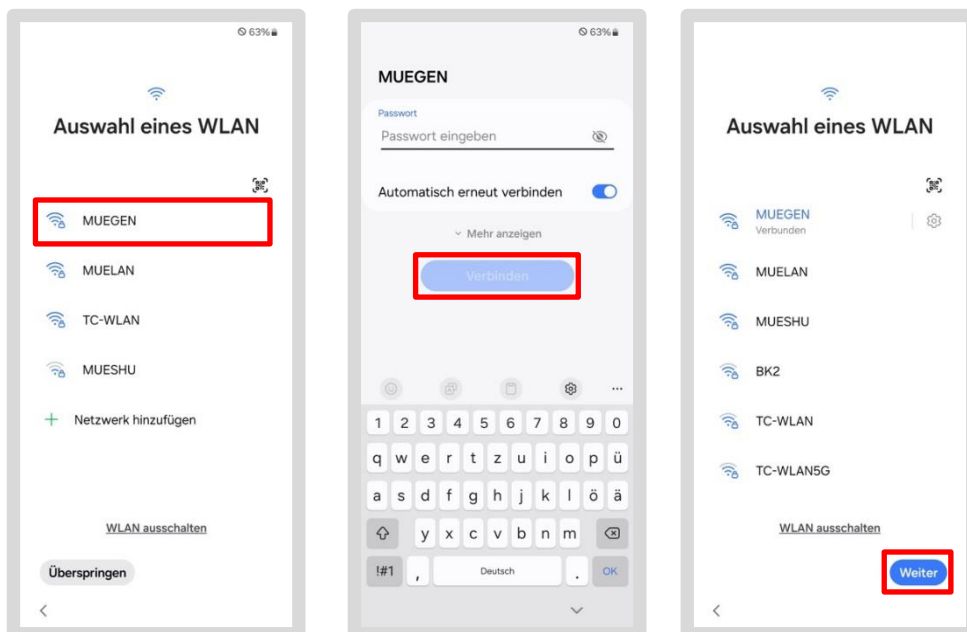
- Nutze deine **mobilen Daten**, sofern eine SIM Karte in deinem Smartphone/Tablet vorhanden ist (das könnte unter Umständen kostenpflichtig sein!)
- Richte einen Hotspot mit deinem privaten Smartphone/Tablet ein

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.

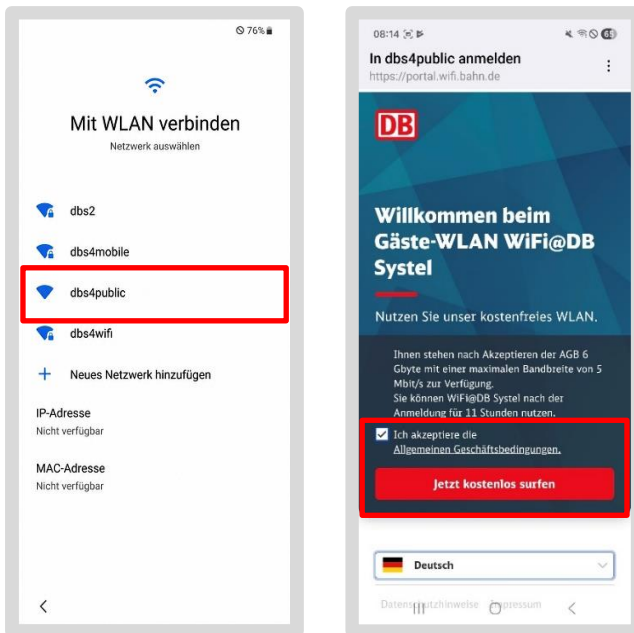
- > Gehe zu [Kapitel 4 Samsung in der DB anmelden](#)

3.4 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“



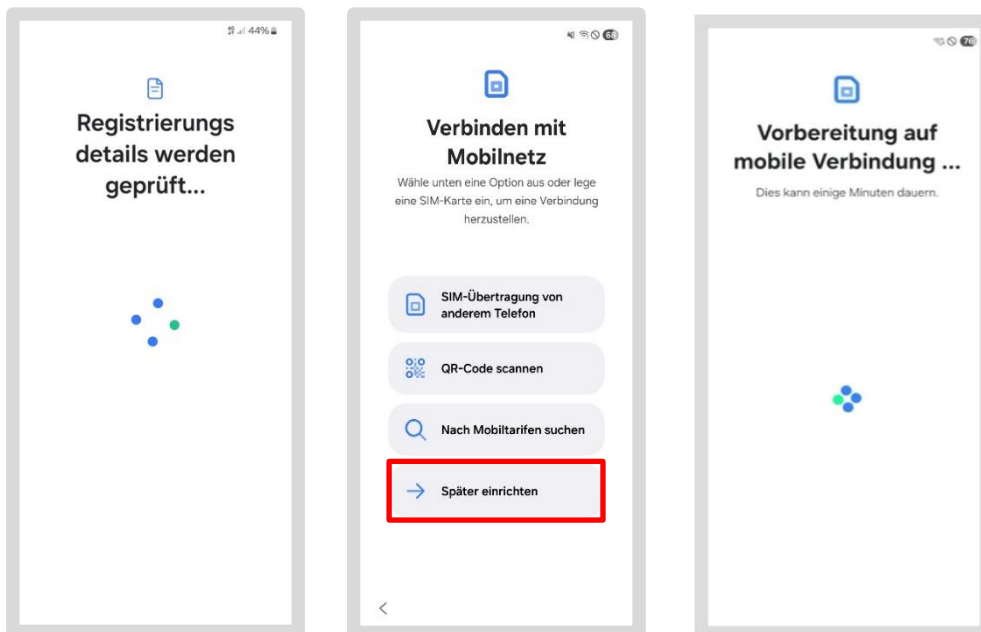
Sobald dein Smartphone/Tablet mit dem WLAN verbunden ist, startet die Verknüpfung mit dem DB Netzwerk.

- > Gehe zu [Kapitel 4 Samsung in der DB anmelden](#)

4 Samsung in der DB anmelden

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.

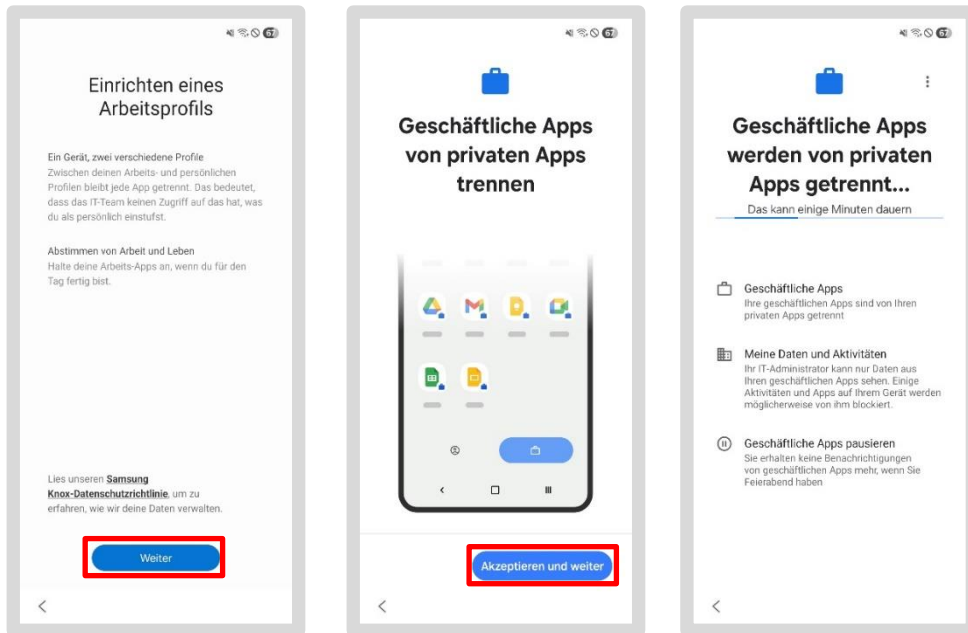
- Halte dein Tablet im **Hochformat**, wenn du es bis hier im Querformat gehalten hast
- Es wechseln nun einzelne Screens durch
- Tippe auf „Später einrichten“, es werden nun wieder einige Screen dargestellt, ohne dass du etwas tun musst



4.1 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 eingerichtet
- Bestätige die folgende Abfrage mit „Weiter“
- Wenn „Einrichten eines Arbeitsprofils“ erscheint tippe auf „Weiter“ oder „Zustimmen“
- Wenn „Der IT-Administrator kann dieses Gerät steuern & Apps blockieren“ (Der Text kann abgeschnitten sein) erscheint tippe auf „Weiter“

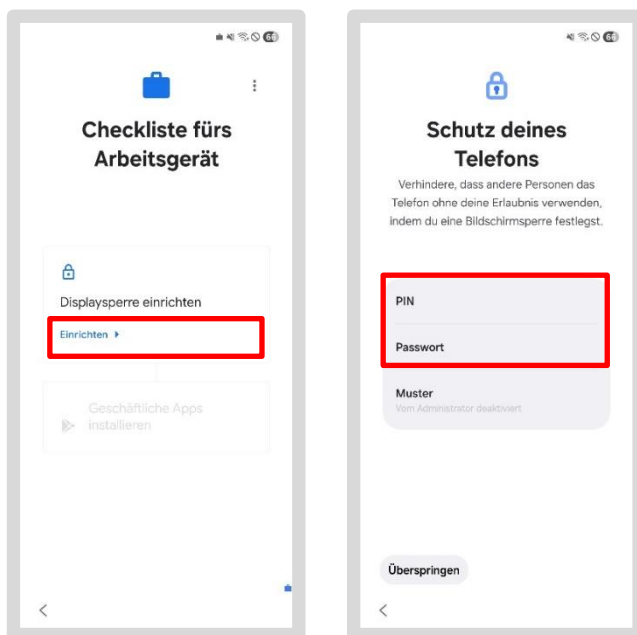


- Die Aktualisierung des Geräts kann etwas oder auch sehr lange dauern, gedulde dich hier!
- Die erforderlichen Apps werden installiert
- Es kann sein, dass hier die Abfrage zu einem privaten Konto erscheint
- > Gehe in diesem Fall zu [Kapitel 4.4 Google Konto – nicht notwendig](#)
- Wenn diese Abfrage nicht erscheint, setze die Anleitung ganz normal fort
- > Gehe zu [Kapitel 4.2 Bildschirmsperre festlegen](#)

4.2 Bildschirmsperre festlegen

Im nächsten Schritt richtest du die Bildschirmsperre für dein Gerät 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
- Wenn „Einrichten von biometrischen Daten“ kommt, tippe auf „Überspringen“

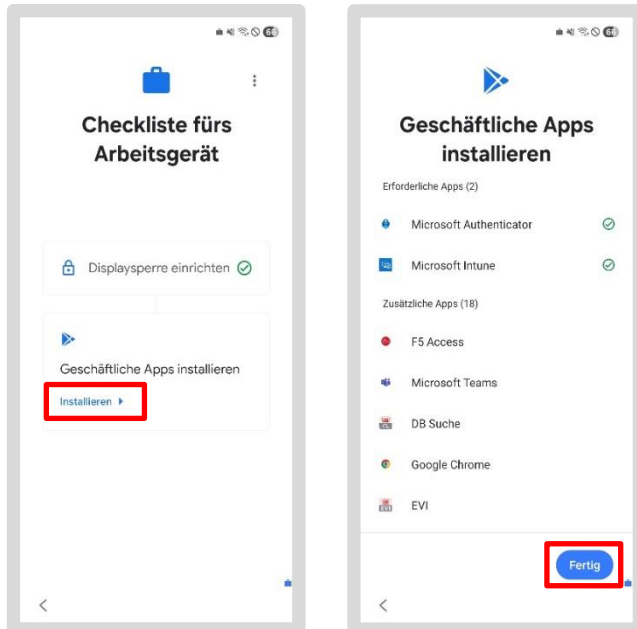


- Achte auf die Datenschutz- und Nutzungshinweise in der Anleitung Ersteinrichtung
- Bestätige mit „Weiter“ und dann bei zweimaligem Eingeben mit „OK“
- Falls der Screen „Private Konten“ kommt: Tippe bei der Abfrage auf „Später“
- Es kann sein, dass hier die Abfrage zu den Google Diensten erscheint
 - > Gehe in diesem Fall zu Kapitel 4.5 Google Dienst aktivieren
- Wenn diese Abfrage nicht erscheint, setze die Anleitung ganz normal fort
 - > Gehe zu Kapitel 4.3 DB Apps installieren

4.3 DB Apps installieren

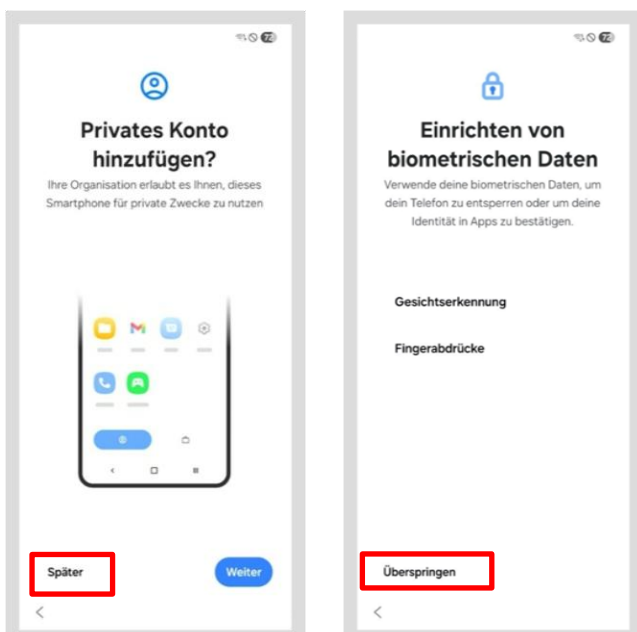
Im nächsten Schritt werden für dein DB Smartphone/Tablet wieder alle DB Apps installiert. Folge den Anweisungen auf dem Bildschirm.

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



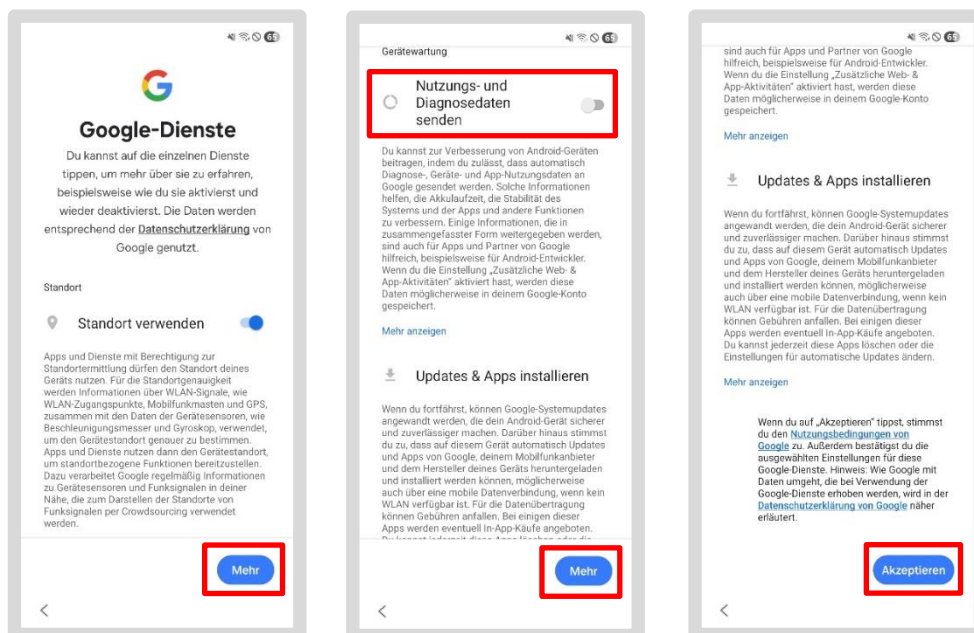
4.4 Google Konto – nicht notwendig

- Für dein DB Smartphone/Tablet wird **kein privates** Google Konto benötigt!
- Bei Bedarf kannst du dies später nachholen
- Tippe deshalb auf „Später“
- Wenn „Einrichten von biometrischen Daten“ kommt, tippe auf „Überspringen“



4.5 Google Dienst aktivieren

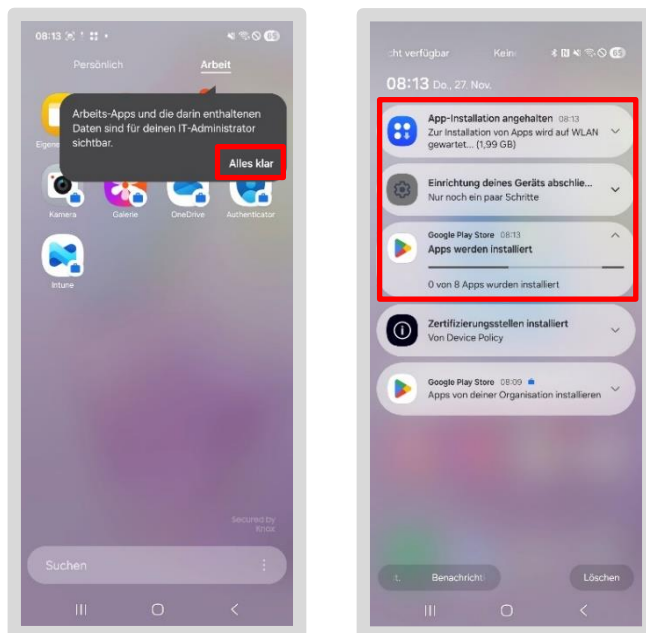
- Tippe auf „Mehr“ bei den Google-Diensten
- Bei **Nutzungs- und Diagnosedaten senden**: Tippe zum Ausschalten der Funktion auf den Schieberegler
- Scrolle weiter und tippe dann auf „Akzeptieren“



> gehe zu [Kapitel 4.6 Automatische Installation DB Apps](#)

4.6 Automatische Installation DB Apps

- Es folgen die weiteren Screens...warte bis der Startscreen erscheint
- mit einem Wischen von unten nach oben ist die Unterteilung in den Bereich Persönlich/Arbeit zu sehen
- Tippe auf „Alles klar“
- Wische von oben nach unten. Hier zeigen dir die Notifications, ob noch Apps geladen bzw. installiert werden
- Tippe auf die Notification und du siehst, wie viele Apps noch zu installieren sind



- **Beachte:** „Einrichtung deines Geräts abschließen“ ist für das Einrichten deines DB Smartphone/Tablets nicht notwendig. Ignoriere es!
- 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 2 Start Wiederherstellung: dein Smartphone/Tablet zurücksetzen

Wichtig!

Dein Smartphone/Tablet ist noch nicht mit dem
DB Management verbunden!

Hole Dir den **befristeten Zugriffspass (TAP)**
und gib diesen in der *Intune App* ein.

Folge dafür der Schritt-für-Schritt-Anleitung in
> Kapitel 5 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen

5 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen

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

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

Wenn du bereits einen Zugriffspass erstellt hast:

- > Gehe weiter zu [Kapitel 6 Gerät aktivieren mit dem befristeten Zugriffspass](#)
- > Ansonsten geh weiter zu [Kapitel 5.1 Befristeten Zugriffspass \(TAP\) erstellen](#)

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

5.1 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 5.2 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 2 Start Wiederherstellung: Smartphone/Tablet zurücksetzen](#)

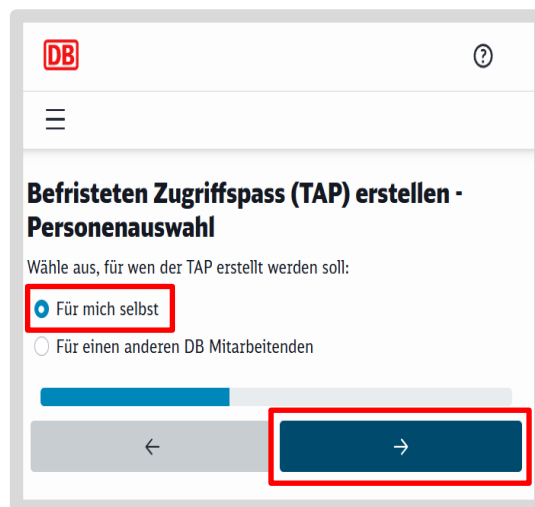
Beachte: Dein Tap ist nur 60 Minuten und für mehrere Smartphones/Tablets gültig!

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

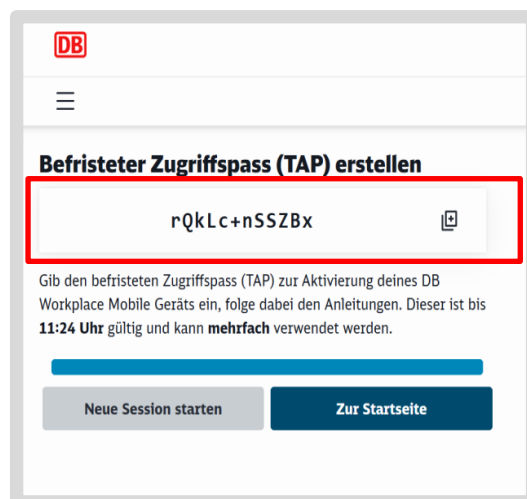
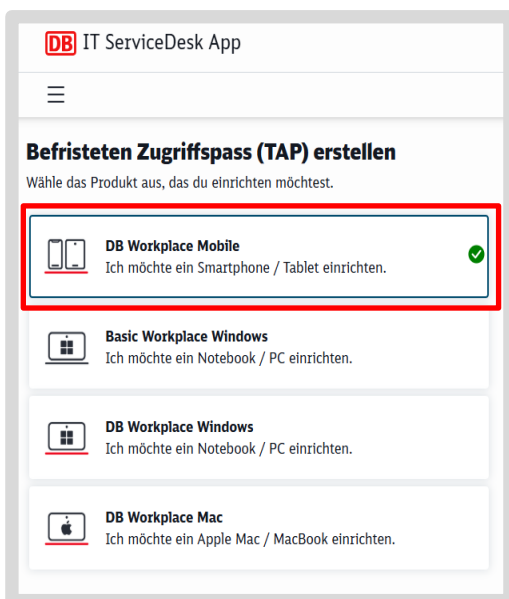
Wenn du die Willkommen App nicht installiert hast:

- 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 weiter zu Kapitel 6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP)

Wichtig!

Dein Smartphone/Tablet ist noch nicht mit dem
DB Management verbunden!

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

> Gehe jetzt zu Kapitel 6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP)

5.2 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

DB IT ServiceDesk App

Hilfe

Befristeten Zugriffspass (TAP) erstellen

Mit diesem Self Service kannst du einen befristeten Zugriffspass (TAP) erstellen, um ein DB Workplace oder Basic Workplace Gerät einzurichten.

Der TAP kann erstellt werden für:

- dich selbst
- einen Mitarbeitenden aus dem gleichen Unternehmen (siehe EVI 7)

Anmelden

Gib deine DB User Zugangsdaten ein

DB User Anmeldename
Max Mustermann

DB User Passwort

[Wie kann ich mich an anderen Umgebungen anmelden?](#)

DB

Einen befristeten Zugriffspass (TAP) ausstellen - Personenauswahl

Wähle aus, für wen der TAP erstellt werden soll:

Für mich selbst

Für einen anderen DB Mitarbeitenden

Halte die DB User Anmeldedaten des DB Mitarbeitenden für den nächsten Schritt bereit.

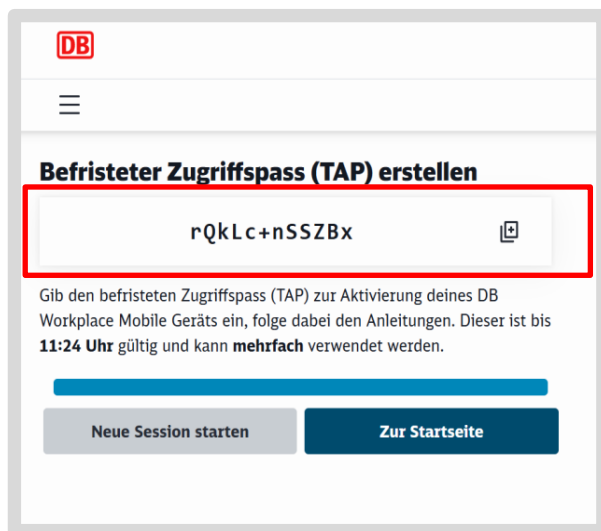
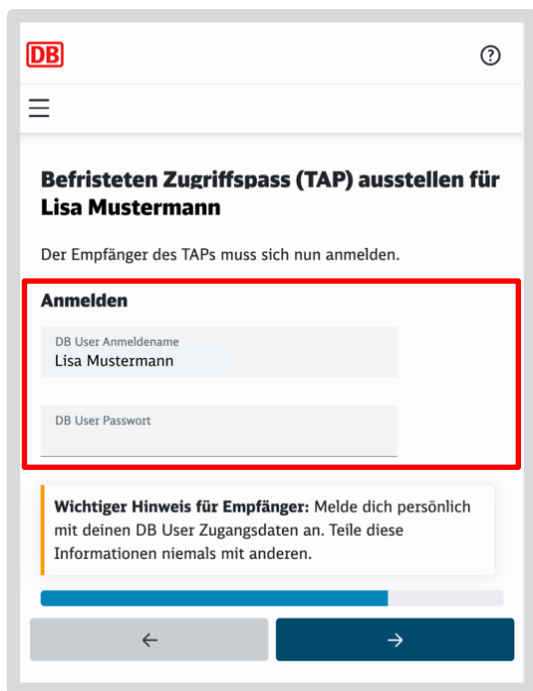
Q Lisa Mustermann

DB User:	Lisa.Mustermann
Name:	Lisa Mustermann
E-Mail:	Lisa.Mustermann@deutschebahn.com
Abteilung:	XX.X Y-Y-123
Unternehmen:	DB Systel GmbH

DB User:	Lise.Mustermann
Name:	Lise Mustermann
E-Mail:	Lise.Mustermann@deutschebahn.com
Abteilung:	XX.X Y-Y-145
Unternehmen:	DB Systel GmbH

Ich bestätige, dass ich die Identität des Mitarbeitenden festgestellt habe.

- 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 Kollege:in kann jetzt sein Smartphone/Tablet in der Intune App aktivieren
- > Gehe weiter zu Kapitel 6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP)

Wichtig!


Dein Smartphone/Tablet ist noch nicht mit dem
DB Management verbunden!
Gib den **befristeten Zugriffspass (TAP)**
in der *Intune App* ein.

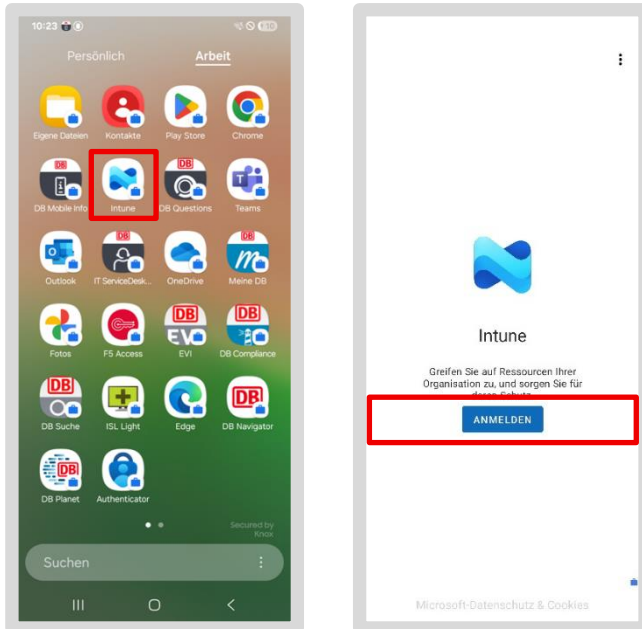
> Gehe jetzt zu Kapitel 6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP)

6 Gerät aktivieren mit dem befristeten Zugriffspass (TAP)

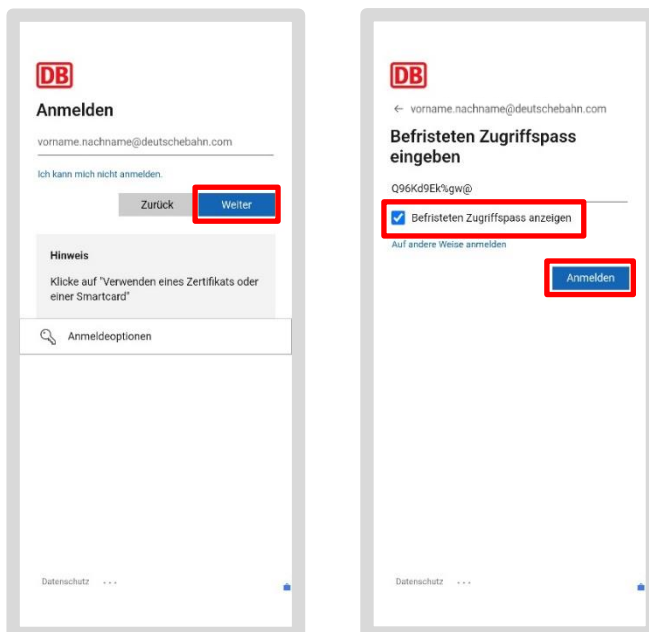
> **Beachte:** Prüfe, ob du einen befristeten Zugriffspass (TAP) wie in Kapitel 5 Gerät aktivieren - Befristeten Zugriffspass (TAP) erstellen beschrieben und erhalten hast!

> **Hinweis:** Eine Video-Anleitung findest du unter [db.de/mobile-videoanleitung](https://www.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“
- 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 5 Gerät aktivieren - Befristeten Zugriffspass \(TAP\) erstellen](#) beschrieben
- > Ansonsten gehe weiter zu [Kapitel 6.1 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.

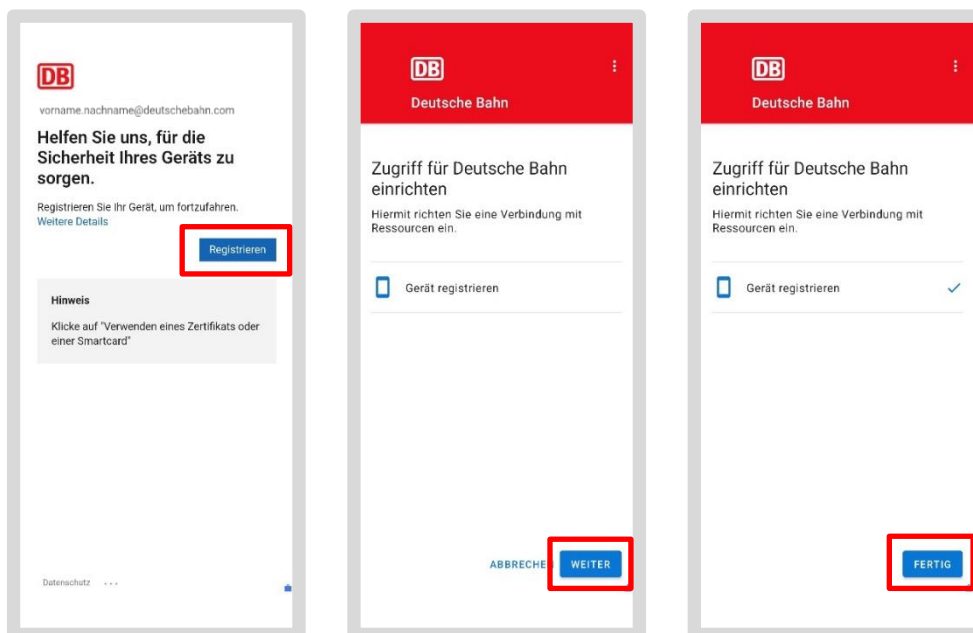
6.1 Zugriff auf alle DB Apps und Webseiten einrichten

Nun wird der Zugriff auf das *DB Management* 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.

6.2 DB Apps

Beachte: Die Bereitstellung der Zertifikate kann **5 Minuten bis 24 Stunden** dauern. Erst danach kannst du deine Apps, wie z.B. *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 „Arbeit“ herunterladen.

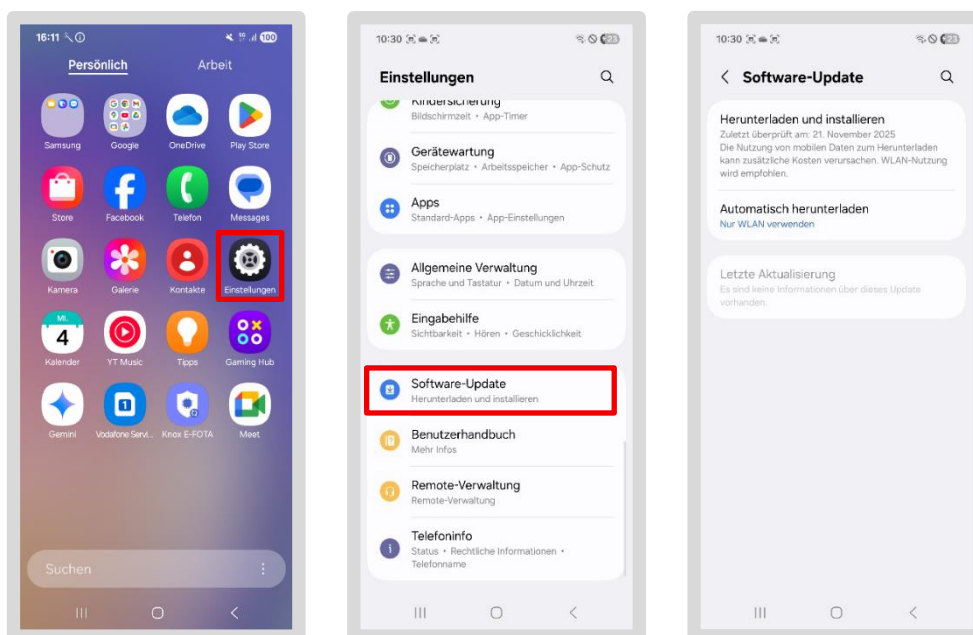
Die **Willkommen App** ist **nicht mehr** auf dem DB Smartphone/Tablet, dafür gibt es die **App DB Mobile Info** mit allen Informationen, nützlichen Links und Daten rund um dein DB Smartphone/Tablet.

7 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.

7.1 Nach Betriebssystem Updates suchen

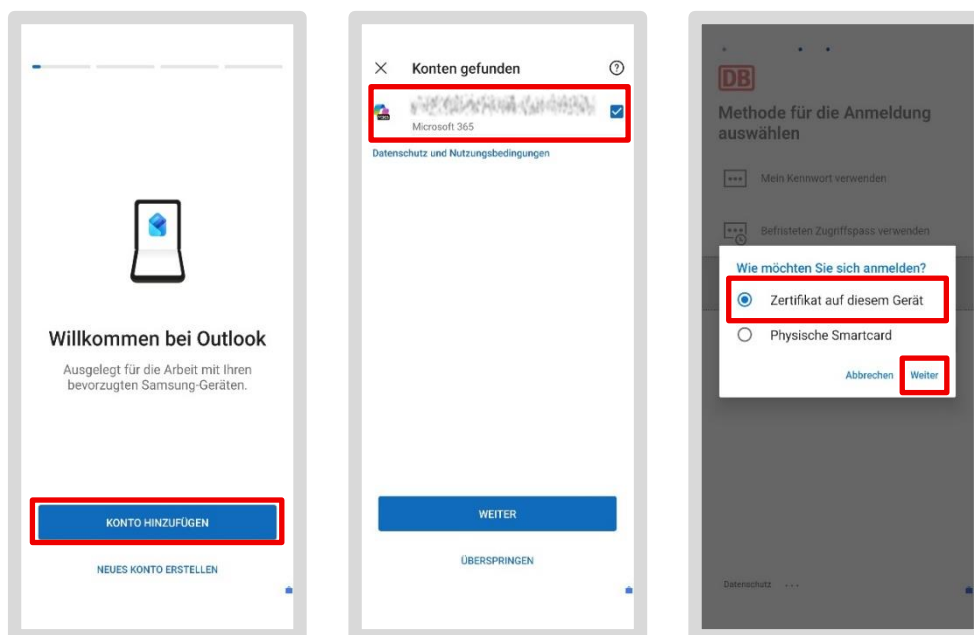
- Gehe auf deinem Smartphone/Tablet in den Bereich „Persönlich“
- Tippe auf die App *Einstellungen*
- Tippe auf „System-Update“
- Dort steht, ob ein Update angeboten wird. Führe anstehende Updates durch, tippe dafür auf „Update installieren“



7.2 Outlook

> **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 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 5.1 Befristeten Zugriffspass \(TAP\) erstellen](#) beschrieben
- Alternativ: wähle „andere Anmeldeoption wählen“ und dann „Zertifikat auf diesem Gerät“
- 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

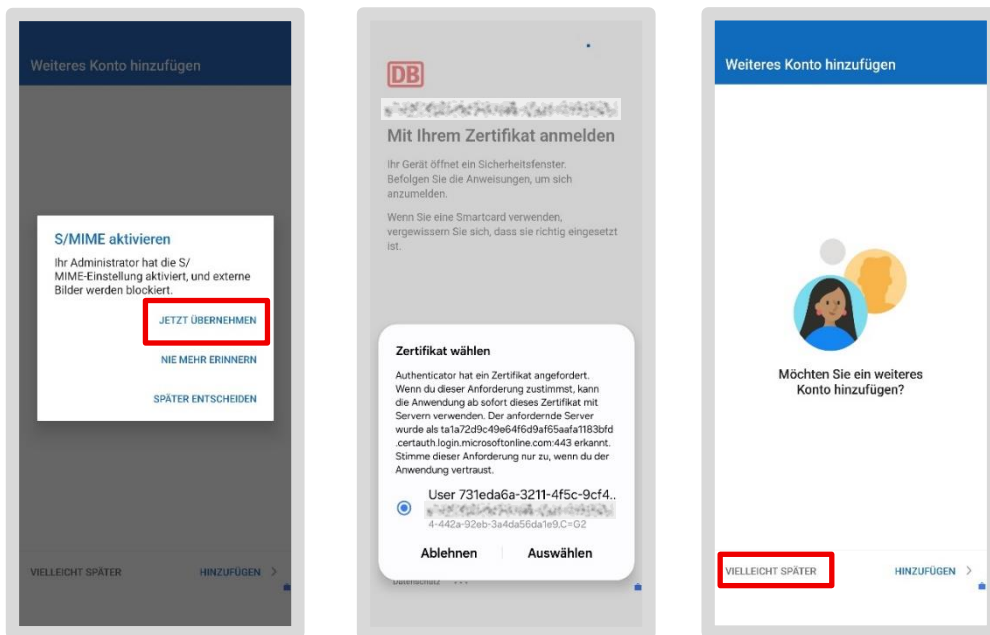
- Die DB stellt dafür die sogenannte S/MIME-Verschlüsselung zur Verfügung
- Tippe auf „Jetzt übernehmen“ bei der Abfrage, ob du S/MIME aktivieren möchtest

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

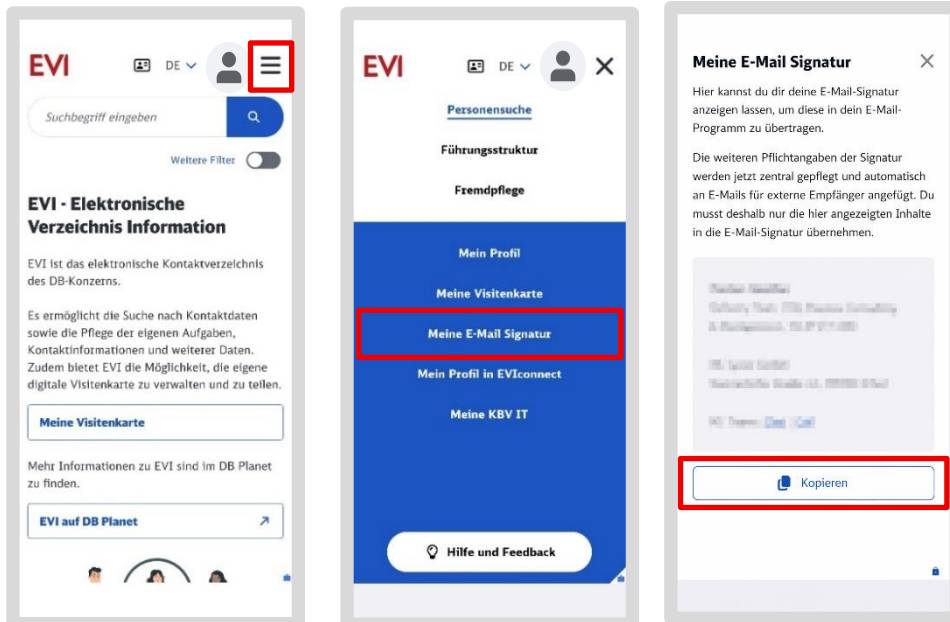
Android 16: Bei Smartphones/Tablets mit Android 16 kann es vorkommen, dass der Schritt zur Aktivierung von S/MIME übersprungen wird. In diesem Fall muss die Einrichtung von *Outlook* abgeschlossen und die App neu gestartet werden! Anschließend erscheint die Abfrage zur Aktivierung.

7.2.1 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“.

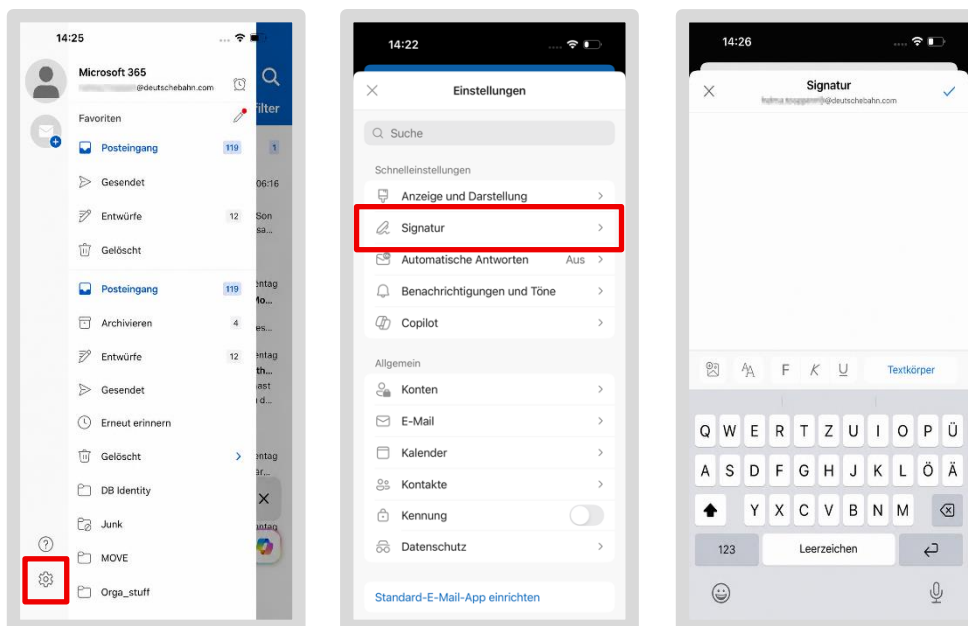
So bekommst du deine E-Mail Signatur aus EVI:

- 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 mit
- 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.

7.2.2 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 Smartphone/Tablet, ob iPhone/iPad oder BKU-Rechner/Basic Workplace Rechner, du dich anmeldest, du bist immer auf dem aktuellen Stand.

7.3 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 1x die App.

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

7.3.1 MS Defender App einrichten

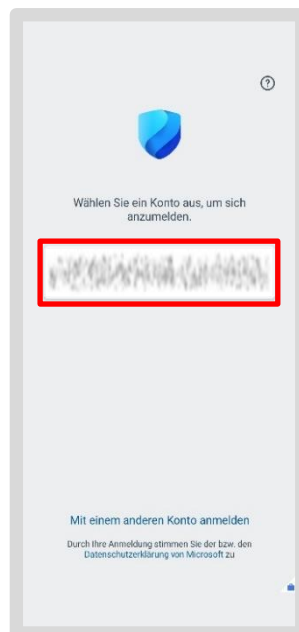
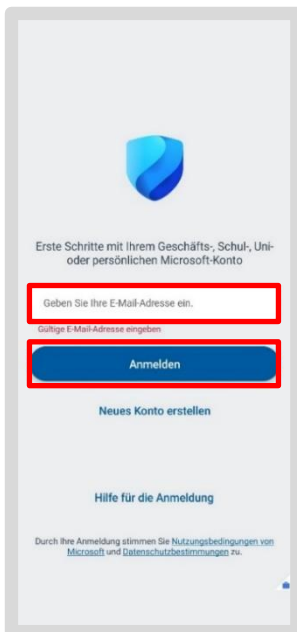
Um die *MS Defender App* auf deinem Smartphone/Tablet einzurichten, musst du folgende Schritte durchführen:

- 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

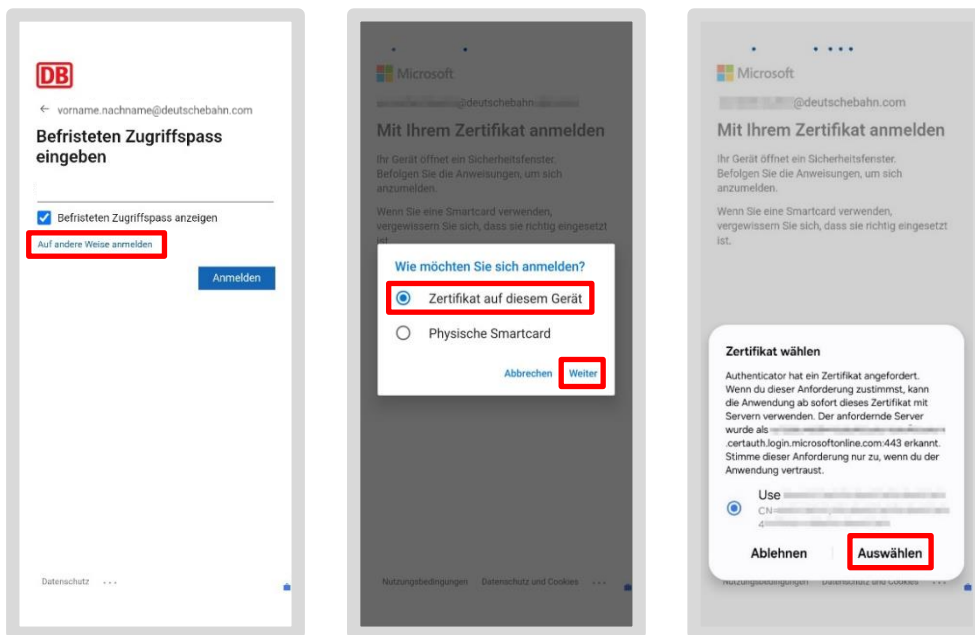


Wenn du innerhalb von einer Stunde dein Smartphone/Tablet mit der Intune App aktiviert hast, kann es sein, dass du hier nochmal aufgefordert wirst dein befristeten Zugriffspass einzugeben.

- Tippe auf „Auf andere Weise anmelden“



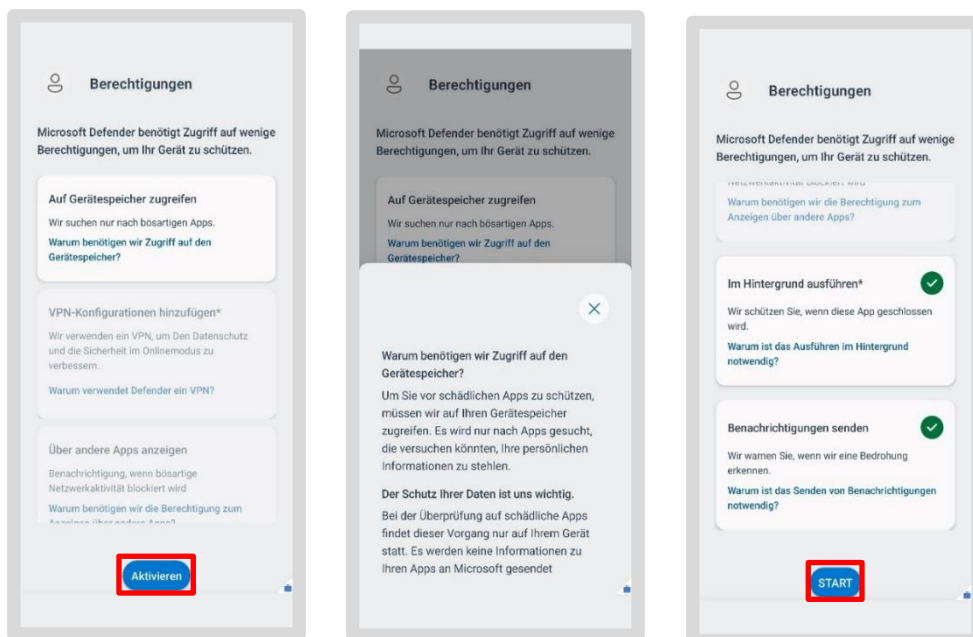
- Tippe bei der Abfrage auf „Zertifikat auf diesem Gerät“ und tippe auf „Weiter“
- Wähle das Zertifikat aus



7.3.2 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

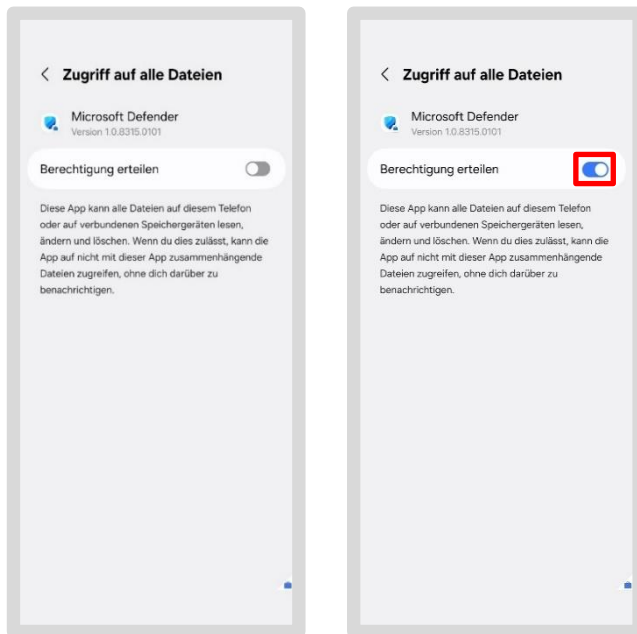


Hintergrundinfo Berechtigungen:

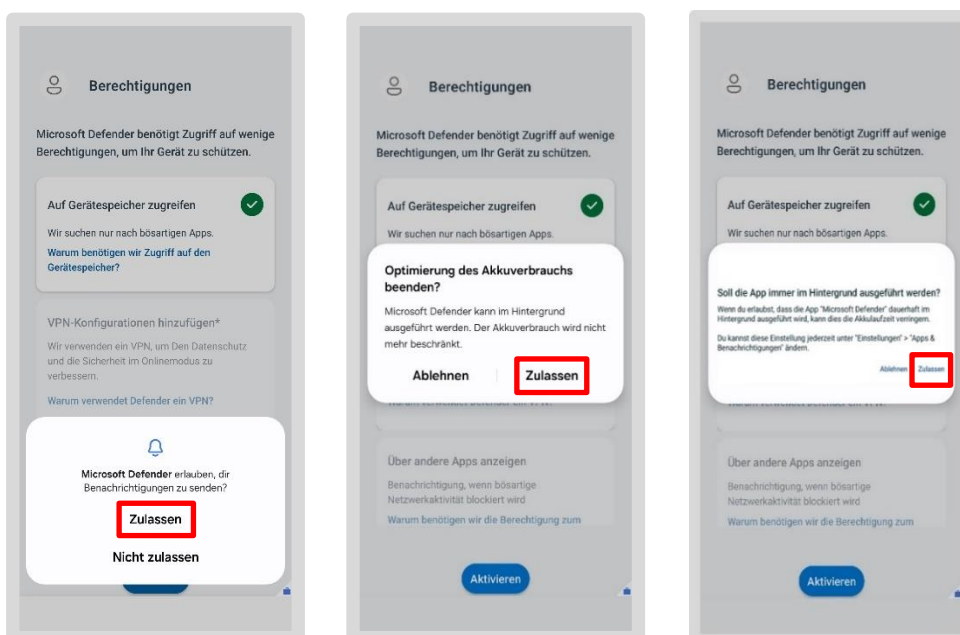
Diese Berechtigungen sind erforderlich, damit die Anwendung einwandfrei funktioniert und die Sicherheit auf deinem Gerät gewährleistet ist.

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“



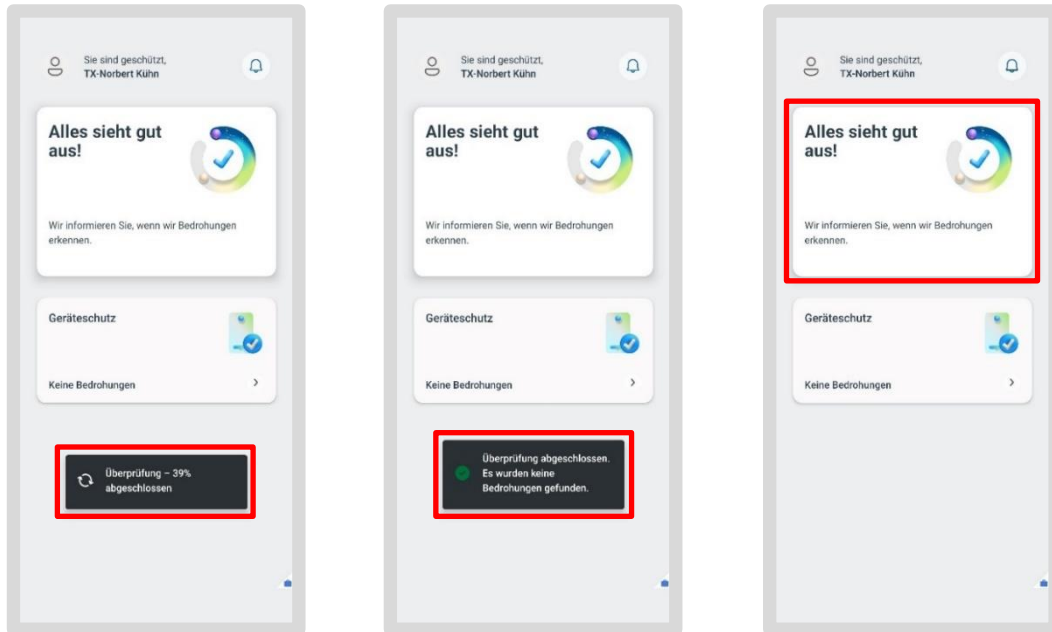
- Tippe bei allen folgenden Abfragen jeweils auf „Zulassen“



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.

7.4 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

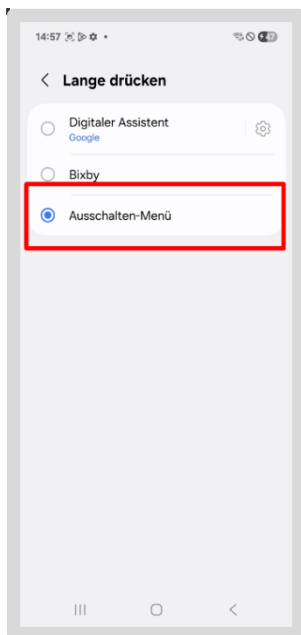
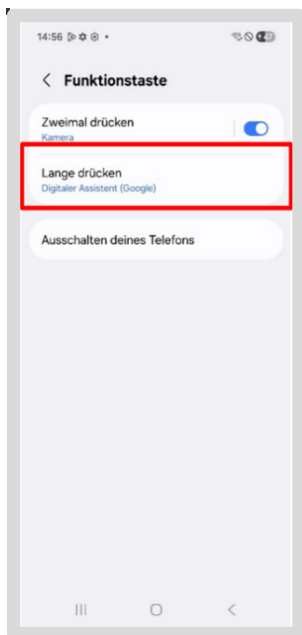
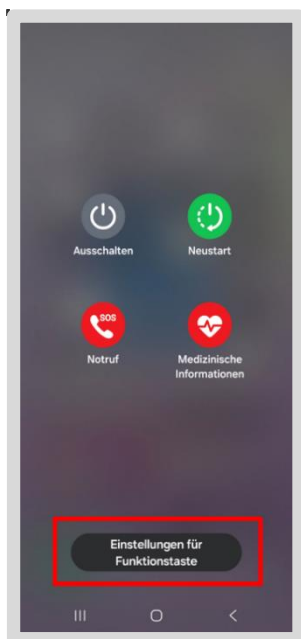


- Tippe anschließend auf „Installieren“
- Wenn du nun eine Datei öffnest, öffnet sich die App automatisch

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

7.5 Bixby-Taste ausschalten

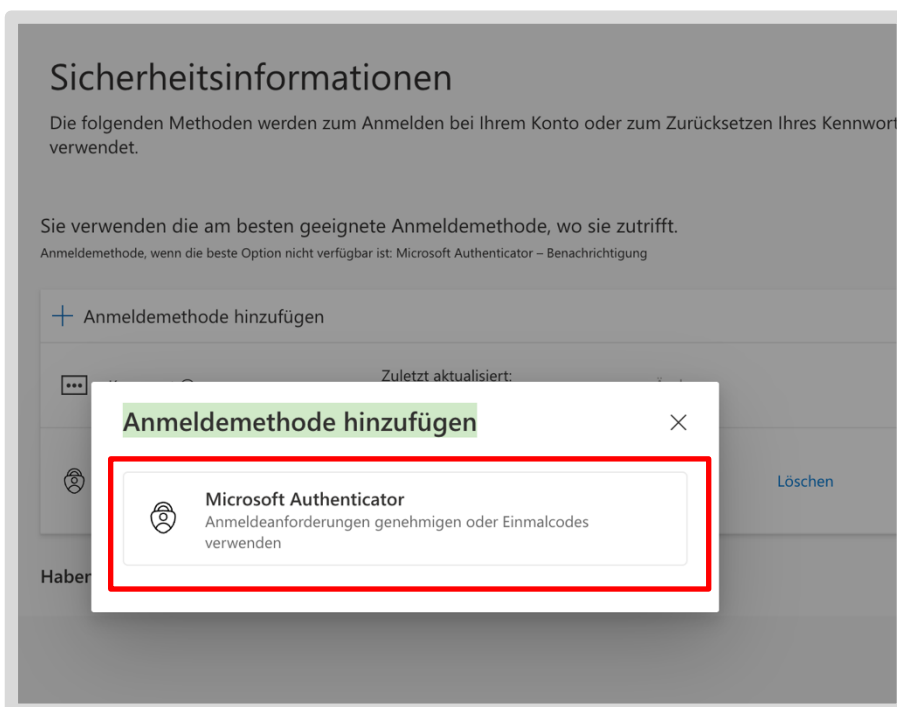
- Die Power-Taste startet standardmäßig den Bixby-Sprachassistenten. Aus Sicherheitsgründen muss dieser deaktiviert werden:
- Wische einmal von oben nach unten über den Bildschirm. Es öffnet sich das Kontrollzentrum
- Tippe auf das Power-Icon oben rechts neben dem Einstellungsicon
- Wähle „Einstellungen für Funktionstaste“
- Ändere die Funktion bei „Lange drücken“ auf „Ausschalten-Menü“



7.6 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

Tip: Solltest du Schwierigkeiten haben, die Verbindungen in der Authenticator-App nach der Wiederherstellung 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 wiederhergestellt!

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