



Operating system version: Android 15 or later

Migration Nokia/HMD

DB Workplace Mobile

DB Systel GmbH | 15 August 2026

Table of contents

1 The migration process at a glance	4
2 Steps required before migration	5
2.1 Book a migration appointment	5
2.2 Back up your data	5
2.3 Authenticator app – optional	5
2.4 Creating a Temporary Access Pass (TAP) – Expert mode	6
3 Start migration: Reset smartphone/tablet	7
3.1 Resetting your smartphone/tablet yourself	7
3.2 Reset your smartphone/tablet via the IT ServiceDesk app	8
4 Set up again	9
4.1 Select language	9
4.2 Set up Wi-Fi	10
4.3 Setting up Wi-Fi in DB buildings	11
5 Install Nokia/HMD Enterprise Mobility Management	12
5.1 Set up work profile	13
5.2 Set up screen lock	14
5.3 Installing DB apps	15
5.4 Google account – not required	15
5.5 Enable Google service	16
5.6 Complete setup	16
6 Activate device – Create a temporary access pass (TAP)	19
6.1 Create a temporary access pass (TAP)	19
6.2 Create a temporary access pass for a colleague	22
7 Activate the device in the DB	24
7.1 Set up access to all DB apps and websites	25
7.2 DB Apps	26
8 Required settings	27
8.1 Check for operating system updates	27
8.2 Outlook	28
8.2.1 Set up Outlook /Create an email account/Set up email encryption	28
8.2.2 Set up an email signature	29

8.2.3 Email synchronisation – All emails always up to date	31
8.3 MS Defender app – must be opened	31
8.3.1 Setting up the MS Defender app	31
8.3.2 Grant permissions	33
8.4 DB M 365	35
8.5 Reactivating the Microsoft Authenticator app	36

1 The migration process at a glance

The entire migration process to DB Workplace Mobile summarised here:



Planning the migration

- **As soon as you have received an email: Book an appointment in the PME tool**
> see [section 2.1 Booking an appointment for migration](#)



Technical migration preparation

- **Reminder email** shortly before the appointment, confirming that the migration can begin



Personal migration preparation

- **Back up your data**
> See [section 2.2: Backing up your data](#)
- *If you use the Authenticator app*
> see [section 2.3 Authenticator app – optional](#)
- **Perform a system update** – check this in the System Settings



Migration to DB Workplace Mobile

- **Reset** the smartphone/tablet
> see [Chapter 3 Start migration: Reset smartphone/tablet](#)
- **Create and make a note of** the temporary access pass (TAP)
> see [Chapter 6 Activate device – Create temporary access pass \(TAP\)](#)
- **Activate** the smartphone/tablet in Microsoft Intune
> see [Chapter 7: Activate device in the database](#)

Important!

Your smartphone/tablet is only activated with the Connected to the DB network when the **Temporary Access Pass (TAP)** has been entered in the *Intune app*. Outlook or Teams are not the right apps for this!

Follow these instructions step by step!

2 Steps required before migration

2.1 Book a migration appointment

- **Book an appointment for the migration in the PME tool at db.de/pme as soon as you are prompted to do so by email:**
 - If you are unable to do this yourself, ask your cost centre manager or authorised purchaser to book it for you. Appointments can be booked Monday to Friday for the following weekday (Mon–Fri) until 12 noon.
- **If you are unable to keep the migration appointment:** You can cancel the appointment by 12 noon the day before (Mon–Fri)!
 - **From the booked migration date, you have 28 days** to migrate your smartphone/tablet. The last possible date is displayed in PME. After that, your device will be automatically deleted and migrated to DB Workplace Mobile using Microsoft Intune.

2.2 Back up your data

> **Note:** You can find a video guide at db.de/mobile-videoanleitung

- **Back up your data** as soon as you have received an appointment confirmation email for the migration

To do this, follow these steps:

- a) Back up your work data and settings
- b) Back up your personal data and settings

If applicable:

- c) Remove your Samsung or Google account from your smartphone/tablet
- d) Remove all memory cards from your smartphone/tablet

> You can find instructions on how to back up your data at [Instructions - Back up data](#)

2.3 Authenticator app – optional

Note: This information applies only to users who actively use the Authenticator App, for example, for administrative access via the so-called ‘2-account’ or for multi-factor authentication, e.g. for VPN on a Basic Workplace MAC.

- Please note that the Authenticator App cannot be used during the migration
- No further steps are required
- After the migration, the app must be reactivated; this is described in [Section 8.5 Reactivating the Microsoft Authenticator App](#)
- If you need to use the Authenticator app during the migration, use another smartphone or tablet to connect it to the Authenticator app. To do this, follow the step-by-step guide to [setting up multi-factor authentication \(MFA\)](#)

2.4 Creating a Temporary Access Pass (TAP) – Expert mode

If you only have one DB smartphone/tablet and can reset your device without assistance, create the Temporary Access Pass (TAP) before resetting it.

- > To do this, go to Chapter 6.1 Creating a Temporary Access Pass (TAP)
- Then reset your device

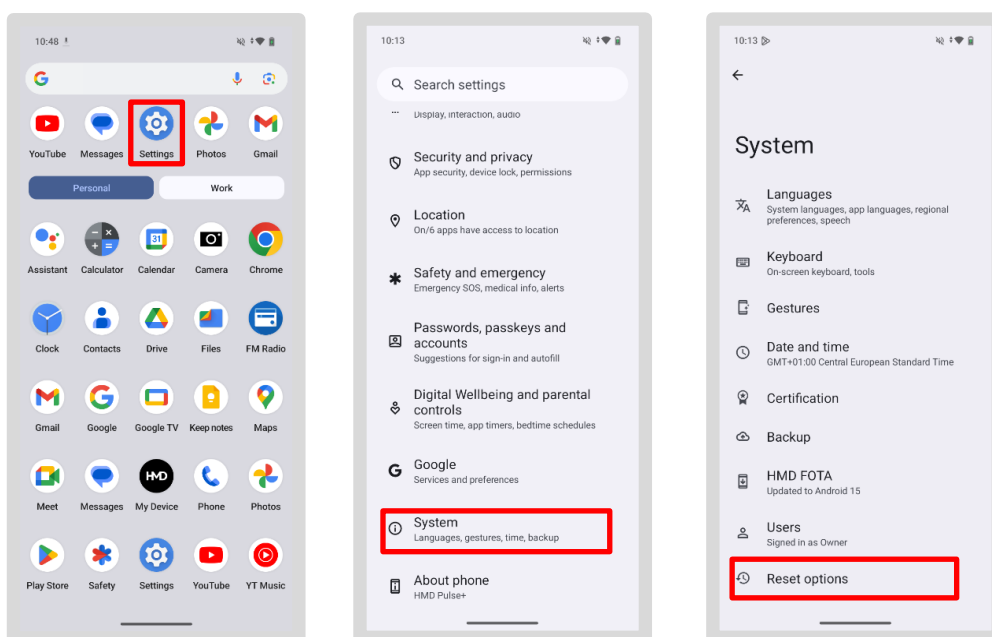
3 Start migration: Reset smartphone/tablet

Note: The screens below may look different depending on your smartphone/tablet model.

3.1 Resetting your smartphone/tablet yourself

> **Note:** You can find a video guide at db.de/mobile-videoanleitung

- Go to the “Private” section on your smartphone/tablet
- Tap the *Settings* app
- Tap “System” and then “Reset options”
- Scroll down further and tap on “Erase all data (reset to factory settings)”



- You will see a message explaining what will be deleted by the reset
 - Check that you have backed up your work data (instructions: [Backing up data](#))
 - Then tap the “Erase All Data” button, enter your screen lock (PIN or password) and tap “Erase All Data”
 - Wait a few minutes; your smartphone/tablet will reset automatically
- > Then go to [Chapter 4: Set up again](#)

3.2 Reset your smartphone/tablet via the IT ServiceDesk app

If your smartphone/tablet is no longer working, follow these steps:

- Open the IT ServiceDesk app and submit a request to reset your smartphone/tablet under 'New Service Request'
- If you are unable to open the app, please call this number:
- IT ServiceDesk Migration Hotline (Mon–Fri 7:00–18:00)
 - Internal: Tel. 9833-8699
 - External: Tel. 0361 430 8699
- IT ServiceDesk
 - Internal: Tel. 91-5555
 - External: Tel. 0361 430 8200
 - Select menu option 0 here
- IT ServiceDesk DB Cargo

Tel. 91 7777 (internal)

Tel. 00800 327 978 35 (external)

- Select menu option 0 here
- If other issues arise, consider the following in advance:
 - **Where did the problems** occur?
 - **Identify the source of the error** so we can provide you with support more quickly
 - **For certificate issues:** After registration, wait **between 5 minutes and 24 hours** until all information and certificates have been transferred to your smartphone/tablet.

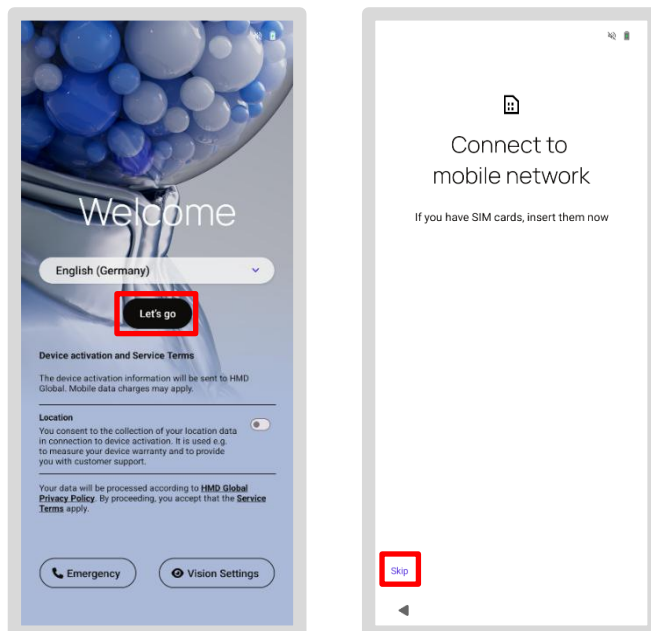
> Then go to Chapter 4: Set up again

4 Set up again

4.1 Select language

> **Note:** You can find a video guide at db.de/mobile-videoanleitung

- Hold your tablet in **portrait mode** to see the screens exactly as they appear in the guide
- Switch on your smartphone/tablet
- Make sure your smartphone/tablet is either connected to a power source or has a high battery level during the migration
- Check that the desired language is selected. If not, change it
- Then tap “*Let’s get started*”
- If a SIM card is inserted in your smartphone/tablet, follow the steps on the screen
- On the next screen, tap “*Skip*”



4.2 Set up Wi-Fi

To set up your Wi-Fi, choose one of these options:

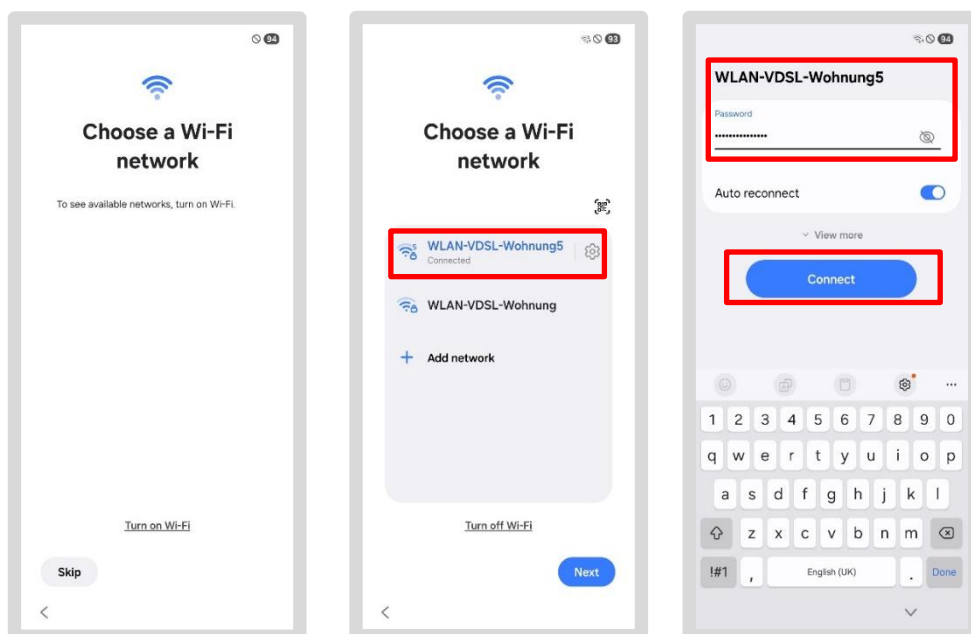
- Use your **mobile data**, provided there is a SIM card in your smartphone/tablet (this may incur charges!)
- Set up a hotspot using your personal smartphone/tablet

or

- Use a hotspot from a colleague's DB smartphone
- Use your home Wi-Fi if you're working from home

To select a different Wi-Fi network, do the following:

- Tap the Wi-Fi network you want to select
- Enter your personal login details and tap “Connect”
- If prompted a second time, tap “Continue”



Once your smartphone/tablet is connected to the Wi-Fi, the connection to the DB network will start.

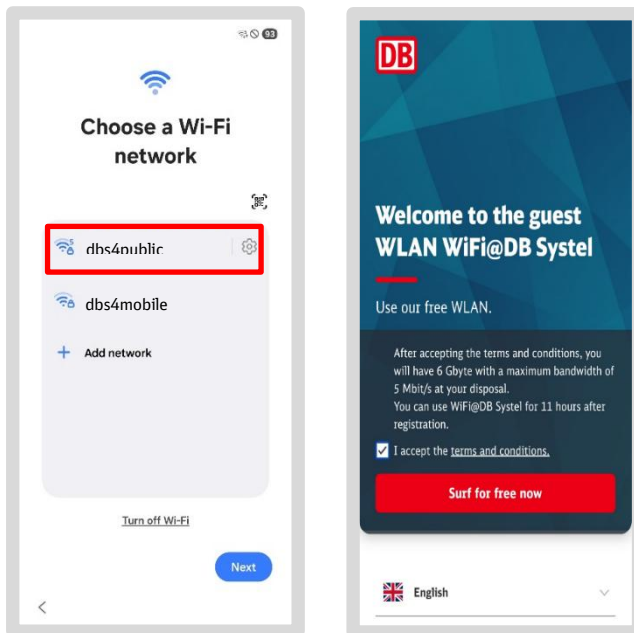
> Go to [Chapter 5: Installing Nokia/HMD](#)

4.3 Setting up Wi-Fi in DB buildings

As the “dbs4public” Wi-Fi in DB buildings does not always work satisfactorily, we recommend following one of the steps outlined in [Chapter 3.2 Setting up Wi-Fi](#).

If you are in a **DB building** and wish to use the “dbs4public” Wi-Fi, proceed as follows:

- Tap the “dbs4public” Wi-Fi network
- A dialogue box will open; accept the terms and conditions
- Tap on “Surf for free now”
- Tap on “Close”



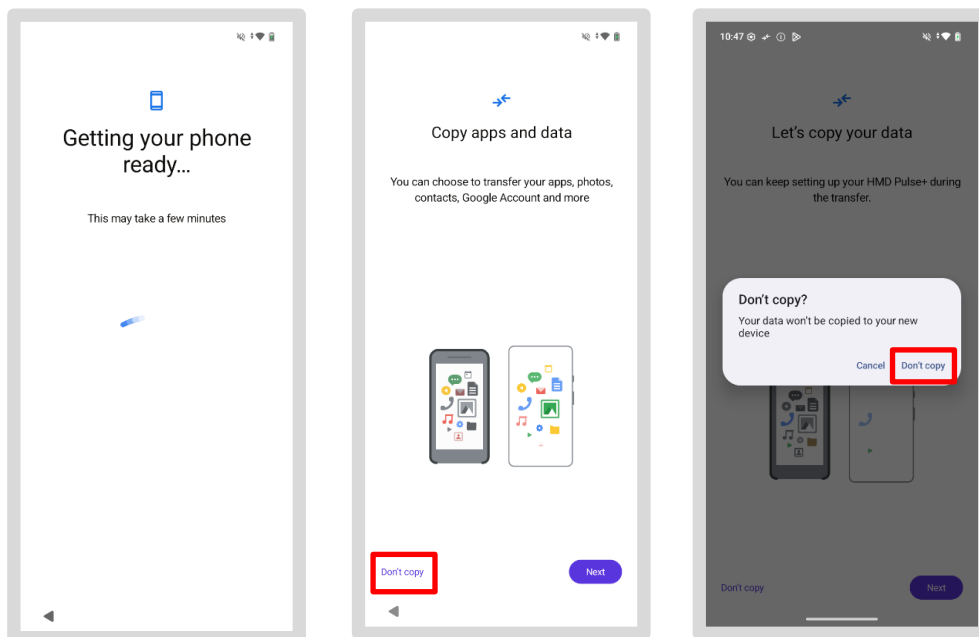
As soon as your smartphone/tablet is connected to the Wi-Fi, the connection to the DB network will start.

> Go to [Chapter 5: Installing Nokia/HMD](#)

5 Install Nokia/HMD Enterprise Mobility Management

In the next step, your DB smartphone/tablet must be reconnected to the DB network (specifically to Enterprise Mobility Management, or EMM for short). As the information changes, wait until instructions appear. Depending on your network connection, the screens may flicker or change rapidly.

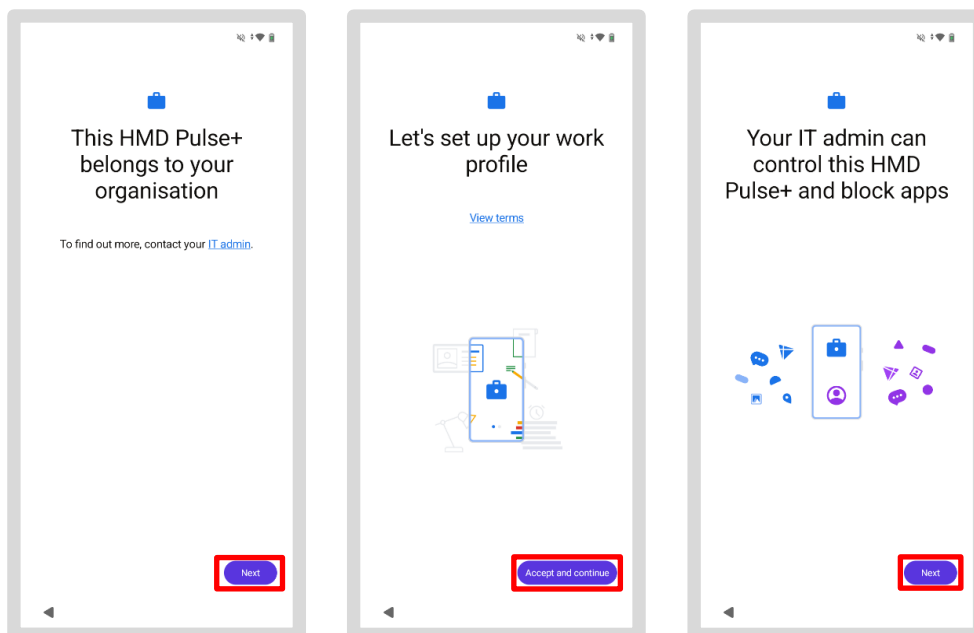
- Hold your tablet in **portrait mode** if you have been holding it in landscape mode up to this point
- Individual screens will now scroll by
- If a prompt to copy apps and data appears at this stage, first tap 'Do not copy' and, if prompted again, tap 'Do not copy' once more



5.1 Set up work profile

A work profile is required to assign work apps to your smartphone/tablet. This must be set up here:

- Your smartphone/tablet is now being set up
- Confirm the following prompt by *selecting 'Next'*
- Confirm the following screens by selecting “Accept & continue” and “Continue”

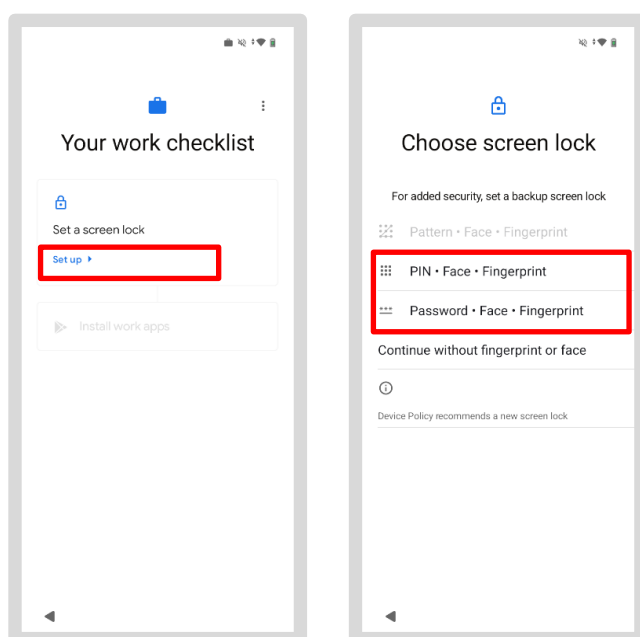


- Updating the smartphone/tablet may take a while, or in some cases quite a long time, so please be patient!
 - The required apps are being installed
- > Go to [Chapter 5.2 Set up screen lock](#)

5.2 Set up screen lock

In the next step, you will set up the screen lock for your smartphone/tablet. This is mandatory with DB for data protection reasons and reliably protects your data.

- Tap on “Set up”
- Choose the option that suits you best. Tap one of the two options (PIN or password) and then set your own personal screen lock
- Make sure the new password is a new 6-digit combination

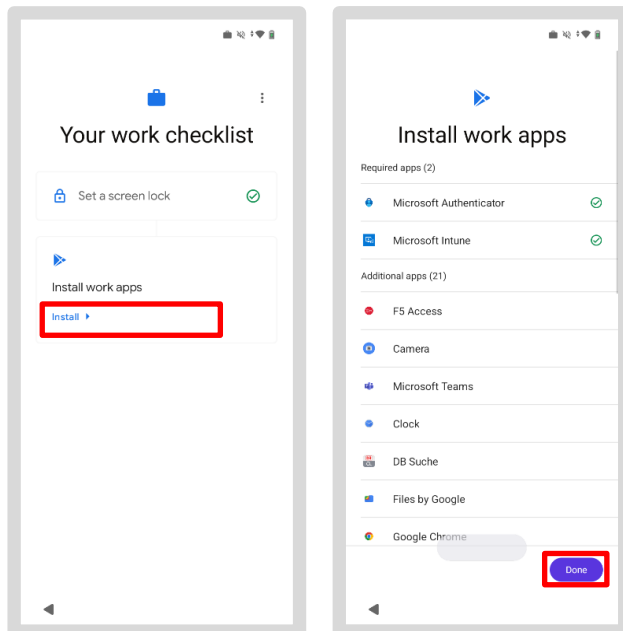


- Please note the privacy and usage information in the initial setup guide
 - Confirm by tapping “Next” and then “Confirm” after entering it twice
 - If the “Private Accounts” screen appears tap “Later” when prompted
- > Go to Chapter 5.3 Installing DB Apps

5.3 Installing DB apps

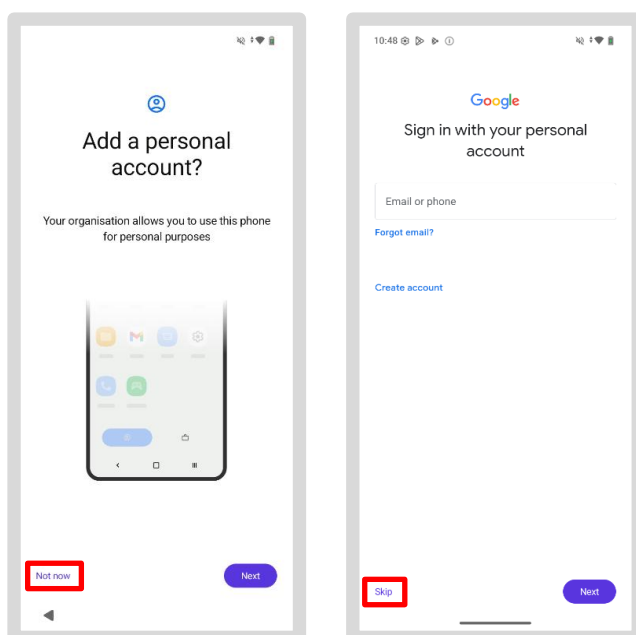
In the next step, all DB apps will be reinstalled on your DB smartphone/tablet.

- Tap “Install”
- Scroll down and tap “Done”



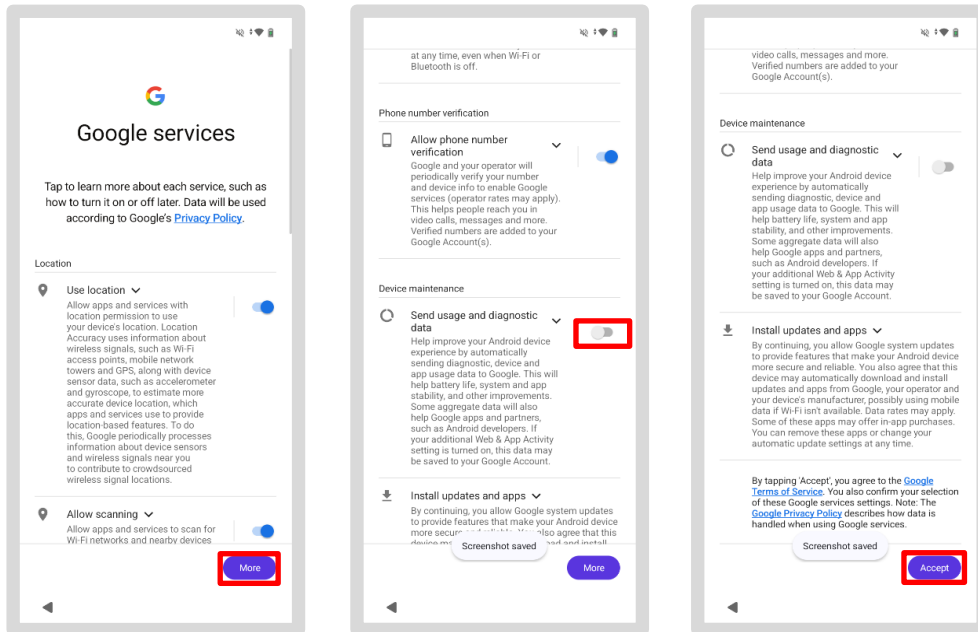
5.4 Google account – not required

- You will be asked for a personal Google account
- Tap “Later”. **No personal** Google account is required for your DB smartphone/tablet!
- You can do this later if necessary
- So, in the next step, tap “Skip”



5.5 Enable Google service

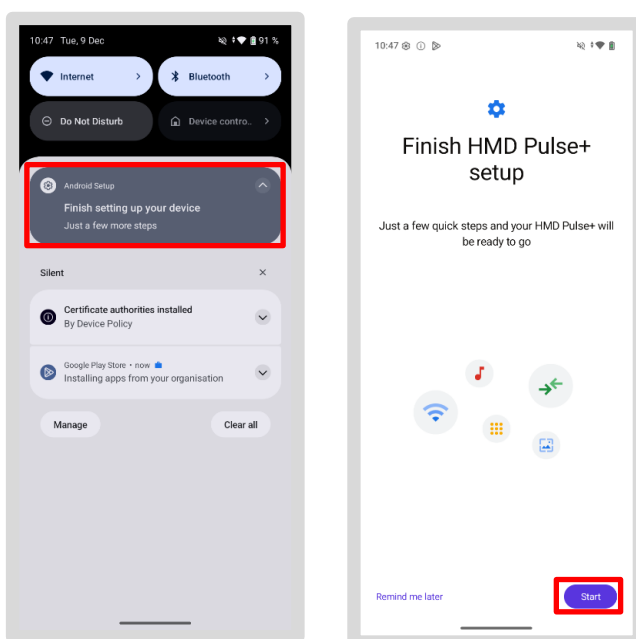
- Tap 'More' under Google Services
- Under 'Send usage and diagnostic data': Turn the feature off!
- Scroll down and then tap "Accept"



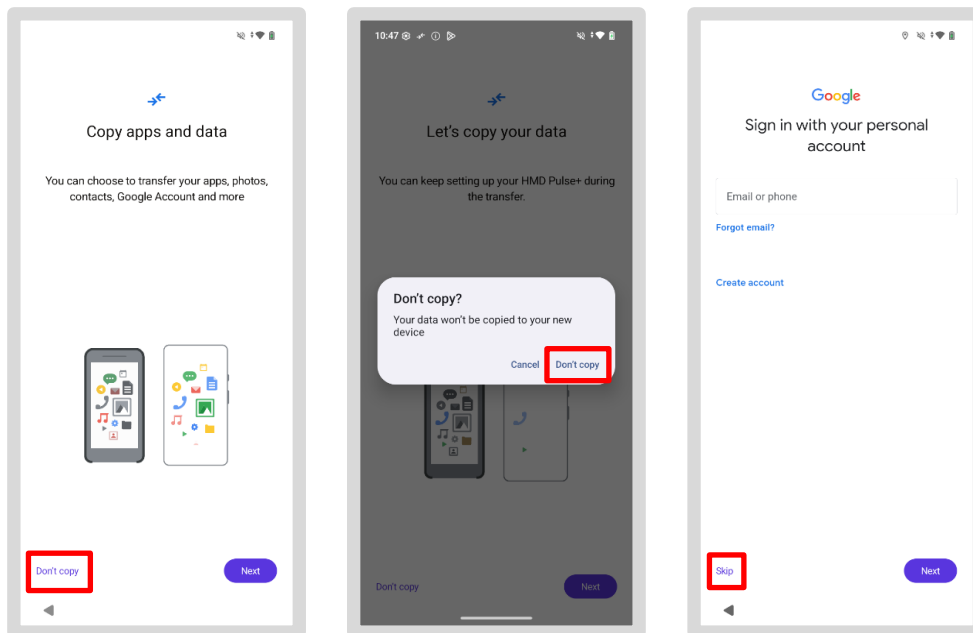
> Go to Chapter 5.6: Complete setup

5.6 Complete setup

- Swipe down on your screen and tap "Finish setup"
- Tap "Start" and wait
- When asked whether to copy apps and data, tap "Don't copy"

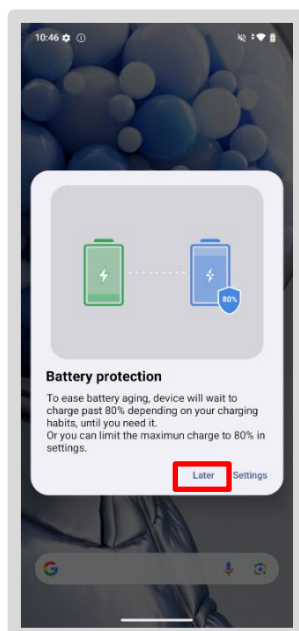


- When asked about your personal account, tap “Skip”
- You **don’t** need to log in to the DB apps with your personal account!



You will then be taken back to your home screen:

- If you are prompted to access the battery saver settings at this point, tap “Later” first
- You can adjust this setting at any time later



- Swipe down from the top to check your notifications and see if any apps are still being downloaded or installed
- Tap the notification to see how many apps still need to be installed

- Wait here for a while until all apps have been installed

Note: if your device does not behave as described or does not display the screens shown in these instructions, reset it again. To do this, go to Chapter 3 Start Migration: resetting your smartphone/tablet

Important!

Your smartphone/tablet is not yet connected to the
DB network yet!

Get the **temporary access pass (TAP)**
and enter it in the *Intune app*.

To do this, follow the step-by-step instructions in
> Chapter 6: Activate device – Create a temporary access pass (TAP)

6 Activate device – Create a temporary access pass (TAP)

To set up your smartphone/tablet on the DB network, you will need the following:

- A valid Temporary Access Pass (TAP) – db.de/tap
- your DB username and DB password
- the Intune app

For your information:

The DB User is the user account for all employees within the DB Group. It consists of a password of your choice and an automatically generated login name.

- > You can reset your **DB user password** at db.de/passwort
- > You can find instructions on how **to change your password** in [Change DB User Password](#)
- > You can find out **how to obtain your DB User** in [Prerequisite: DB User](#)
- > You can find your **DB User name** in *DeBI* at: db.de/debi

6.1 Create a temporary access pass (TAP)

- > **Note:** You can find a video guide at db.de/mobile-videoanleitung

There are several ways to create the temporary access pass (TAP):

Option 1:

You have a **second smartphone/tablet** or a BKU/Basic Workplace computer that is already logged into the DB network. In this case, stay in the current section and continue on the next page.

Option 2:

A **colleague** from the same company (such as DB Sales or DB Long-Distance) can assist you provided they have a DB smartphone/tablet (or iPhone/iPad) or a BKU/Basic Workplace computer. Go to:

- > [Chapter 6.2 Create a temporary access pass for a colleague](#)

Option 3 – Expert mode:

You **only** have a **smartphone/tablet** and were able to use it long enough to create a temporary access pass (Tap) before resetting it. Make a note of your access pass and go to:

- > [Chapter 3 Start migration: Reset smartphone/tablet](#)

Please note: Your Tap is valid for just 60 minutes and can be used on multiple smartphones/tablets!

If you still have the Welcome app installed:

- open the “Welcome App” and tap on “Help”
- Then click on “Temporary Access Pass (TAP)” to create it

If you haven’t installed the Welcome App:

- Open your default browser
- Go to db.de/tap and enter your DB username and DB password
- Select “For myself” and tap the blue button
- Now select “DB Workplace Mobile”
- You will then be shown the temporary access pass (TAP)
- This is now valid for 60 minutes and can be used on multiple smartphones/tablets

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen with the 'Register' section. It prompts the user to enter their DB user login details, showing a username field with 'Max Mustermann' and a password field. The right screenshot shows the 'Create a Temporary Access Pass (TAP) - Person selection' screen. It asks the user to choose for whom the TAP should be created, with 'For myself' selected. A blue arrow button is highlighted at the bottom right.

- Write down the temporary access pass (TAP) on a piece of paper or in a notebook

Note: You’ll need it later when setting up the **Intune app!**

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen with the instruction 'Select the product you want to set up.' It lists four options: 'DB Workplace Mobile' (highlighted with a red box and a green checkmark), 'Basic Workplace Windows', 'DB Workplace Windows', and 'DB Workplace Mac'. The right screenshot shows the 'Create a Temporary Access Pass (TAP)' screen where the user enters the generated TAP code 'y&r3%9=cg2u#'. Below the code entry field, it says 'Enter the Temporary Access Pass (TAP) to activate your DB Workplace Mobile device, following the instructions. This is valid until 3:34 p.m. and can be used several times.' At the bottom, there are two buttons: 'Start a new session' and 'To the homepage'.

Important!

The **TAP** must only be entered in the **Intune app**, even if you are asked for it in another DB app or on another device.

- Write down the Temporary Access Pass (TAP) on a piece of paper or in a notebook
- You will need it later when setting up and activating the device in the Intune app
- You can now activate your smartphone/tablet in the Intune app

> Go straight to Chapter 7: Activate device in the DB

Important!

Your smartphone/tablet is not yet connected to the DB network!

Enter the **temporary access pass (TAP)** in the *Intune app*.

To do this, follow the step-by-step instructions in

> Chapter 7: Activate device in the DB

6.2 Create a temporary access pass for a colleague

To create a TAP for a colleague, follow these instructions:

If you still have the Welcome app installed:

- Open the Welcome App and tap on 'Help'
- Then click on "Temporary Access Pass (TAP)" to create it

If you have a DB Workplace Windows or Mac:

- Open your default browser
- Go to db.de/tap and enter your DB username and DB password
- Enter your DB username and DB password
- Select "For another DB employee" and click the blue button

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' page. It includes a header with the DB logo and a menu icon. The main heading is 'Create a Temporary Access Pass (TAP)'. Below it, a sub-heading reads 'This self-service allows you to create a temporary access pass (TAP) to set up a DB Workplace or Basic Workplace device.' A section titled 'The TAP can be created for:' lists two options: 'yourself' and 'an employee from the same company (see EVI)'. A 'Register' section follows, asking for 'DB user login details'. A red box highlights the input fields for 'DB User Anmeldename' (containing 'Max Mustermann') and 'DB User Password'. A link 'How can I log in to other environments?' is visible below. At the bottom are back and forward navigation buttons.

The right screenshot shows the 'Create a Temporary Access Pass (TAP) - Person selection' page. It has a similar header. The main heading is 'Create a Temporary Access Pass (TAP) - Person selection'. Below it, a sub-heading reads 'Choose for whom the TAP should be created:'. Two radio buttons are present: 'For myself' and 'For another DB employee' (which is selected). A red box highlights the search results for 'Max Mustermann', showing fields for 'DB User: Name', 'E-mail', 'Department', and 'Company: DB Systel GmbH'. Below the search results is a checkbox 'I confirm that I have established the employee's identity.' which is checked. At the bottom are back and forward navigation buttons.

- Select the correct person and confirm their identity
- Hand over control in *Teams* to the colleague(s) (if working remotely via *Teams*)

or

- Let the colleague use the computer
- The DB colleague enters the DB user password
- The access pass will then be displayed; **it is valid for 60 minutes and can be used on multiple smartphones/tablets**
- Take back screen control if you were using *Teams*
- Write down the temporary access pass on a piece of paper or in a notebook

Issue a Temporary Access Pass (TAP) for Lisa Mustermann

The TAP recipient must now sign in.

Sign in

DB user login name
Lisa Mustermann

DB user password

Important note for recipients: Sign in personally with your DB user credentials. Never share this information with anyone else.

← →

Create a Temporary Access Pass (TAP)

y&r3%9=c g2u#

Enter the Temporary Access Pass (TAP) to activate your DB Workplace Mobile device, following the instructions. This is valid until **3:34 p.m.** and can be used **several times**.

Start a new session To the homepage

- You'll need it later to set up and activate the device in the Intune app
 - The colleague can now activate their smartphone/tablet in the Intune app
- > Go straight to [Chapter 7: Activate device in the DB](#)

Important!

Your smartphone/tablet is not yet connected to the DB network yet!
Enter the **temporary access pass (TAP)** in the *Intune app*.

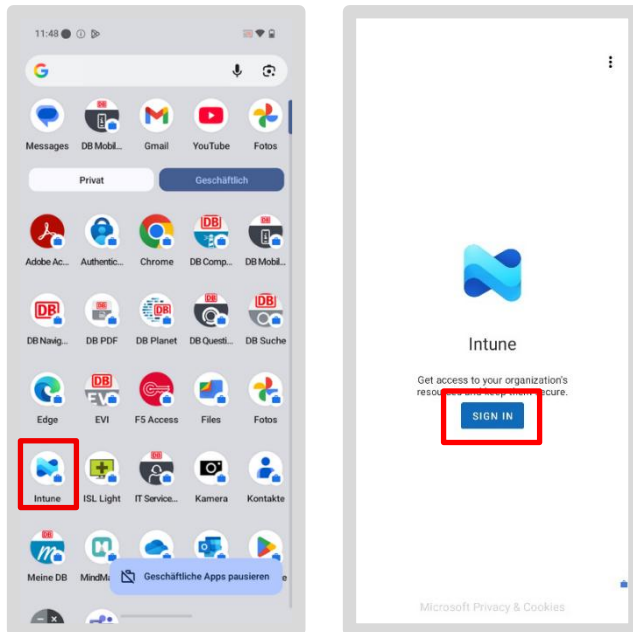
To do this, follow the step-by-step instructions in
> [Chapter 7: Activate device in the DB](#)

7 Activate the device in the DB

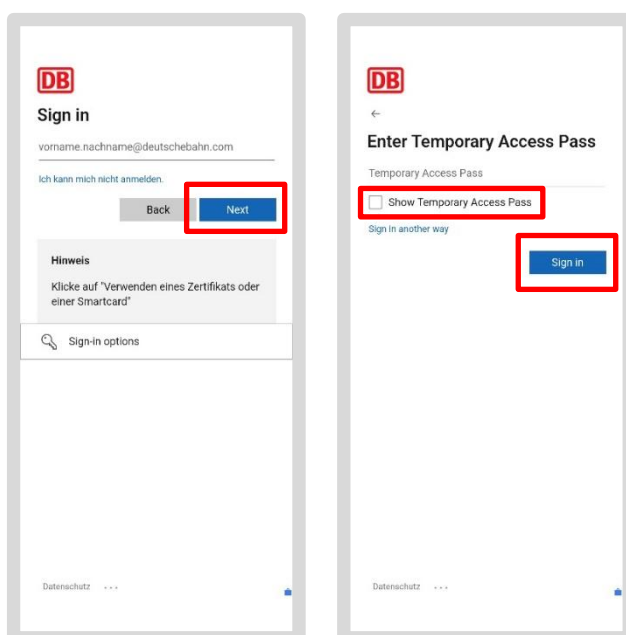
> **Please note:** Check whether you have created and received a temporary access pass (TAP) as described in Chapter 6, 'Creating a temporary access pass (TAP)'!

> **Note:** You can find a video tutorial at db.de/mobile-videoanleitung

- Open the “Intune” app 
- Then tap the “Log in” button



- Enter your **DB user email address** (not: DB User) and tap “Continue”
- **Tip:** Tick the box next to “Show temporary access pass”
- Enter your temporary access pass and tap “Log in”



If you receive an error message:

- Create a new temporary access pass and repeat the login process as described in [Chapter 6: Activate device – Create temporary access pass \(TAP\)](#)
- > Otherwise, go to [Chapter 7.1 Setting up access to all DB apps and websites](#)

Note: As long as the temporary access pass (TAP) is valid (within 60 minutes) and you open, for example, Outlook, Teams or the IT ServiceDesk app, you will be asked for the temporary access pass; enter the temporary access pass you have noted down here as well.

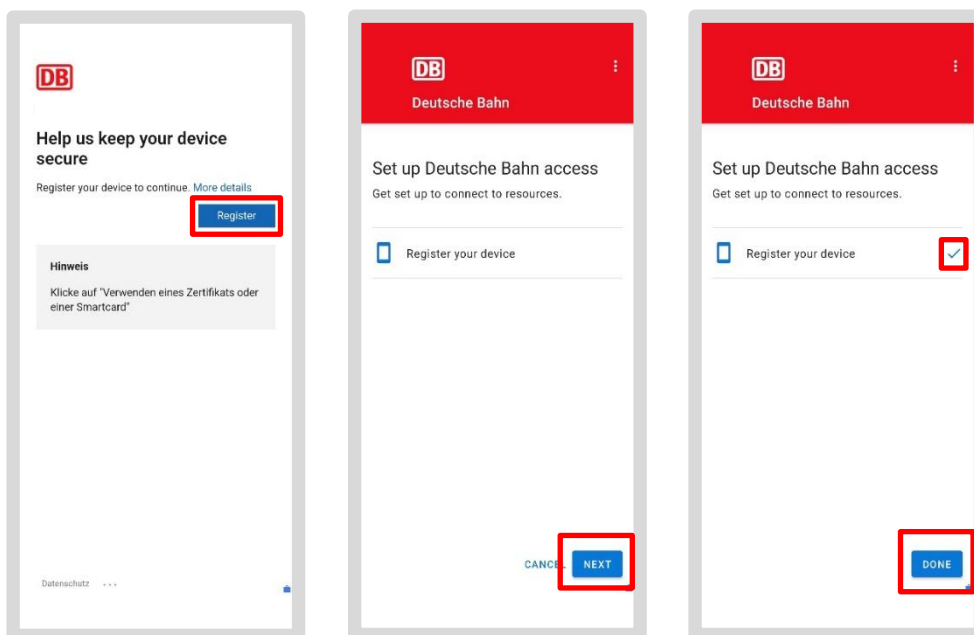
7.1 Set up access to all DB apps and websites

Access to the DB network is now being set up:

- Tap 'Register' and then 'Next'
- When the tick appears next to "Register device", tap the "Done" button

Note: If the "Done" button does not appear, activation is not complete

- Open the Intune app again and go through the steps from [Chapter 6, 'Activate device with the temporary access pass \(TAP\)'](#), step by step



Note:

After registration, wait between 5 minutes and 1 hour

until all information and certificates have been transferred to your smartphone/tablet. You can then use your apps such as *Outlook*, *Teams*, etc.

7.2 DB Apps

Please note: The provision of certificates can take **between 5 minutes and 24 hours**. Only then can you use your apps such as Outlook, Teams, etc.

Once setup is complete, the DB apps, such as the Outlook app or Teams app, will download automatically.

Your company-specific or business-unit-specific apps will then be downloaded.

You can download further DB apps from the work Google Play Store (the app with the suitcase icon) in the 'Work' section.

The **Welcome app** is **no longer** available on the DB smartphone/tablet; instead, there is the **DB Mobile Info app**, which contains all the information, useful links and data relating to your DB smartphone/tablet.

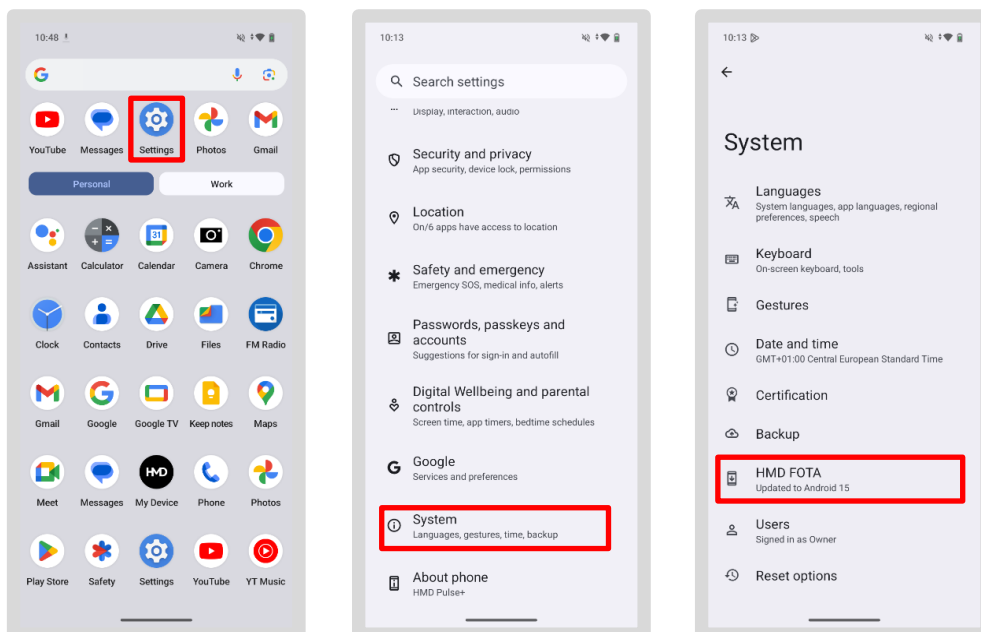
8 Required settings

Please note: It may take **between 5 minutes and 24 hours** for the certificates to be issued. Only then will you be able to use your apps such as Outlook, Teams, etc.

8.1 Check for operating system updates

On your smartphone/tablet, go to the “Personal”/“Private” section

- Tap the “Settings” app
- Then scroll down and select “System”
- Now tap on “HMD FOTA”
- It will show whether an update is available and what type
- Install any pending updates by tapping “Install update”

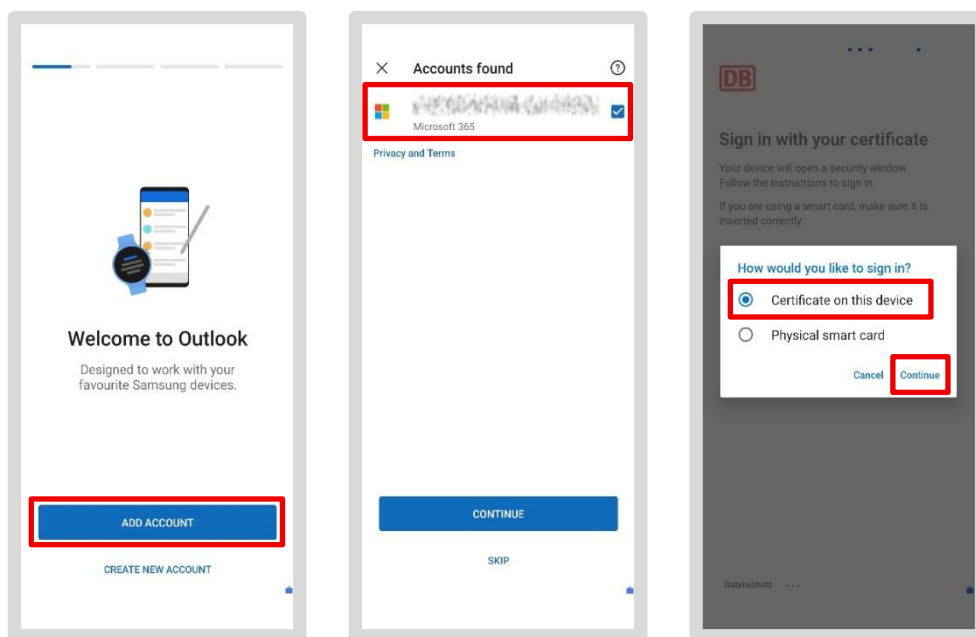


8.2 Outlook

8.2.1 Set up Outlook /Create an email account/Set up email encryption

> **Note:** You can find a video guide at db.de/mobile-videoanleitung

- Go to your “Work/Business” section and tap on the “Outlook” app
- Your email account should already be set up automatically – if not, tap “Add account”
- In the next step, select your email address and tap “Next”



When prompted to log in, you may be asked for a TAP:

- If your temporary access pass is still valid, enter it here or create a new one as described in [section 6.1 Creating a temporary access pass \(TAP\)](#)
- Alternatively: under “Select other login option”, select the option “Certificate on this device”
- Tap “Select” when prompted for the certificate

If you wish to send data requiring special protection (e.g. personal data) by email, you must also encrypt the content of the email

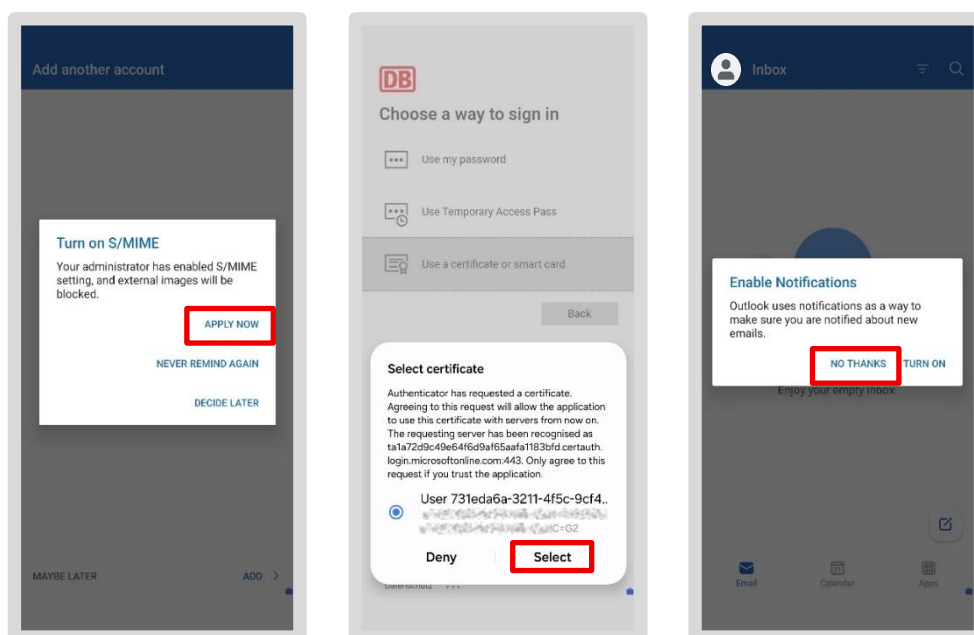
- DB provides S/MIME encryption for this purpose
- Tap “Apply now” when asked if you wish to activate S/MIME

This is followed by the certificate prompt. You can identify the certificate valid for you as follows:

- First line: **"User ds2232..."** (followed by numbers and letters)"
- Second line: **"CN-DB user name"**, e.g. LisaMustermann 89sd7es0ßwd (followed by numbers and letters)
- Select the text snippet and tap "Select"

Your email account is now being set up:

- Tap *"Maybe later"* when asked if you want to add another account
- And tap *"No thanks"* to disable notifications



- Your emails are now being loaded (this process may take a few minutes)
- You can then read and write emails again

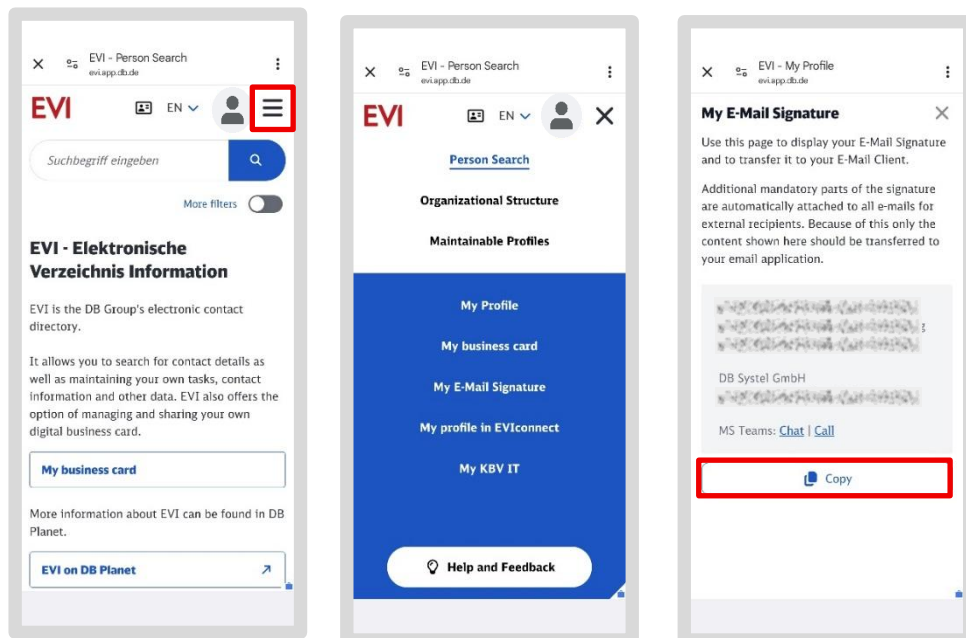
Android 16: On devices running Android 16, the step to enable S/MIME may be skipped. In this case, you must complete the Outlook setup and restart the app! The prompt to enable S/MIME will then appear.

8.2.2 Set up an email signature

An email signature is a mandatory part of business communication. It appears at the end of an email and, by law, must contain certain information, such as the company name and the official registered office of your DB company. You can find the text for your email signature in DB's central directory, known as the 'EVI'.

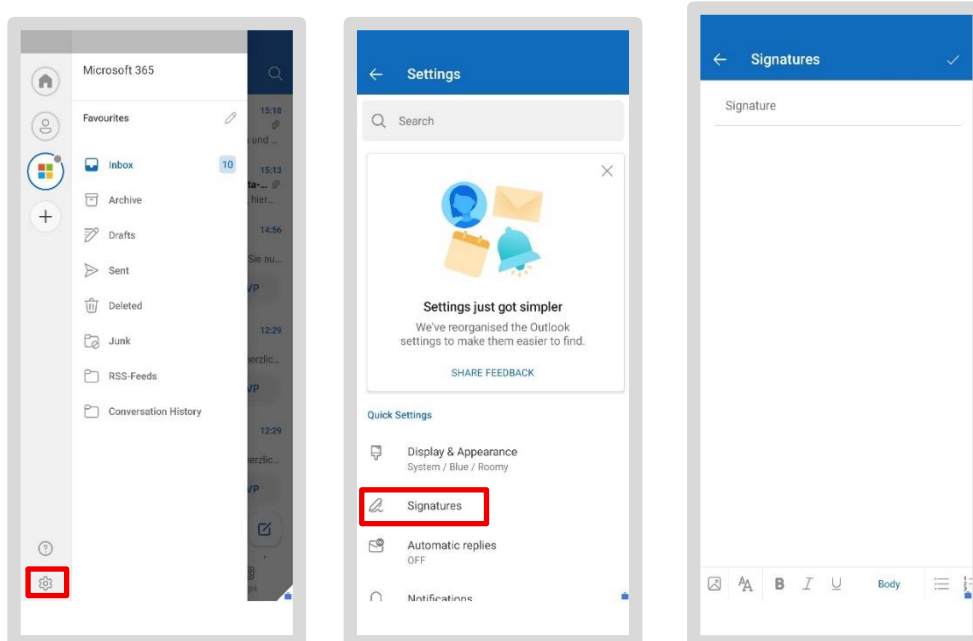
Here's how to get your email signature from EVI:

- Open the *EVI* app
- Tap the three lines in the top right-hand corner next to your profile picture
- Then tap on “*My email signature*”
- Your personal signature is displayed in the grey box. Copy it by tapping on “*Copy*”



Paste the signature into Outlook:

- Open the *Outlook* app and tap your profile picture in the top left
- Tap the cog icon in the bottom left
- Now tap on “*Signature*”



- A field for the signature will open. If there is already an entry there, delete it by tapping “✕”
- Now long-press the field until the “Paste” option appears and tap it
- Your copied signature from EVI will be inserted

Close the window – your signature will now be automatically inserted into all new emails

Note: If you have set up multiple email accounts, you can use the “*Signature per account*” slider to set up a separate signature for each account. Otherwise, the saved signature will be used for all your email accounts.

8.2.3 Email synchronisation – All emails always up to date

All your emails are automatically backed up in the *Outlook app* and synchronised with your linked Office account. This means that no matter which iPhone/iPad, or whether you log in via an iPhone/iPad or a BKU computer/Basic Workplace computer, you are always up to date.

8.3 MS Defender app – must be opened

After activating Outlook and Teams, activate the “*Microsoft Defender for Endpoint Mobile*” app (MS Defender app for short) on your smartphone/tablet. The app protects against cyber attacks and scans existing apps for malicious software. To activate the protection, open the app once.

Due to the wide variety of different DB smartphones/tablets, there may be minor differences in the description for individual steps.

8.3.1 Setting up the MS Defender app

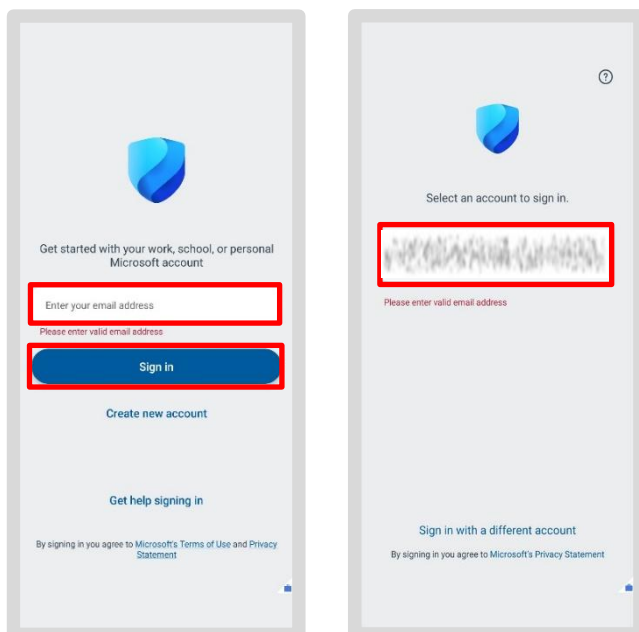
To set up the MS Defender app on your smartphone/tablet, you must follow these steps:

- Go to the Work/Business section and open the “DB Google Play Store”
- Search for the app “Microsoft Defender: Antivirus” and tap “Install”

- Tap the *MS Defender app* icon to open the app

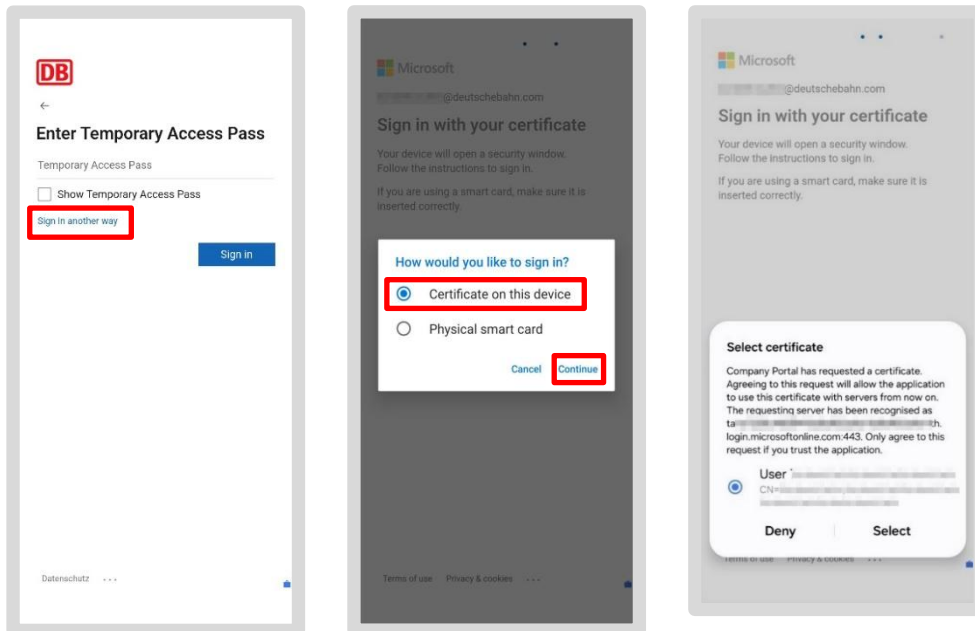


- You will be asked for your work email address
- Tap the “Sign in” button or the app will automatically take you to the next screen, where your email address will be displayed
- Tap your work email address



If you have activated your smartphone/tablet with the Intune app within the last hour, you may be asked here to enter your temporary access pass again.

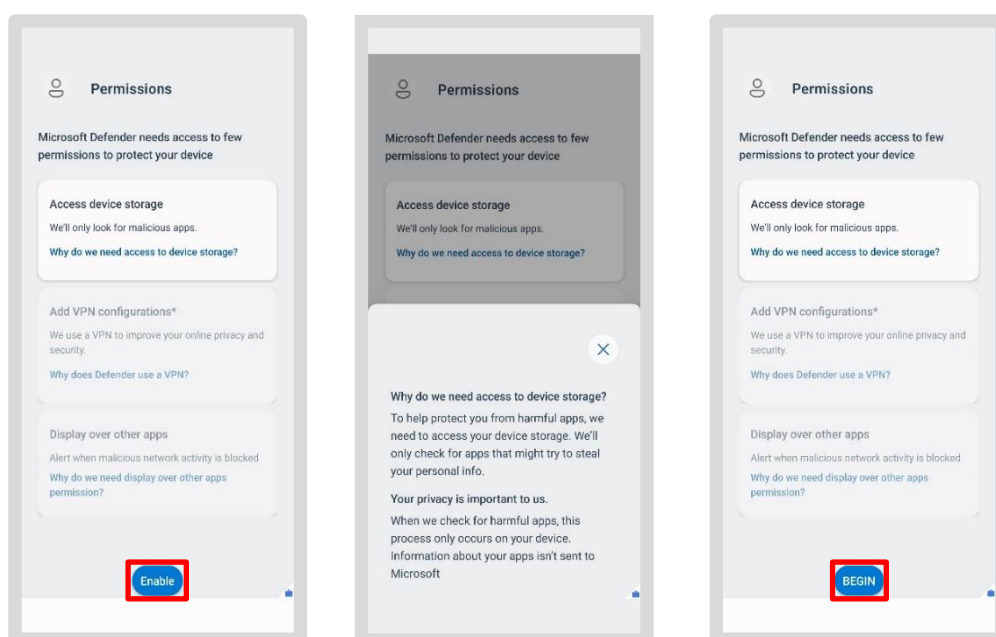
- Tap ‘Sign in another way’
- When prompted, tap “*Certificate on this device*” and then tap “Continue”
- Select the certificate



8.3.2 Grant permissions

The app will now ask you for the necessary permissions. At this point, the screens may appear in a different order to the instructions. If your first screen matches the one shown:

- Tap “Activate”
- Then tap “Start”
- The *Settings* app on your smartphone/tablet will open

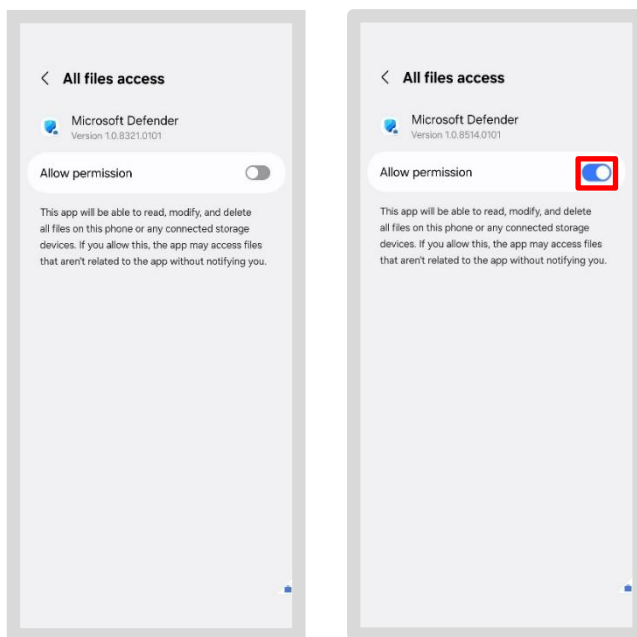


Background information on permissions:

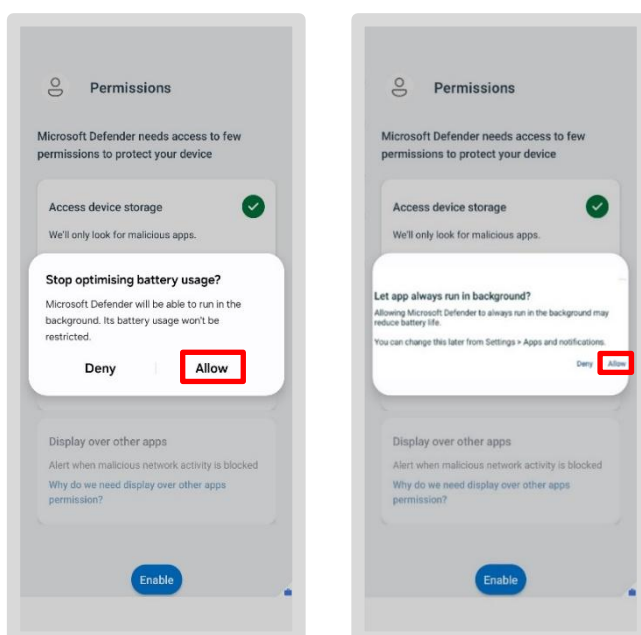
These permissions are required to ensure the app works properly and to guarantee security on your device.

You can view an information window for each individual permission (e.g. by tapping “Why do we need access to the device storage?”). However, some items cannot be selected (they are greyed out, e.g. “Add VPN configuration”) or are already enabled (green tick, e.g. “Run in the background”), as these are system-defined.

- Now slide the slider to the right to grant the permission
- Tap “Allow” when prompted



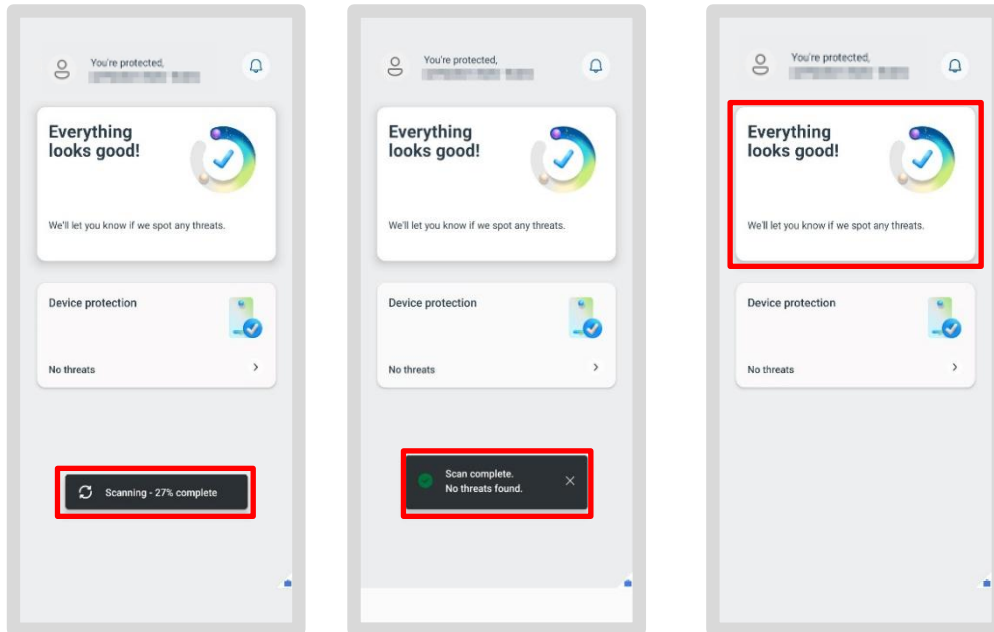
- Tap “Allow” for all subsequent prompts



Note: Depending on your device type, you may be asked for different permissions! As a result, you may only see one of the prompts shown.

You will then be taken to the MS Defender app's home screen. A scan for malware on your smartphone/tablet will be carried out automatically straight away. Progress updates will be displayed during the scan.

The result is displayed in writing on the home screen. If a green tick is visible, no malware has been detected.



You have successfully completed the initial setup! The device is now protected against malware.

8.4 DB M 365

You can also open and read Word, Excel, PowerPoint or PDF files on your smartphone or tablet. To do this, simply download the relevant apps once:

- Open the Google Play Store
- Search for the relevant app using the search bar, for example Word, Excel, PowerPoint or the PDF Reader



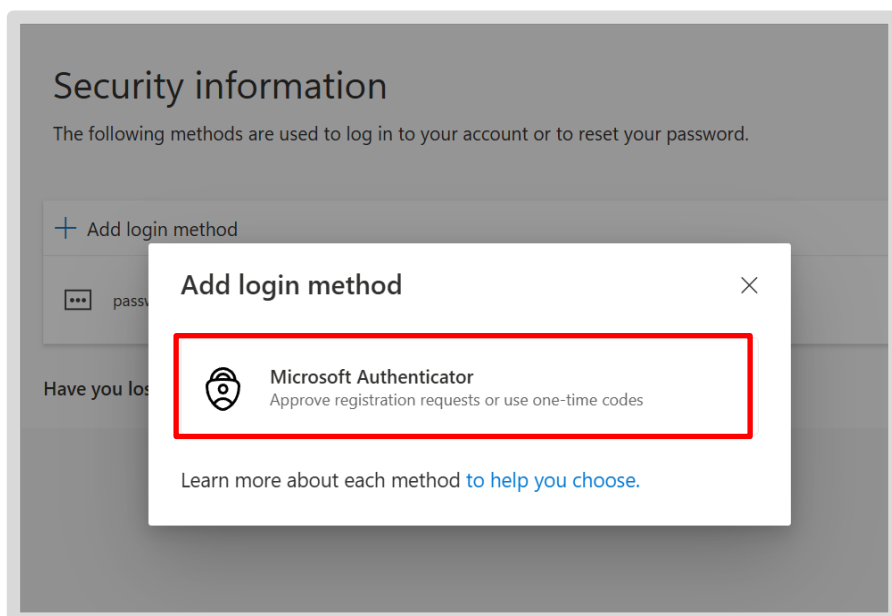
- Then tap on “Install”. The app will now be downloaded and will appear in your “Work/Business” section
- When you open a file, the app will open automatically

Please note: You can only open one file at a time. It is not possible, for example, to open several Word files simultaneously.

8.5 Reactivating the Microsoft Authenticator app

If you have used the Authenticator app, proceed as follows:

- Tap db.de/authenticator on your BKU or Basic Workplace computer
- Tap the ‘plus icon’ and the ‘Add login method’ button
- A dialogue box will open; select “Microsoft Authenticator”



- Switch to your smartphone/tablet and open the Microsoft Authenticator app
- Open this page for [step-by-step instructions](#), tap the “MFA setup guide” button and follow the steps provided
- You can then use the Microsoft Authenticator app for authentication on your smartphone/tablet
- If you have used the **Authenticator app for websites or tools**, re-enable the app on those websites

Tip: If you have difficulty reactivating the connections in the Authenticator app after recovery, use the self-service option: “Reset Microsoft Authenticator app (MFA)”: db.de/resetmfa and then follow the steps.

Congratulations!

You have successfully migrated your work smartphone/tablet!

You can find more information about your smartphone/tablet in the app: DB Mobile Info.

- > You can find out how to save your contacts to OneDrive and import them back in the setup guide under [‘Back up contacts to OneDrive’](#)
- > You can find a detailed setup guide at db.de/mobile-setup