



Betriebssystem-Version iOS 26.5

Migration iPhone/iPad

DB Workplace Mobile

DB Systel GmbH | 26.06.2026

Inhaltsverzeichnis

1 Der Ablauf der Migration auf einen Blick	3
2 Migration starten	4
2.1 Authenticator App – optional	4
2.2 Aufheben des Blockierungsmodus – optional	4
2.3 Erstellen eines befristeten Zugriffspass (TAP) - Expertenmodus	4
2.4 Migration sofort nach der Mitteilung starten	5
2.5 Migration zu einem späteren Migrationszeitraum starten	5
2.6 Migration in dem Migrationszeitraum starten	6
3 iPhone/iPad in der DB anmelden	7
3.1 Konfiguration durchführen	7
4 Befristeten Zugriffspass (TAP) erstellen	8
4.1 Befristeten Zugriffspass (TAP) erstellen	8
4.2 Befristeten Zugriffspass für eine(n) Kollegen:in erstellen	11
5 Gerät aktivieren: Unternehmensportal App	13
5.1 Zugriff auf alle DB Apps und Webseiten einrichten	14
5.2 E-Mail Verschlüsselung einrichten	16
5.3 DB Apps	17
6 Einstellungen am Gerät vornehmen	18
6.1 iOS-Betriebssystem Updates installieren	18
6.2 Outlook einrichten / E-Mail-Konto erstellen	19
6.2.1 E-Mail Signatur einrichten	19
6.2.2 E-Mails verschlüsseln	21
6.2.3 Die E-Mail Synchronisierung – Alle E-Mails immer auf dem aktuellen Stand	21
6.3 Microsoft Defender App einrichten	21
6.3.1 Berechtigungen vergeben	22
6.4 Microsoft Authenticator App wieder aktivieren	24
6.5 Aktivieren des Blockierungsmodus – optional	24
6.6 Hinweise zur Nutzung von Apps	25
6.7 Dateien sichern	25

1 Der Ablauf der Migration auf einen Blick

Der gesamte Migrationsprozess auf DB Workplace Mobile ist hier zusammengefasst:



Technische Migrationsvorbereitung

- **Erinnerungs-E-Mail** einen Tag vor dem Termin, dass die Migration gestartet werden kann



Persönliche Migrationsvorbereitung

- Erstelle Screenshots oder Notizen von deinen fachlichen Apps, diese sind dann wieder erneut herunterzuladen
- Falls du die Authenticator App nutzt:
> siehe [Kapitel 2.1 Authenticator App - optional](#)



Starte Migration

- **Nach Erhalt der Migrations-E-Mail:**
Am darauffolgende Tag ist eine Mitteilung auf deinem iPhone/iPad
> siehe [Kapitel 2 Migration starten](#)



Migration auf DB Workplace Mobile

- **Erstelle und notiere** den befristeten Zugriffspass (TAP)
> siehe [Kapitel 4 Befristeten Zugriffspass \(TAP\) erstellen](#)
- **Aktiviere** das iPhone/iPad Microsoft Intune-Unternehmensportal App, kurz *Unternehmensportal App*
> siehe [Kapitel 5 Gerät aktivieren: Unternehmensportal App](#)
- **iPhone/iPad, das nicht in diesem Zeitraum migriert wurde,** muss nach dem Ablauf neugestartet - in manchen Fällen - wiederhergestellt werden. Hierbei können dienstliche und private Daten verloren gehen

Wichtig!

Dein iPhone/iPad ist noch nicht mit dem DB Management (Intune) verbunden.

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

Outlook oder Teams sind dafür die falschen Apps!

Folge dieser Anleitung Schritt-für-Schritt!

2 Migration starten

Die Migration auf das Managementsystem Intune kann von dir selbst gestartet werden, ebenso der Zeitpunkt wann du die Migration durchführen möchtest.

So ist der Ablauf:

- Du erhältst eine E-Mail mit der Information, ab welchem Datum (z. B. 15.06.2026) du die Migration starten kannst. Der Migrationszeitraum beträgt **bis zu vier Wochen**
- Am folgenden Tag erscheint auf deinem iPhone/iPad eine Mitteilung mit dem Titel „Registrierung erforderlich“
- Du kannst selbst entscheiden, ob du die Migration **sofort** starten möchtest oder **zu einem späteren Zeitpunkt** innerhalb des Migrationszeitraums

2.1 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.

- Während der Migration kann die *Authenticator App* **nicht genutzt** werden!
- Wenn Du Webseiten oder Apps mit einem anderen Account über die Authenticator App nutzt, so notiere Dir das, Du musst sie nach der Migration erneut verknüpfen
- Es sind keine weiteren Schritte notwendig
- Nach der Migration muss die App erneut aktiviert werden, das wird in Kapitel 6.4 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:
 - > Einrichtung der Multi-Faktor-Authentifizierung (MFA)

2.2 Aufheben des Blockierungsmodus – optional

Wenn du für das iPhone/iPad den Blockierungsmodus aktiviert hast, ist es notwendig diesen vor der Migration aufzuheben.

> Hierzu gehe auf die Apple Support Seite und deaktiviere den Modus

2.3 Erstellen eines befristeten Zugriffspass (TAP) - Expertenmodus

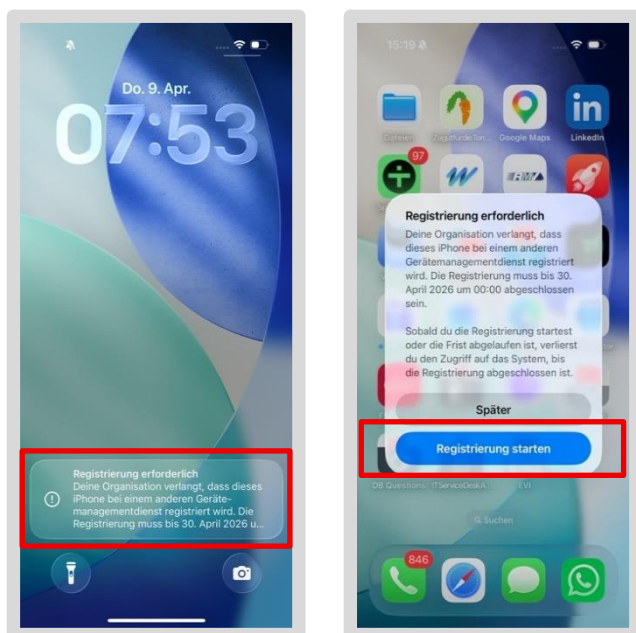
Wenn du nur ein DB iPhone/iPad besitzt und ohne fremde Hilfe dein Gerät zurücksetzen kannst, dann erstelle dir vor dem Zurücksetzen den befristeten Zugriffspass (TAP).

- > Springe dafür in Kapitel 4 Befristeten Zugriffspass (TAP) erstellen
- Starte danach mit der Migration

2.4 Migration sofort nach der Mitteilung starten

Um die Migration sofort zu starten, gehe wie folgt vor:

- Tippe auf die Mitteilung und im nachfolgenden Dialog auf „Registrierung starten“
- > Gehe zu Kapitel 3 iPhone/iPad in der DB anmelden



2.5 Migration zu einem späteren Migrationszeitraum starten

Wenn es zeitlich für dich ungünstig ist jetzt dein iPhone/iPad zu migrieren, gehe so vor:

- Tippe auf die Mitteilung und dann in nachfolgenden Dialog auf „Später“
- Bis zum Ablauf der Frist siehst du täglich die Mitteilung auf dem Startbildschirm deines iPhones/iPads

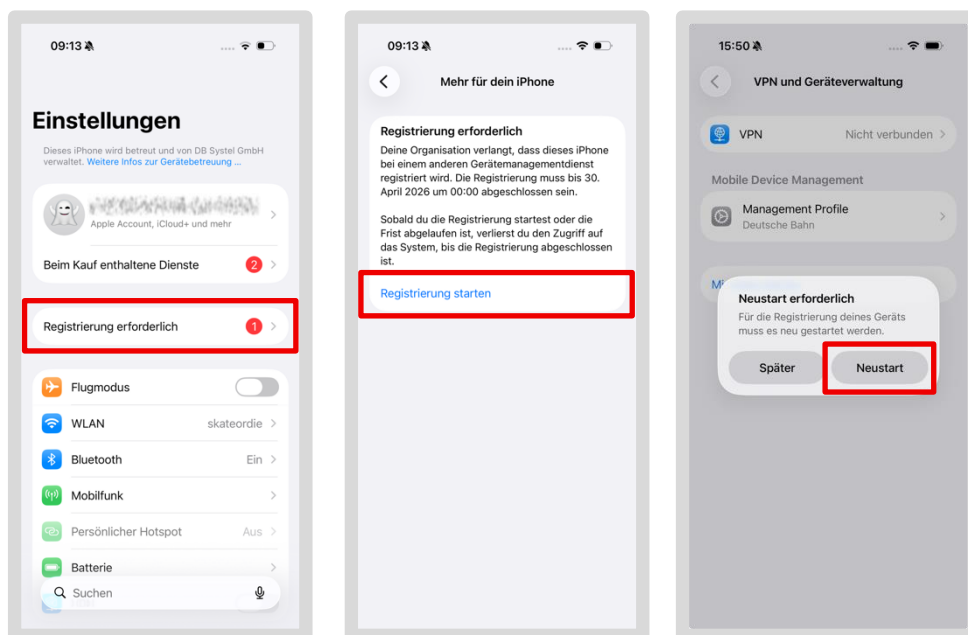
> Gehe zu Kapitel 3 iPhone/iPad in der DB anmelden



2.6 Migration in dem Migrationszeitraum starten

Wenn du nicht auf die tägliche Mitteilung warten möchtest, sondern ohne die Mitteilung migrieren möchtest, gehe so vor:

- Öffne die App *Einstellungen*
 - Tippe auf „Registrierung erforderlich“ und anschließend auf „Registrierung starten“
 - Tippe auf „Neustart“, um dein Gerät neu zu starten
- > Gehe zu Kapitel 3 iPhone/iPad in der DB anmelden

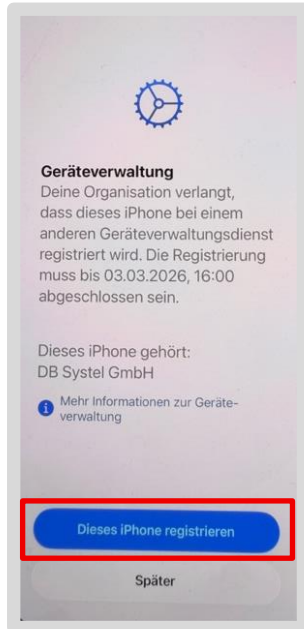


> **Hinweis:** Wenn Du eine E-Mail erhalten hast, aber keine Mitteilung erscheint und auch keine Aufforderung „Registrierung erforderlich“ auf deinem iPhone/iPad erscheint. Erstelle ein Ticket in der *IT ServiceDesk App*, wie in DB Questions beschrieben.

3 iPhone/iPad in der DB anmelden

Im nächsten Schritt muss dein DB iPhone/iPad wieder mit dem DB Management (Intune) verbunden werden.

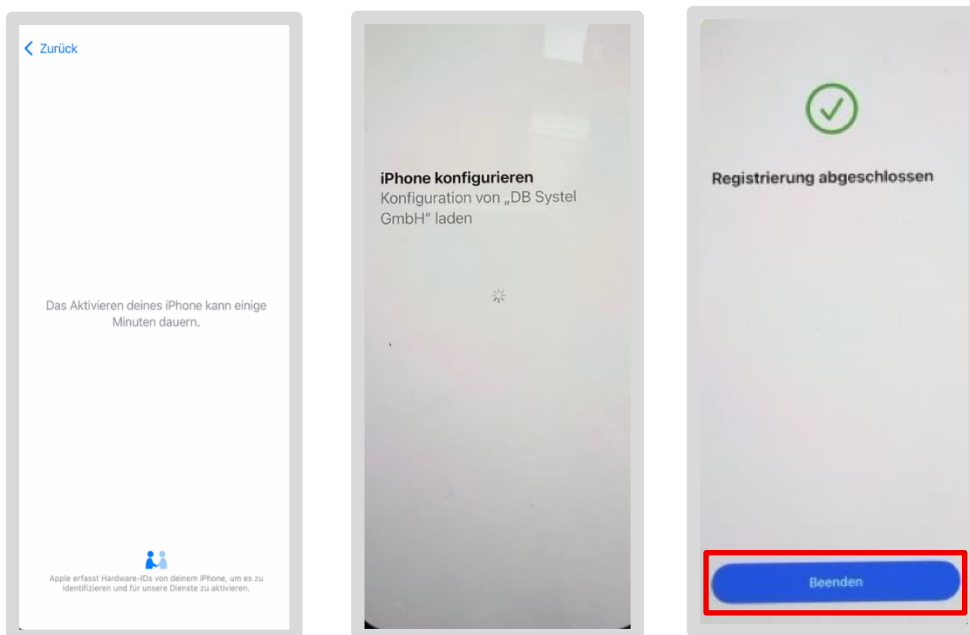
- Bestätige die folgenden Abfragen mit „Dieses iPhone registrieren“



3.1 Konfiguration durchführen

In diesem Schritt erhält dein iPhone/iPad die Enterprise Konfiguration. Dieser Vorgang kann einige Minuten dauern.

- Tippe dann auf „Beenden“



4 Befristeten Zugriffspass (TAP) erstellen

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

- einen gültigen befristeten Zugriffspass (TAP) - db.de/tap
- deinen DB User Name und DB User Passwort
- die Microsoft Intune-Unternehmensportal App, kurz Unternehmensportal 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 oder öffne die IT ServiceDesk App und gehe auf „Mein Profil“

4.1 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 iPhone/iPad** oder einen DB Workplace Windows oder Mac, 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 DB Workplace Windows oder Mac besitzt. Gehe hier zu:

- > [Kapitel 4.1 Befristeten Zugriffspass für eine\(n\) Kollegen:in erstellen](#)

Variante 3 - Expertenmodus:

Du besitzt **nur ein iPhone/iPad** 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 5 Gerät aktivieren: Unternehmensportal App](#)

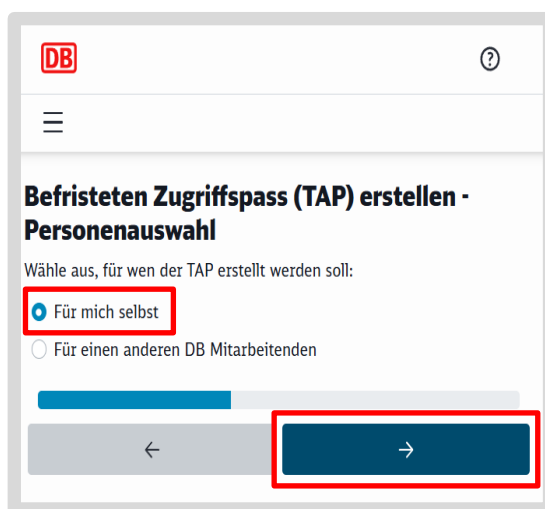
Beachte: Dein Tap ist nur 60 Minuten und für mehrere Smartphones/Tablets gültig!

Über die Willkommen App im iPhone/iPad, gehe so vor:

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

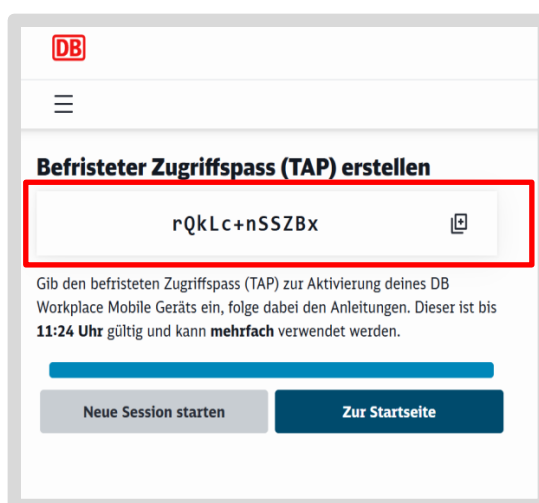
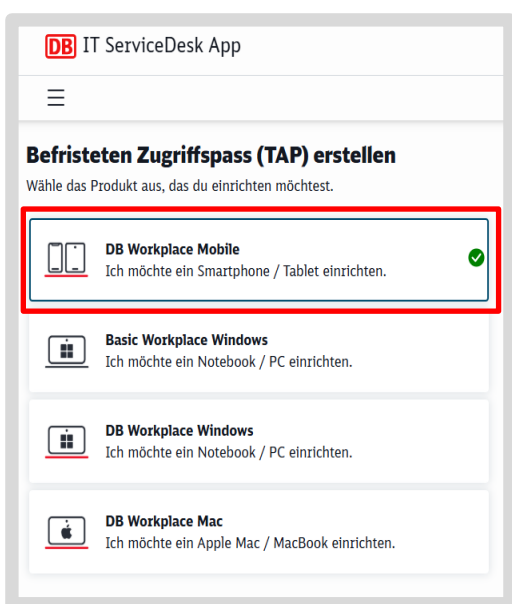
Über deinen DB Workplace Windows oder Mac:

- 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 **Unternehmensportal App**!



Wichtig!

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

- Du kannst jetzt dein iPhone/iPad in der *Unternehmensportal App* aktivieren
- > Gehe direkt weiter zu Kapitel 5 Gerät aktivieren: Unternehmensportal App

Wichtig!

Dein iPhone/iPad ist noch nicht mit dem DB Management (Intune) verbunden !

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

Folge dafür der Schritt-für-Schritt-Anleitung in
> Kapitel 5 Gerät aktivieren: Unternehmensportal App

4.2 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

The left screenshot shows the 'Befristeten Zugriffspass (TAP) erstellen' screen. It includes instructions on how to create a TAP and a list of options: 'dich selbst' and 'einen Mitarbeitenden aus dem gleichen Unternehmen (siehe EVI 7)'. The 'Anmelden' section has fields for 'DB User Anmeldename' (Max Mustermann) and 'DB User Passwort', which are highlighted with a red box. A blue arrow button is at the bottom right.

The right screenshot shows the 'Einen befristeten Zugriffspass (TAP) ausstellen - Personenauswahl' screen. It has radio buttons for 'Für mich selbst' and 'Für einen anderen DB Mitarbeitenden' (selected). Below is a search bar with 'Lisa Mustermann' and a list of search results. The first result is highlighted with a red box and shows details for Lisa Mustermann. At the bottom, there is a checkbox 'Ich bestätige, dass ich die Identität des Mitarbeitenden festgestellt habe.' which is checked.

- 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

Beachte: Du brauchst ihn zur Einrichtung und Aktivierung der *Unternehmensportal App*!

The left screenshot shows the 'Befristeten Zugriffspass (TAP) ausstellen für Lisa Mustermann' screen. It includes a red box around the 'Anmelden' section, which contains fields for 'DB User Anmeldename' (filled with 'Lisa Mustermann') and 'DB User Passwort'. Below this is a 'Wichtiger Hinweis für Empfänger' section. At the bottom are back and forward navigation arrows.

The right screenshot shows the 'Befristeter Zugriffspass (TAP) erstellen' screen. It features a red box around the TAP code 'rQkLc+nSSZBx'. Below the code, it states: '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.' At the bottom are buttons for 'Neue Session starten' and 'Zur Startseite'.

- Der/die Kollege:in kann jetzt sein Smartphone/Tablet in der *Unternehmensportal App* aktivieren
- > Gehe direkt weiter zu Kapitel 5 Gerät aktivieren: Unternehmensportal App

Wichtig!

Dein iPhone/iPad ist noch nicht mit dem DB Management (Intune) verbunden !

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

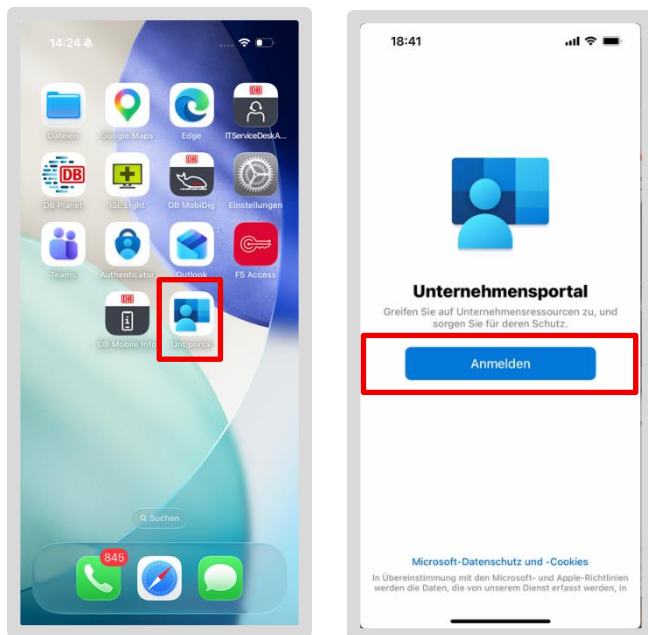
Folge dafür der Schritt-für-Schritt-Anleitung in
> Kapitel 5 Gerät aktivieren: Unternehmensportal App

5 Gerät aktivieren: Unternehmensportal App

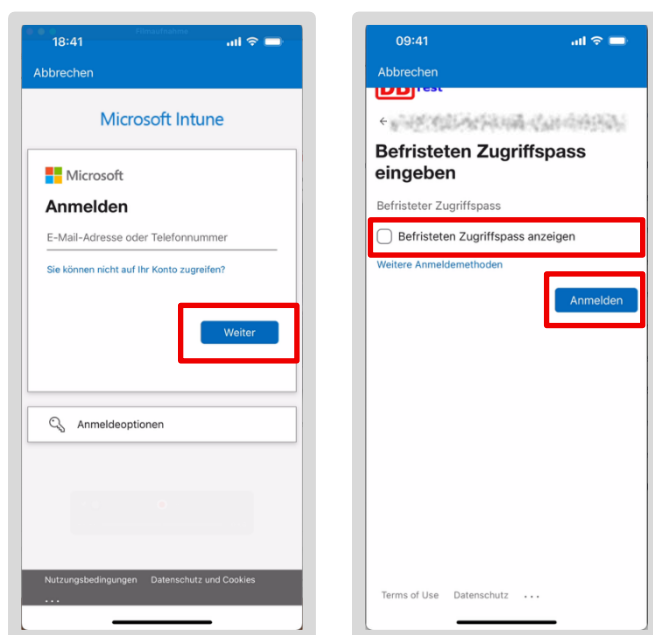
> **Beachte:** Prüfe, ob du einen befristeten Zugriffspass (TAP) wie in Kapitel 4 Befristeten Zugriffspass (TAP) erstellen beschrieben erstellt und erhalten hast!

> **Hinweis:** Eine Video-Anleitung dazu ist hier zu finden: db.de/mobile-videoanleitungen

- Öffne die *Unternehmensportal* App (Unt. Portal)
- Tippe dann auf den Button „Anmelden“



- Gib deine **DB User E-Mail-Adresse** ein (Nicht den 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:

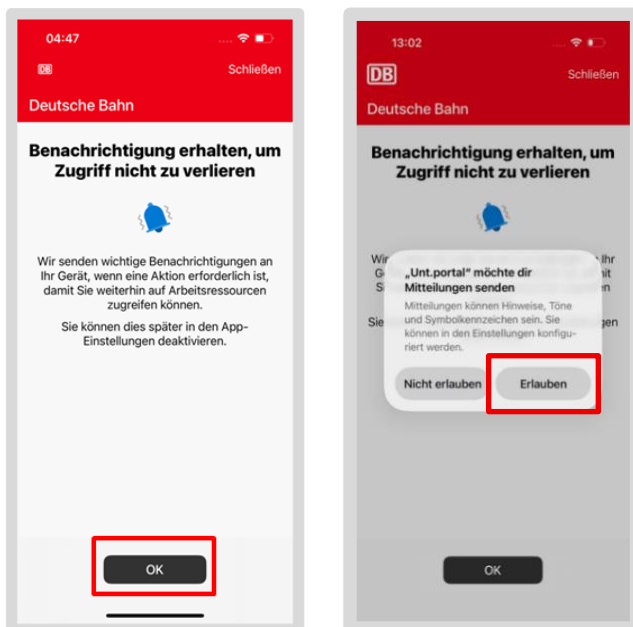
- erstelle dir einen neuen befristeten Zugriffspass und wiederhole die Anmeldung, wie in Kapitel 4.1 Befristeten Zugriffspass (TAP) erstellen beschrieben
- > Gehe weiter zu Kapitel 5.1 Zugriff auf alle DB Apps und Webseiten einrichten

5.1 Zugriff auf alle DB Apps und Webseiten einrichten

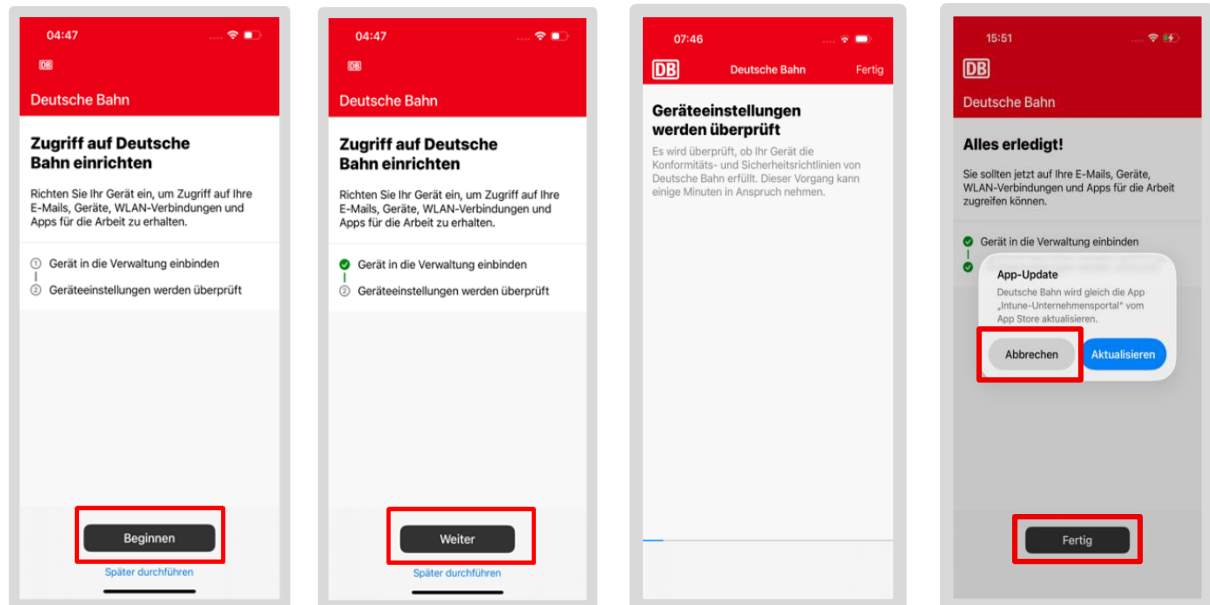
Beachte: Die Bereitstellung der Zertifikate kann **5 Minuten bis 1 Stunde** dauern. Erst danach kannst du deine Apps wie *Outlook*, *Teams*, etc. nutzen.

Wichtig: Bleibe während aller Schritte an deinem iPhone/iPad, sonst richtet sich das iPhone/iPad nicht in der *Unternehmensportal App* ein und du bist nicht arbeitsfähig!

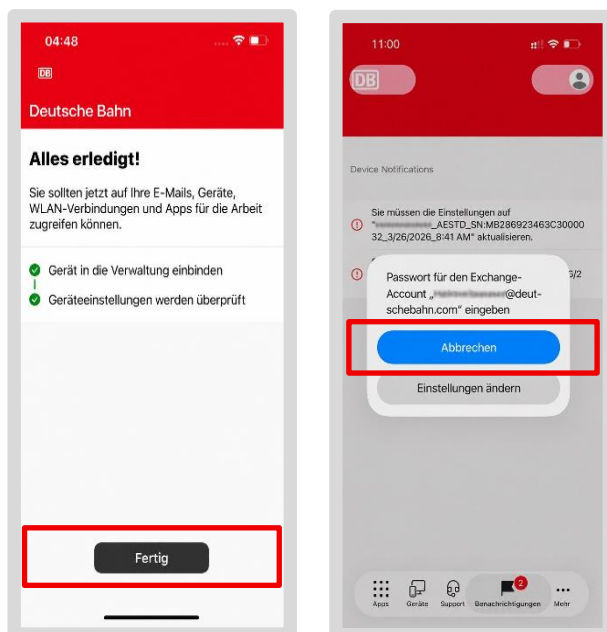
- Bei der Abfrage zu Benachrichtigung erhalten tippe auf „OK“
- Tippe dann bei dem Dialog auf „Erlauben“



- Tippe auf „Beginnen“, um den Zugriff auf das DB Management zu erhalten
- Tippe dann auf „Weiter“
- Tippe bei den folgenden Abfragen auf „Abbrechen“ und tippe dann auf „Fertig“



- **Hinweis:** Die Geräteeinstellungen werden überprüft, warte einen Augenblick!
- Wenn der Dialog zum Aktualisieren jetzt wieder hochkommt, tippe auf „Aktualisieren“
- Wenn der Dialog zur Abfrage des Exchange-Account erscheint, tippe auf „Abbrechen“

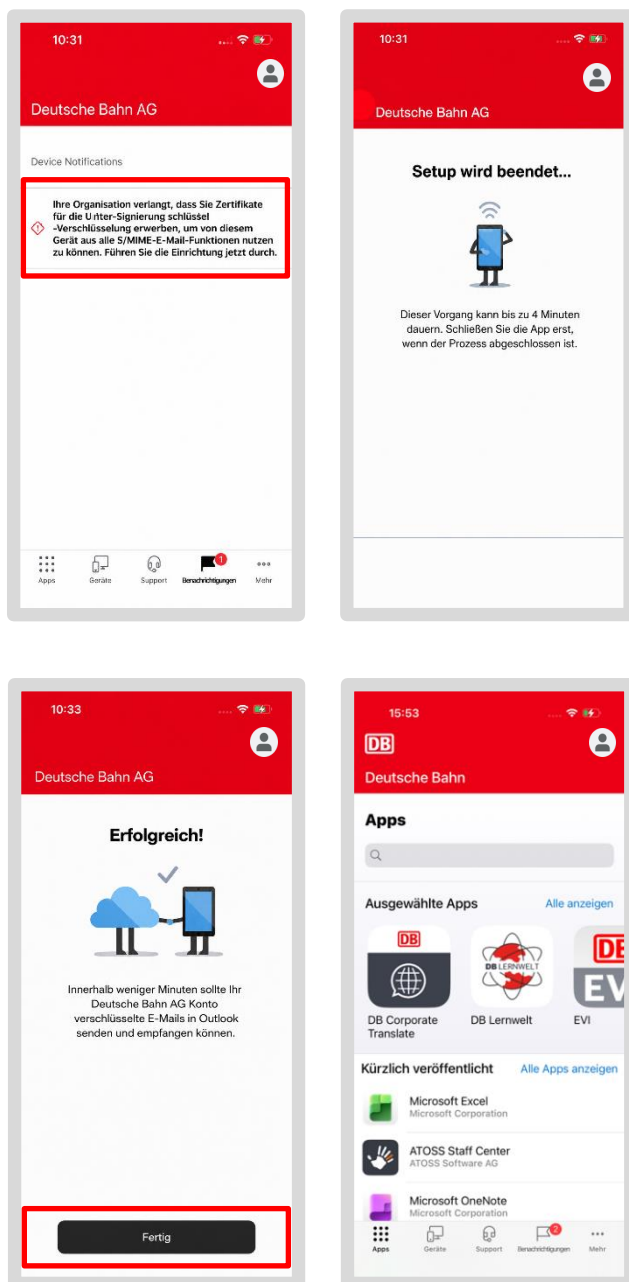


5.2 E-Mail Verschlüsselung einrichten

Wenn „Alles erledigt!“ erscheint:

- Wische im hellgrauen Bereich von oben nach unten, um die Seite zu aktualisieren
- Es erscheint eine Mitteilung zur Einrichtung von Zertifikaten für E-Mail-Signierung und -Verschlüsselung
- Tippe auf die Mitteilung, dann werden diese geladen und es erscheint „Setup wird beendet...“
- Tippe auf „Fertig“, verschlüsselte E-Mails können nun empfangen werden
- Du siehst nun alle DB Apps, die in der *Unternehmensportal App* herunterladbar sind

> Möchtest Du die Verschlüsselung erst später einrichten, dann schau auf [DB Questions](#)

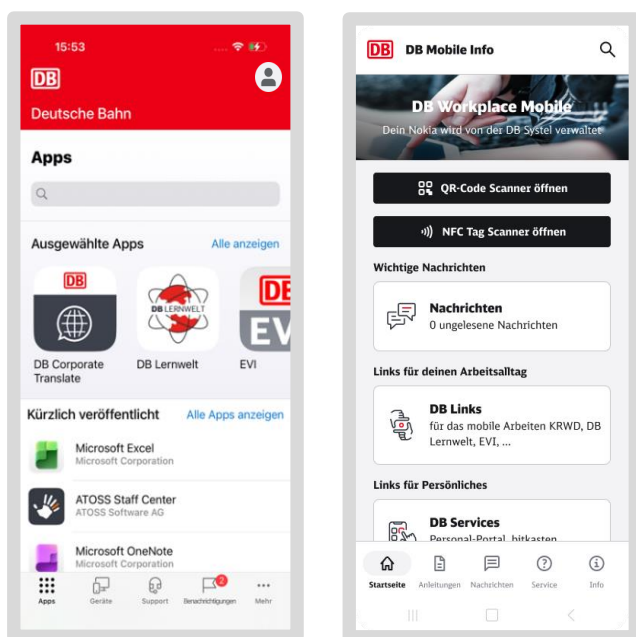


5.3 DB Apps

Nach Abschluss der Migration werden DB Apps wie z. B. *Outlook* oder *Teams* automatisch heruntergeladen. Deine unternehmensspezifischen bzw. geschäftsfeldspezifischen Apps werden danach geladen.

- Weitere DB Apps kannst du aus der *Unternehmensportal App* herunterladen
- Falls du ASES bzw. ATOSS Staff Center als Zeiterfassung nutzt, ist hier die Anleitung zu den wichtigsten Funktionen des ATOSS Staff Center
- Wenn Du den *DB Navigator* für Dein Deutschlandticket nutzt, kannst du es so wieder in der App aktivieren
- Nutze Safari als Standardbrowser für Weblinks, wie DB Planet oder DB Questions
- Mit der DB Passwort App speicherst du Passwörter auf deinem iPhone/iPad
- Nutze die *App Outlook* für E-Mails, Kalender und Kontakte, die Synchronisation mit den nativen Apple *App Mail* und *App Kalender* wird nicht mehr angeboten
- Für private Apps benötigst du eine private Apple-ID, gebe hierfür deine private E-Mail ein

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

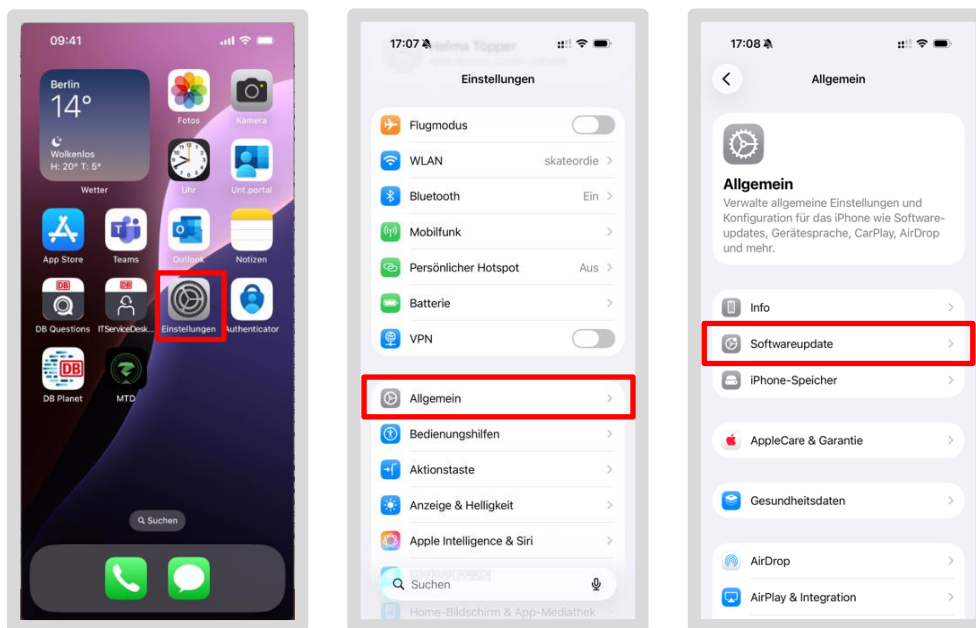


6 Einstellungen am Gerät vornehmen

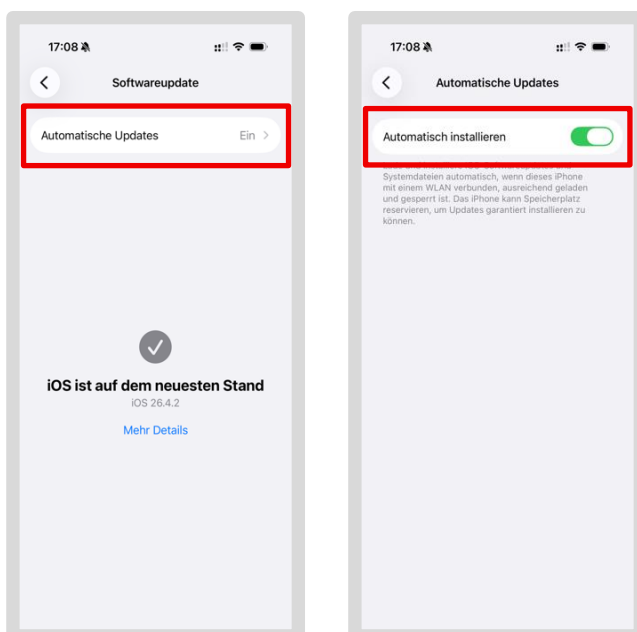
Beachte: Die Bereitstellung der Zertifikate kann **5 Minuten bis 1 Stunde** dauern. Erst danach kannst du deine Apps wie *Outlook*, *Teams*, etc. nutzen.

6.1 iOS-Betriebssystem Updates installieren

- Öffne die App Einstellungen
- Tippe auf „Allgemein“
- Tippe dann auf „Softwareupdate“ (hier werden neue Software-Versionen angezeigt)



- aktiviere die Funktion „automatische Updates“



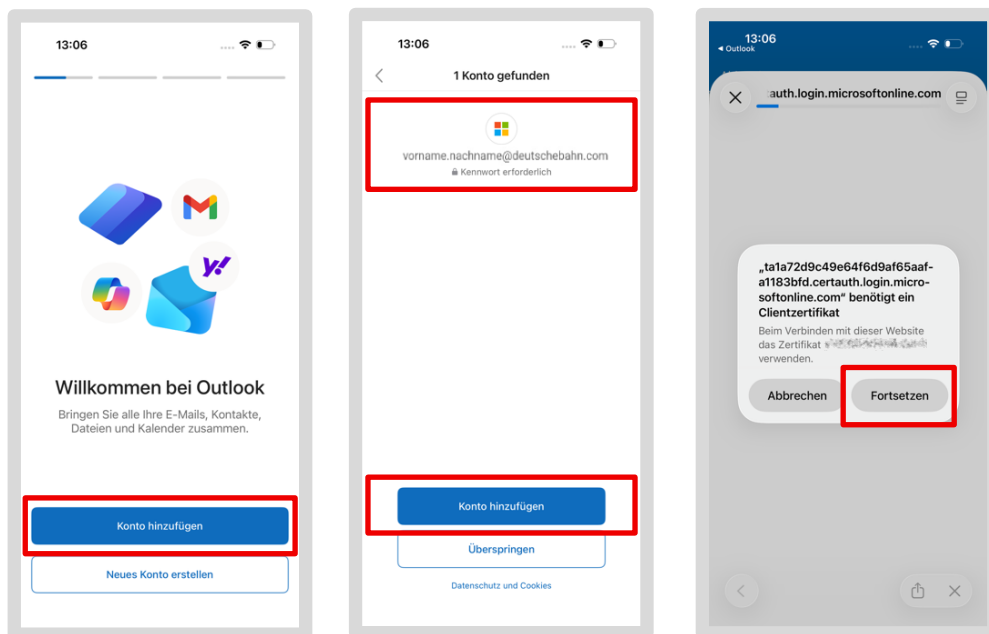
Wichtig:

Wenn ein Button mit „Automatisch aktualisieren“ angezeigt wird, tippe auf diesen und dann auf „Automatisch herunterladen“. Das iPhone/iPad lädt das Update herunter und installiert es, du solltest hierzu mit dem WLAN verbunden sein. Ansonsten kann es passieren, dass dein iPhone/iPad nicht die DB Apps nutzen kann bzw. die Zertifikate für dein iPhone/iPad nicht bereitgestellt werden können!

6.2 Outlook einrichten / E-Mail-Konto erstellen

Beachte: Die Bereitstellung der Zertifikate kann **5 Minuten bis 1 Stunde** dauern. Erst danach kannst du deine Apps wie *Outlook*, *Teams*, etc. nutzen.

- Tippe auf die App *Outlook*
- Dein E-Mail-Konto sollte bereits hinterlegt sein – tippe dann auf „Konto hinzufügen“
- Wähle deine E-Mail-Adresse aus, indem du auf „Konto hinzufügen“ tippst
- Tippe auf „Fortsetzen“ bei der Zertifikatsabfrage



Dein E-Mail-Konto wird nun eingerichtet:

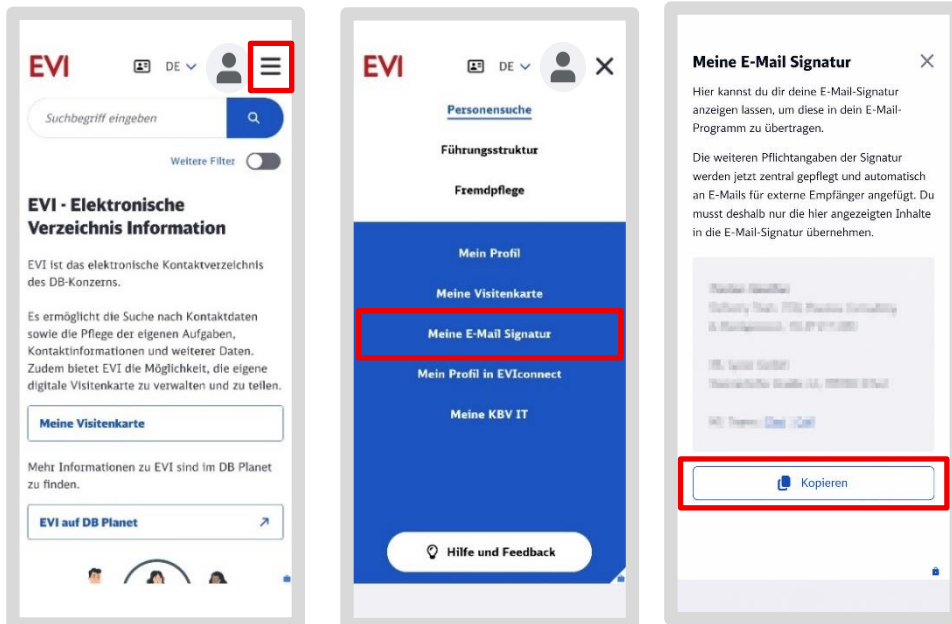
- Tippe auf „Vielleicht später“ bei der Abfrage für ein weiteres Konto hinzufügen
- Und „Nein, danke“ bei Benachrichtigung aktivieren
- Deine E-Mails werden nun geladen (dieser Prozess kann einige Minuten dauern)
- Anschließend kannst du wieder E-Mails lesen und schreiben

6.2.1 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 Telefonbuch der DB, dem sogenannten „EVI“.

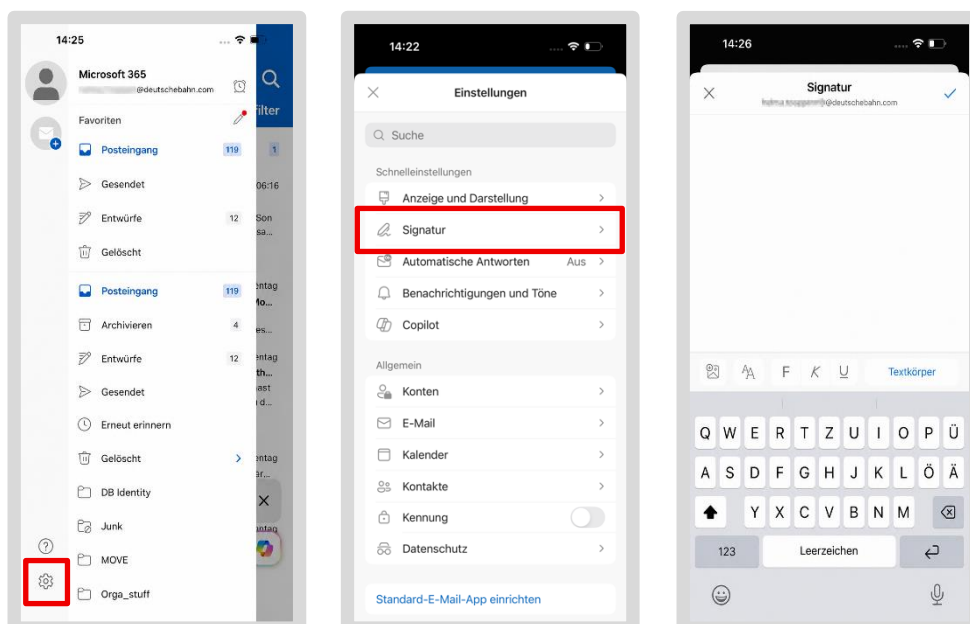
So bekommst du deine E-Mail Signatur aus EVI:

- 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 neu geschriebenen E-Mails 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.

6.2.2 E-Mails verschlüsseln

E-Mails, die du innerhalb des DB-Konzerns versendest, erhalten standardmäßig eine Verschlüsselung. Für die meisten Anliegen reicht diese aus. Du brauchst nichts weiter tun!

Wenn du eine E-Mail versendest, achte aber grundsätzlich auf diese beiden Regeln:

- Die E-Mail enthält nur so viel personenbezogene Daten wie nötig
- Der Betreff der E-Mail enthält keine vertraulichen Informationen
- Sofern du besonders schützenswerte Daten (z.B. Personaldaten) per E-Mail versenden möchtest, musst du zusätzlich den Inhalt der E-Mail verschlüsseln. *Outlook* bietet dir eine E-Mail-Verschlüsselung an.

Verschlüsselung einrichten:

Wenn du das für dein iPhone/iPad nicht bereits erstellt hast, wie in [Kapitel 5.2 E-Mail Verschlüsselung einrichten](#) beschrieben, musst du nichts mehr tun.

> Wenn dies noch fehlt, richte die Verschlüsselung wie in [DB Questions](#) beschrieben ein

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

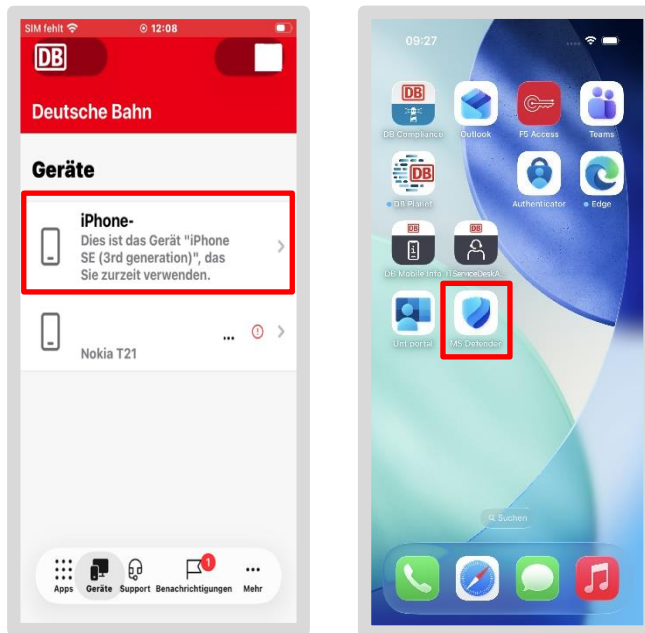
6.3 Microsoft Defender App einrichten

Die App Microsoft Defender: Sicherheit (kurz *MS Defender App*) schützt dein iPhone/iPad vor Schadsoftware, richte deshalb die App auf deinem iPhone/iPad ein.

Gehe so vor:

- Halte dein iPhone/iPad im **Hochformat**, damit die Screens so wie sie in der Anleitung dargestellt angezeigt werden können!
- Überprüfe, ob dein iPhone/iPad eingerichtet und im Unternehmensportal angemeldet ist!
- Öffne hierzu die *Unternehmensportal App* und tippe unten auf „Geräte“

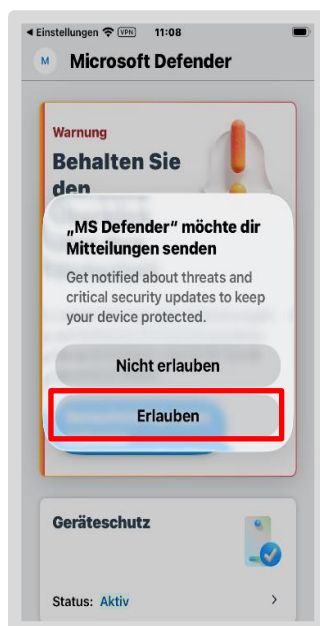
- Wenn du dein iPhone/iPad in der Übersicht siehst, ist es fertig eingerichtet
- Gehe zurück in den Home Screen des iPhones/iPads und suche nach der *MS Defender App*
- Tippe auf das App Icon der *MS Defender App*, um sie zu öffnen



6.3.1 Berechtigungen vergeben

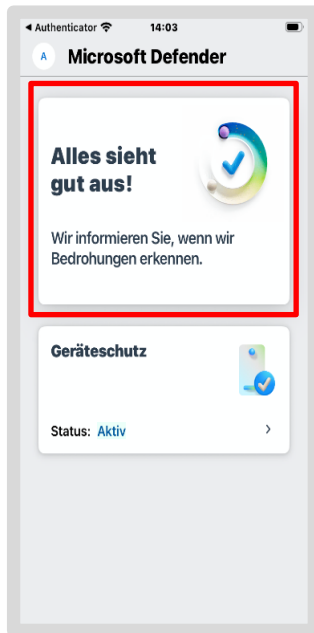
Die *MS Defender App* fragt ob Mitteilungen senden darf:

- tippe auf „Erlauben“



Folgende Bedrohungsanzeigen sind nun sichtbar:

- Wenn ein **grüner Haken** sichtbar ist, wurde **keine Gefahr erkannt**
 - Wenn **kein grüner Haken** sichtbar ist, warte bitte erst mal ein paar Stunden ab und starte die App neu (App schließen und erneut öffnen)
- > Wenn weiterhin kein grüner Haken erscheint, gehe auf: [DB Questions](#)

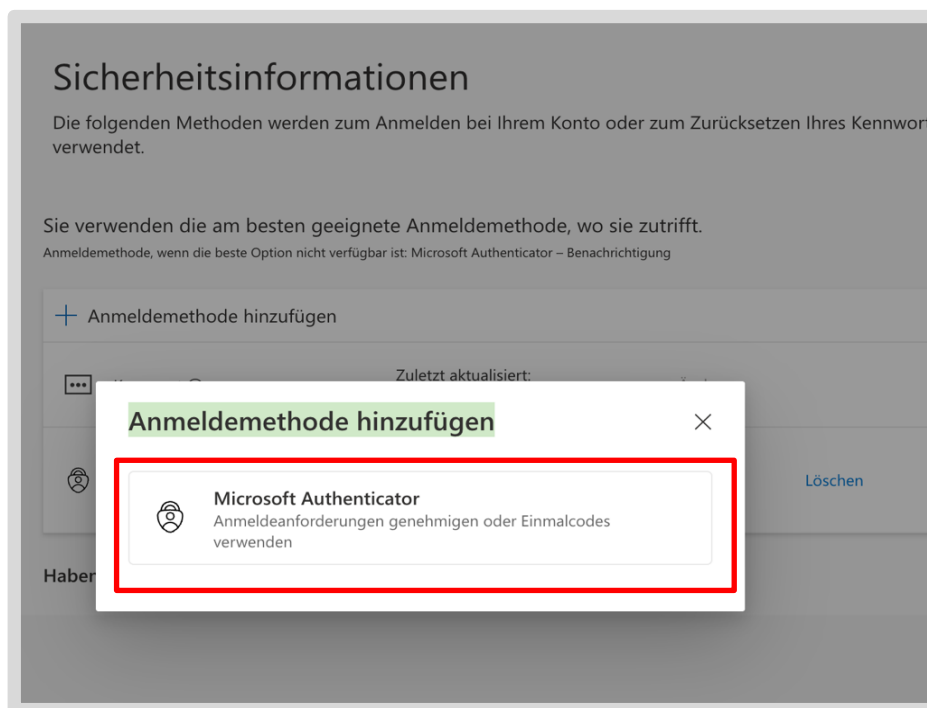


Das iPhone/iPad ist jetzt gegen Angriffe geschützt.

6.4 Microsoft Authenticator App wieder aktivieren

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

- Öffne die Seite auf db.de/authenticator auf deinem BKU- /Basic Workplace bzw. DB Workplace Windows oder Mac
- Tippe auf das „Plus-Icon“ und den Button „Anmeldemethode hinzufügen“
- es öffnet sich ein Dialog, wähle „Microsoft Authenticator“ aus



- Wechsle zu deinem iPhone/iPad 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 iPhone/iPad 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 Migration wieder zu aktivieren, nutze den Self Service: „Microsoft Authenticator App (MFA) zurücksetzen“: db.de/resetmfa und folge dann den Schritten von oben nach unten in diesem Abschnitt.

6.5 Aktivieren des Blockierungsmodus – optional

Wenn es für dein iPhone/iPad wichtig ist den Blockierungsmodus zu aktivieren und du das vor der Migration aktiviert hattest.

> Gehe auf die [Apple Support Seite](#) und aktiviere den Modus wie auf der Seite beschrieben

6.6 Hinweise zur Nutzung von Apps

Messenger

- WhatsApp wird nicht über die *Unternehmensportal App* bereitgestellt und ist nur mit den privat hinterlegten Kontakten nutzbar (Private Nutzung)
- Für die dienstliche Kommunikation nutze die über die *Unternehmensportal App* bereitgestellten Apps (bspw. *Teams*)

Kamera

- Für dienstliche Fotos nutze die *OneDrive App*, dadurch werden Fotos direkt in *OneDrive* gespeichert
- Die Kamera App ist nur für den privaten Gebrauch zu verwenden

6.7 Dateien sichern

- Speichere Dateien, bspw. PDF-Dokumente oder Bilder, nur in *OneDrive*, nicht lokal in der App „Dateien“
- Fotos nur in *OneDrive* speichern
- Dateien nicht über folgenden Weg speichern: „Teilen > Kopie senden (PDF) > Mit einer anderen App senden > PDF erstellen“

> Eine kurze Anleitung zur Datensicherung findest du hier: mobileworkplace.deutschebahn.com/mobile-daten-sichern

Glückwunsch!

Du hast dein dienstliches iPhone/iPad erfolgreich migriert!

Weitere Informationen zu deinem iPhone/iPad 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