DB Systel

Operating system version: Android 15 or later

Initial setup for Samsung/ Nokia/HMD

DB Workplace Mobile

DB Systel GmbH | 15 August 2026

Table of contents

1 Essential app: DB Mobile Info app **5**

2 Unpacking your smartphone/tablet **6**

2.1 Two ways to receive your smartphone/tablet 6

2.2 Have you ordered your new smartphone/tablet yourself and received it now? 6

2.3 Checking the contents of the package 6

2.4 Quick guide to setting up your smartphone/tablet 6

3 Prerequisite: DB User **7**

3.1 You've been with the Group for some time and already have a DB User account 7

3.2 New to the Group; required account: DB User 7

4 Initial set-up for Samsung/HMD **8**

4.1 Inserting the SIM card 8

4.2 SIM PIN 8

4.3 Setting up a screen lock 8

4.4 Setting up Wi-Fi 9

4.5 Setting up Wi-Fi in the DB building 10

4.6 Activating the device – Creating a temporary access pass (TAP) 11

4.6.1 Create a Temporary Access Pass (TAP) 11

4.6.2 Creating a temporary access pass for a colleague 14

4.7 Activating a device using the temporary access pass (TAP) 16

4.8 Setting up access to all DB apps and websites 17

4.9 DB Apps 18

4.10 Change screen lock 18

4.11 Take-Off: 'Log in on a smartphone/tablet' 19

4.12 Notes on switching on the device each day 20

5 Work-related and personal content **21**

5.1 Distinguishing between work and personal content 21

5.2 Downloading DB apps 22

5.3 Managing items on the home screen 22

5.4 Take-Off: Separating personal and work content + grouping apps 22

6 Further settings **23**

6.1 Installing Android operating system updates 23

6.2 Quick Access/Control Centre 23

6.3 Connecting to the internet 25
6.3.1 DB Wi-Fi 25
6.3.2 Public Wi-Fi 25
6.3.3 Via mobile data – your data allowance 25
6.3.4 Your Vodafone contract – Elfe (electronic telecoms bill) 25
6.3.5 Disabling the data warning 25
6.3.6 Offline mode (Airplane mode) 28
6.4 F5 Access – Setting up a VPN connection 28
6.4.1 Set up the VPN connection 28
6.5 Take-Off: Certificates & VPN connection 30
6.6 Improving battery life 30
6.7 Disable Advertising ID 31

7 The most important apps to get you started 32
7.1 Download new DB apps 32
7.2 The DB Mobile Info app 32
7.2.1 Push notifications 33
7.2.2 Scanning QR codes 33
7.3 Outlook 34
7.3.1 Setting up Outlook / Creating an email account / Setting up email encryption 34
7.3.2 Setting up an email signature 36
7.3.3 Email synchronisation – All emails always up to date 38
7.3.4 Creating new contacts in Outlook 38
7.3.5 Synchronising contacts in Outlook 38
7.4 MS Defender app – Must be opened 39
7.4.1 Setting up the MS Defender app 39
7.4.2 Assigning permissions 41
7.5 DB M 365 43
7.6 Microsoft Authenticator app 44
7.7 Take-away: DB Apps 45

8 Backing up data 46
8.1 Backing up work data to OneDrive 46
8.2 Setting up OneDrive 46
8.2.1 Android 15 47
8.2.2 Android 16 48
8.3 Backing up photos 49

8.4 Backing up PDF files 51
8.4.1 Backing up PDF files directly to OneDrive 52
8.5 Backing up contacts to OneDrive 53
8.6 Importing contacts from OneDrive 54
8.7 Backing up contacts via Outlook 56
8.8 Backing up passwords 56
8.9 Backing up personal data 56
8.10 Getting started: Where are your photos, files and documents? 57

9 Data protection and terms of use 59
9.1 Take-Off: Security considerations 61

10 Forgotten your password, returning your device 62
10.1 Forgotten or changing your DB User password 62
10.2 Help via the IT ServiceDesk app 64
10.3 Lost your smartphone or tablet? 65
10.4 Faulty smartphone/tablet 66
10.5 Returning a smartphone or tablet? 66

1 Important app: DB Mobile Info app

This guide explains how to set up your smartphone or tablet. It also provides an overview of all topics relating to your DB smartphone or tablet.

The most important app for the initial set-up is the **DB Mobile Info app!**

There you'll find all the important information about your smartphone/tablet, such as:

- Guides on setting up and restoring your smartphone/tablet
- Useful links for working in the DB world
- You'll receive notifications here whenever there's something important relating to your device

So do have a look and keep up to date!

Note: If your smartphone or tablet hasn't been set up yet, the *DB Mobile Info* app is already installed on your device!

2 Unpack your smartphone or tablet

2.1 Two ways to receive your smartphone/tablet

There are two ways you can receive your smartphone or tablet:

- By placing an order in the digital shop

> Go to section 2.2 Have you ordered your new smartphone/tablet yourself and received it now?

- Or have you received a device via your cost centre or mobile phone administrator?

> Go to section 2.3 Checking the contents of the delivery

2.2 Have you ordered your new smartphone or tablet yourself and now received it?

First, check that your name is on the parcel and that you have received the correct one. Compare it with your order. If the details do not match, ask your cost centre or mobile phone administrator.

> Then proceed to Section 2.3: Checking the contents of the delivery

2.3 Checking the contents of the delivery

If you've received your smartphone/tablet from your cost centre or mobile phone administrator, or via an order placed through the Digitalshop, start with these steps:

Is everything there?

- Smartphone or tablet
- Instruction manual, handover document, terms of use and the tool for inserting the SIM card

If ordered:

- Accessories such as a charging cable, protective case and power bank
- SIM card letter (sent by Vodafone – ask your mobile phone administrator here)

2.4 Quick guide to setting up your smartphone/tablet

You'll receive a printed leaflet along with your smartphone/tablet.

If you'd rather not go through the long setup guide, use the leaflet:

> You can also find the leaflet online at: Quick Guides

> All information about setting up: db.de/mobile-setup

> All information on resetting or restoring your smartphone or tablet: db.de/mobile-restore

3 Prerequisite: DB user

If you don't know what a DB user is, or if you're not sure whether you have a DB user, please continue reading this chapter.

3.1 Long-standing member of the group and already have a DB user

> If you already have a DB User, proceed to Chapter 4: Initial setup for Samsung/HMD

3.2 New to the Group, required account: DB User

Are you new to the DB Group? If so, you'll need a *DB User* to set up your smartphone or tablet. The *DB User* gives you access to many Group applications.

What is the DB User?

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.

To use it, you must first have been issued with a *DB User account* (created by your HR department).

How do I activate my DB User account?

The *DB User* is activated once, **together with a sponsor**. During this process, you set your *DB User password*. You can find out how this works and who your sponsor is here:

> https://db-planet.deutschebahn.com/pages/db-user/apps/content/konto-aktivierung

Once activation is complete, you'll receive a PDF document containing your own *DB User login name*.

How do I change my DB User password?

> If you have forgotten your password, you can change it via the Password Self-Service

> Or follow the instructions in Chapter 10.1: Forgotten or changing your DB User password

4 Initial setup for Samsung/HMD

4.1 Inserting the SIM card

There is a small compartment on the top or bottom of your smartphone/tablet.

- Open the tray using the tool. You'll find it in your device's packaging
- Pull out the card holder and insert the SIM card
- Reinsert the card holder into the smartphone/tablet

4.2 SIM PIN

Connect your smartphone/tablet to the mains using the charger.

- Press the 'Power' button
- Once the device has booted up, it will ask you for a PIN
- This is the PIN for the SIM card you have inserted

You can obtain the PIN as follows:

- Open your SIM card letter from Vodafone
- Peel off the film. Underneath, you'll find a PIN and a Super-PIN
- Enter the PIN into the input field on your smartphone or tablet and confirm by tapping 'OK'

4.3 Set up a screen lock

Next, unlock your device:

- Swipe your finger across the screen once
- You will now be asked for a 'password'
- Now enter the following password: **DB-Device2019**
- Tap 'OK'
- You can change the screen lock now or later

> To do this, go to section 4.11, Change screen lock

4.4 Set up Wi-Fi

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

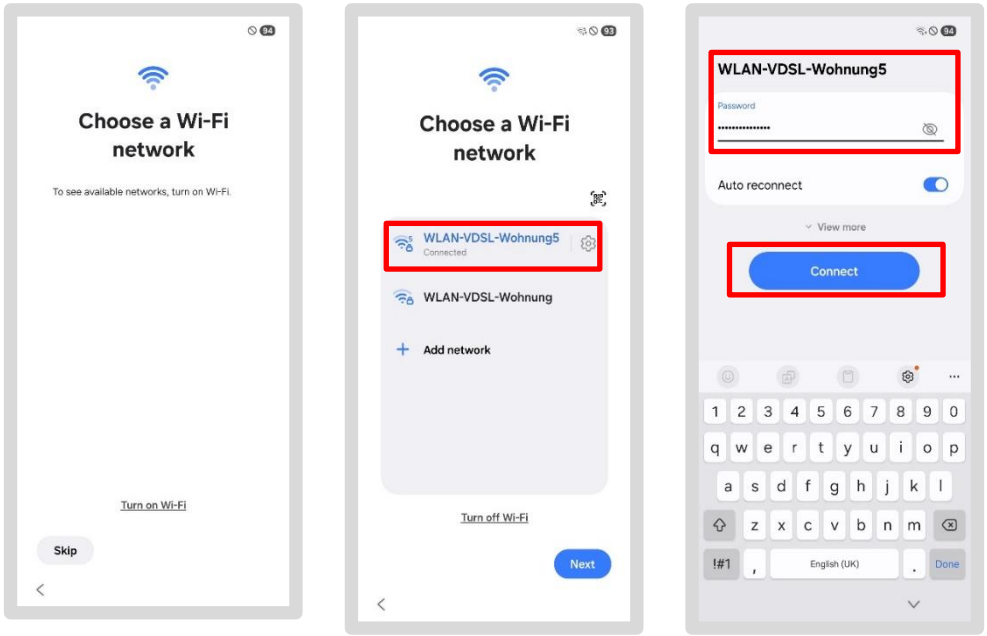
- Use your mobile data, provided you have a SIM card in your smartphone/tablet (this may incur charges!)
- Set up a hotspot using your personal smartphone or tablet

Or

- Use a hotspot from a colleague's DB smartphone or tablet
- For Samsung smartphones/tablets: Use the 'dbs4mobile' Wi-Fi network if you have booked this service (see: https://dbquestions.extranet.deutschebahn.com/question/27780)
- Use your own Wi-Fi if you're working from home

To select a different Wi-Fi network, proceed as follows:

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



As soon as your smartphone or tablet is connected to the Wi-Fi network, the connection to the DB network will be established.

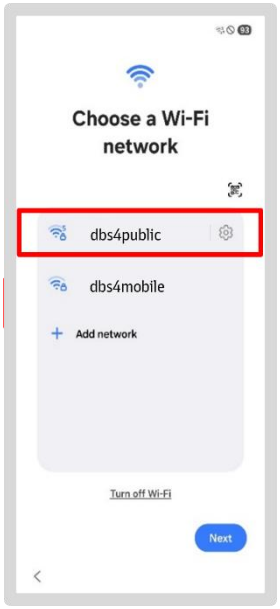
> Go to Section 4.6 Activate device: create a temporary access pass (TAP)

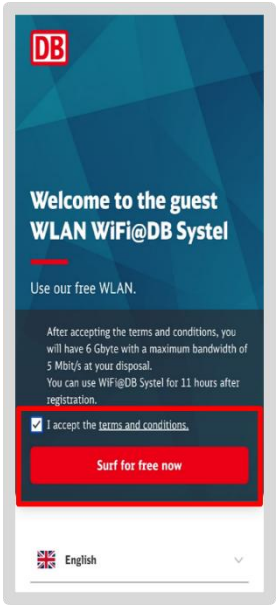
4.5 Setting up Wi-Fi in DB buildings

As the ‘dbs4public’ Wi-Fi does not always work satisfactorily in DB buildings, we recommend following one of the steps outlined in section 4.4, ‘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 *‘Surf for free now’*
- Then tap *“Close”* or wait until the window closes





As soon as your smartphone or tablet is connected to the Wi-Fi, the connection to the DB network will be established.

> Go to Section 4.6 Activate device: create a temporary access pass (TAP)

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

To set up your smartphone/tablet on the DB network, you'll 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 username.

> If you **have forgotten** your **DB User password,** you can reset it at db.de/passwort
. Alternatively, open the *DB Mobile Info* app on your old DB smartphone or tablet, select the 'Service' tab and tap on the 'Reset DB User password' option

> To **change** your **password**, go to Section 10.1 Forgotten or changing your DB User password

> You can find out **how to obtain your DB User** in Chapter 3, Prerequisite: DB User

> You can find your **DB username** in DeBI at: db.de/debi

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

4.6.1 Create a temporary access pass (TAP)

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

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

Option 1:

You have **a second smartphone/tablet** or a DB Workplace Windows or Mac device that is logged into the DB network. In this case, stay in this section and continue the next page.

Option 2:

A colleague from the same organisation (such as DB Sales or DB Long-Distance) can assist you, provided they have a DB smartphone/tablet (or iPhone/iPad) or a DB Workplace Windows or Mac device. Go to:

> Section 4.6.2: Creating a temporary access pass for a colleague

Option 3 – Expert mode:

You **only** have **one 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 4.7 Activating a device with the temporary access pass (TAP)

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

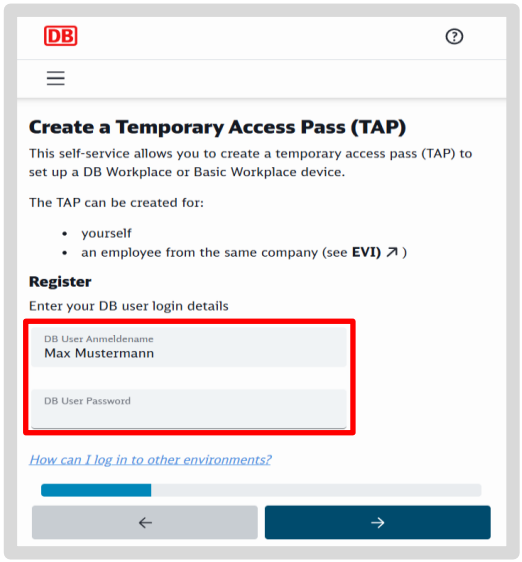
Important! You **cannot** create a temporary access pass (TAP) whilst setting up your new smartphone or tablet. Therefore, leave your old smartphone or tablet switched on and do not reset it just yet. You can also carry out the next steps on your smartphone or tablet.

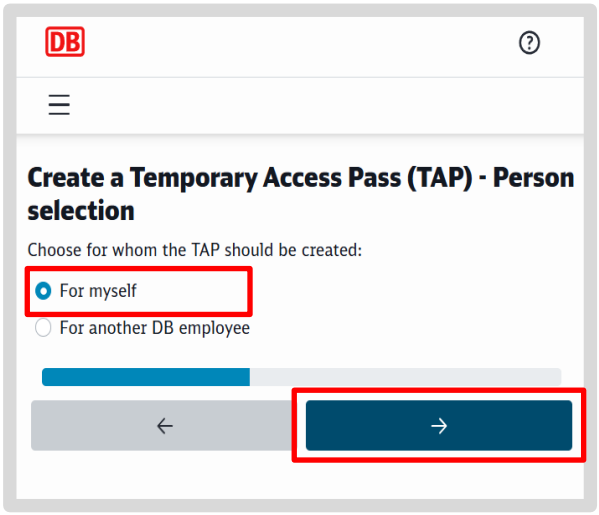
If you still have the Welcome app installed:

- open the *DB Mobile Info* app and tap on ‘Service’
- Then click on ‘Temporary Access Pass (TAP)’ to create it

If you have a DB Workplace Windows or Mac:

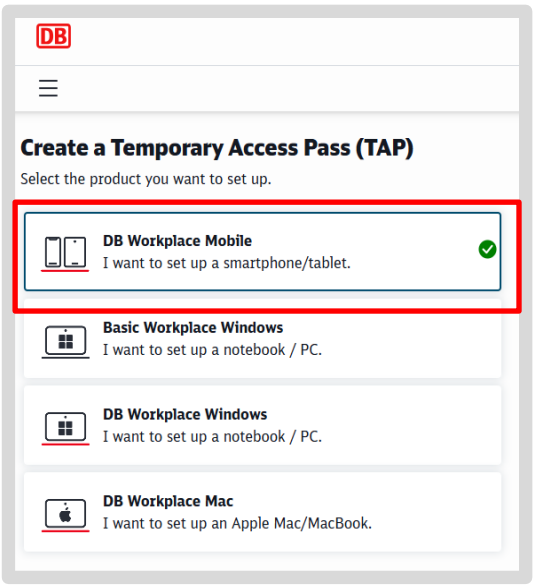
- Open your default browser
- Go to db.de/tap and enter your DB username and DB password
- Select ‘For myself’ and tap the blue button
- Now select ‘DB Workplace Mobile’
- You will then be shown the temporary access pass (TAP)
- This is now valid for 60 minutes and can be used on multiple smartphones/tablets

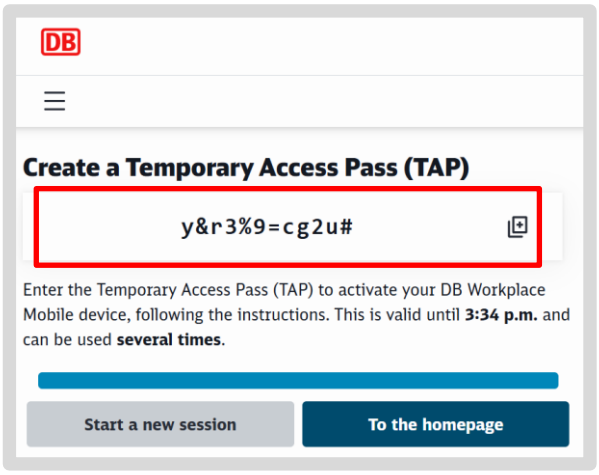




- Make a note of the temporary access pass (TAP) on a piece of paper or in a notebook

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





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.

- Make a note of the temporary access pass (TAP) on a piece of paper or in a notebook
- You'll need it later when setting up and activating your device in the Intune app
- You can now activate your smartphone/tablet in the Intune app

> Go straight to Section 4.7: Activate device using the temporary access pass

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 4.7: Activate device using the temporary access pass

4.6.2 Creating a temporary access pass for a colleague

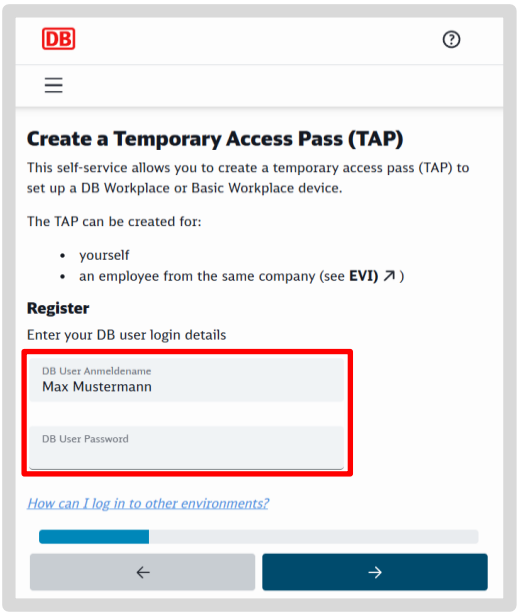
To create a TAP for a colleague, follow these instructions:

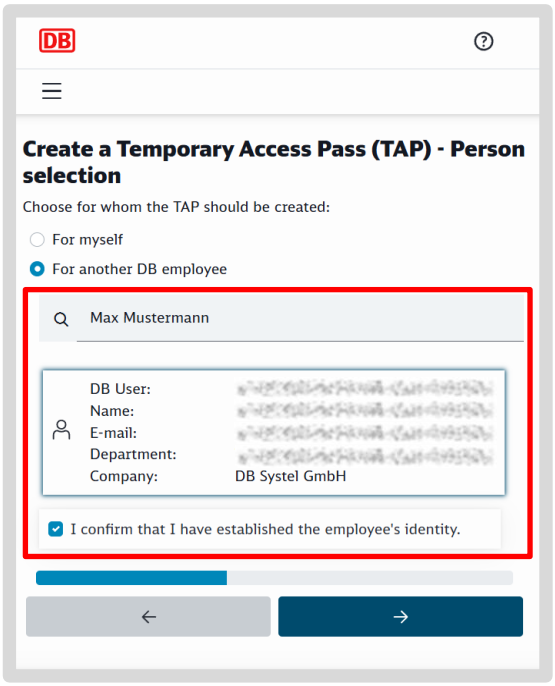
If you still have the Welcome app installed:

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

If you have DB Workplace for 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

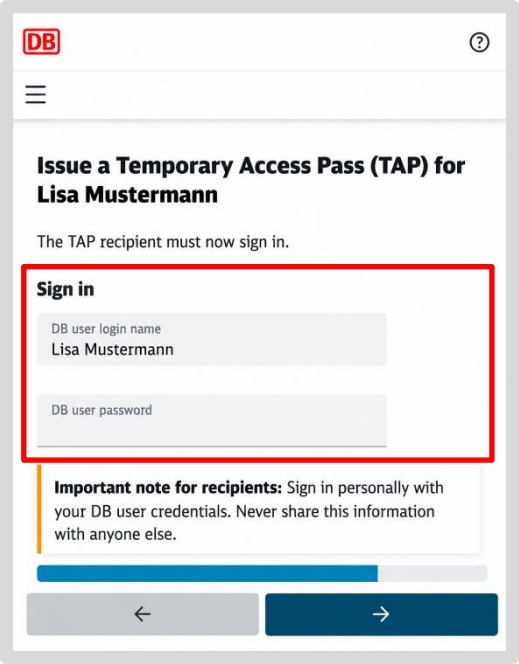


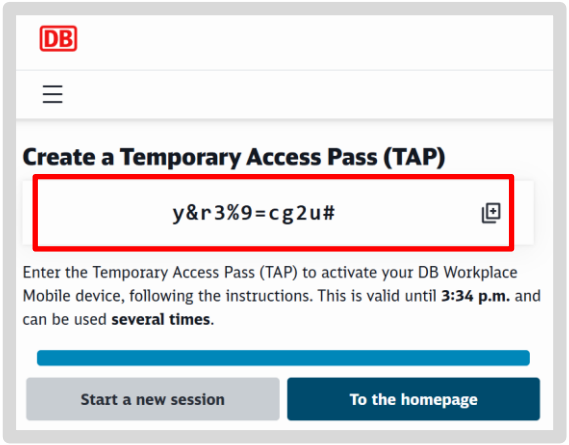


- Select the correct person and confirm their identity
- Assign control in *Teams* to the colleague(s) (if working remotely via *Teams*)

or

- Let the colleague(s) 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 or tablets**
- Restore screen control if you've been using *Teams*
- Write down the temporary access code on a piece of paper or in a notebook
- Write down the temporary access pass on a piece of paper or in a notebook





- You'll need it later to set up and activate the device in the *Intune app*
- Your colleague can now activate their smartphone or tablet in the *Intune app*

> Go straight to section 4.7: Activate device using the temporary access pass

Important!

Your smartphone or 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

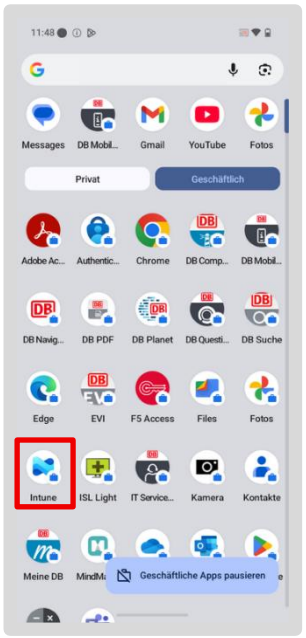
> Chapter 4.7: Activating a device with the temporary access pass

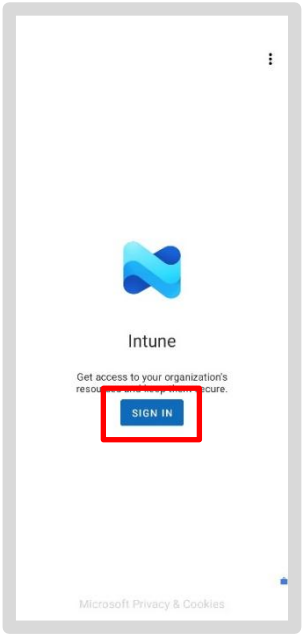
4.7 Activate device using the temporary access pass (TAP)

> **Note**: Check that you have received a temporary access pass (TAP) as described in Chapter 4.6: Activate device – Create a temporary access pass (TAP)!

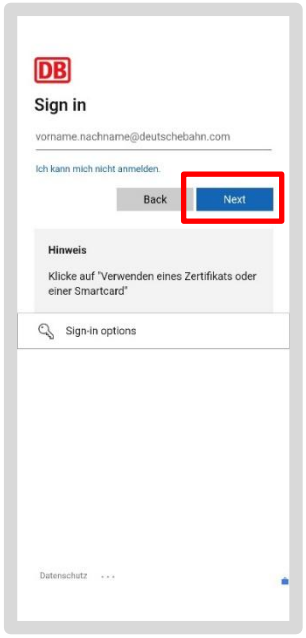
> **Note:** You can find a video tutorial at db.de/mobile-videoanleitung

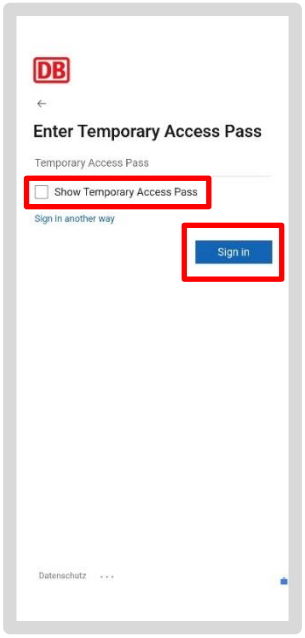
- You do not need the *Welcome app* for activation! Use the Intune app now!
- Go to the 'Work'/'Business' section by swiping up from the bottom
- Open the *Intune app* and tap the 'Sign in' button





- Enter your **DB user email address** (not: DB User) and tap 'Next'
- **Tip:** Tick the box next to 'Show temporary access pass'
- Enter your temporary access pass and tap 'Sign in'





If you receive an error message:

- Generate a new temporary access pass and repeat the sign-in process as described in Section 4.6 Activate device – Generate a temporary access pass (TAP)

> Otherwise, go to Chapter 4.8: 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.

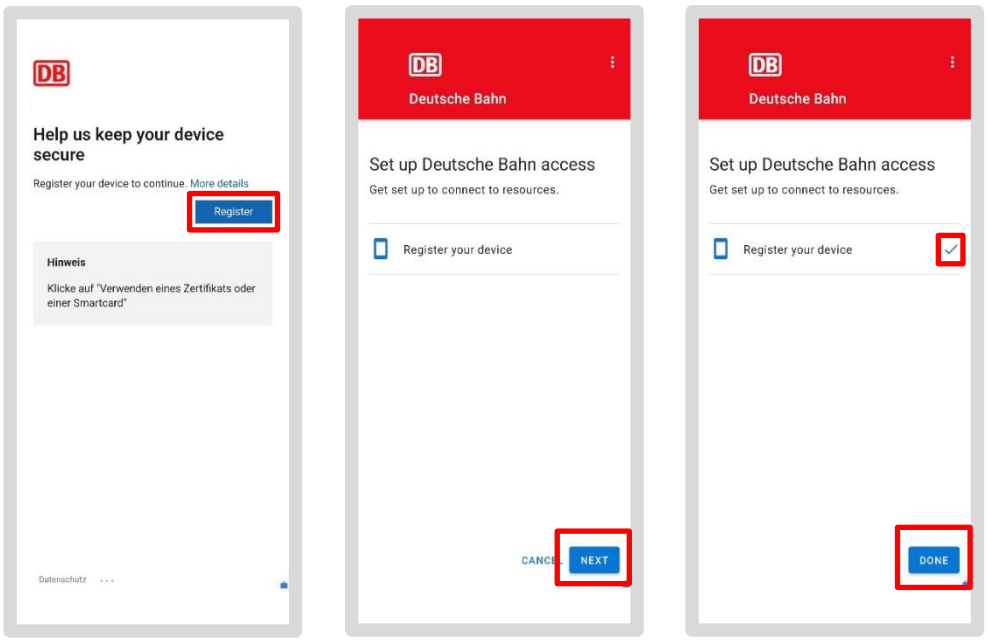
4.8 Setting up access to all DB apps and websites

Access to the DB network will now be set up:

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

Please note: If the *'Done'* button does not appear, activation is not complete

- Open the Intune app again and go through the steps from section 4.6, 'Activate device – Create a Temporary Access Pass (TAP)', step by step



> **Note:** After registration, please wait between 5 minutes and 24 hours!

Once this is done, all the information and certificates will have been transferred to your smartphone or tablet, and you'll be able to use your apps, such as *Outlook*, *Teams*, etc.

4.9 DB Apps

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.

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 other 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's the ***DB Mobile Info app,*** which contains all the information, useful links and details relating to your DB smartphone/tablet.

4.10 Change screen lock

The screen lock is a personal password or a personal combination of numbers that you set yourself to keep your smartphone/tablet secure.

In the next step, change the screen lock and set a new password or a new 6-digit combination. Please also take note of the privacy policy and terms of use.

You can also set up what is known as 'biometric security'. This allows you to unlock your smartphone or tablet using your fingerprint or facial recognition.

Proceed as follows:

- Go to the 'Settings' section
- Tap the 'Settings' app in the 'Personal'/'Privacy' section
- Or swipe down once with your finger from the top of the screen
- A bar with icons will appear
- Tap the cog icon in the top right-hand corner
- Tap 'Lock Screen' and select 'Lock Screen Type'
- Enter your current screen lock. The first time you do this, it will be the password from the 'Unlock' step (**DB-Device2019**)

For tablets:

- In the following menu, select 'No, thanks' and tap 'Next'

Then continue:

- Select 'PIN' or 'Password'
- Enter a new password or PIN. Make sure you remember it!

If you want to set up biometric security:

- Under ‘Biometric data’, select ‘Fingerprints’ or ‘Face’
- Scan your fingerprint or face
- Enter your current device password or PIN
- The device will now scan your face (please note: if you wear glasses, you must remove them during the scanning process)
- Once facial recognition has been set up, a notification will appear
- Confirm the “Quick Face Recognition” message by tapping “OK”

4.11 Take-Off: “Log in on your smartphone/tablet ”

To set up your DB smartphone/tablet for the first time, you’ll need the following:

SIM card & SIM card PIN

- You need the SIM card to make calls on your smartphone/tablet. You’ll find the SIM card and PIN in the letter from Vodafone that you’ll receive in advance
- You must enter the SIM PIN every time you switch on the device
- If you’ve forgotten it, have a look here

Screen lock password

- The first time you unlock the device, the password is **DB-Device2019**
- The screen lock is a personal password or a personal combination of numbers – this protects your smartphone or tablet from unauthorised access
- Next, think of a new PIN or password that you can use to unlock your smartphone or tablet in future, and make sure you remember it well

DB User username & DB User password

- You’ll need your DB User login name and DB User password to log in too many DB apps and websites
- The DB User username consists of your first name and surname
- You set your DB User password yourself during activation
- If you have forgotten your password, change it at https://self.service.deutschebahn.com/my.policy

Please note: Some tools, such as ASES, have their own passwords. You can store these in the ‘Keepass2Android’ app (this applies only to smartphones/tablets running the Android operating system).

- DB user email & temporary access pass (TAP) for activation
- You can obtain your temporary access pass (which is valid for a limited period) via the IT ServiceDesk app

- Use this to log in to the Intune app and activate your smartphone or tablet

In summary:

Setting up your DB smartphone/tablet – follow these steps:

- Insert the SIM card
- Switch on your smartphone or tablet
- Obtain a temporary access pass via the IT ServiceDesk app. You can do this either via your second DB smartphone/tablet, a BKU/Basic Workplace computer, or via a colleague
- Open the Intune app and enter the temporary access pass (TAP)

Along with your smartphone/tablet, you'll receive a printed leaflet. This will help you with the initial setup!

> If you don't have this to hand, you can also find it online at db.de/mobile-setup

4.12 Notes on switching on your device each day

When switching your smartphone/tablet on or off, you must always do the following from now on:

- Unlock the SIM card using the SIM PIN from the SIM card letter sent by Vodafone
- Unlock your smartphone or tablet using your personal password or PIN
- Or the device will recognise you via your fingerprint or face

If you've already switched on the device, only unlock it using your fingerprint or facial recognition when needed.

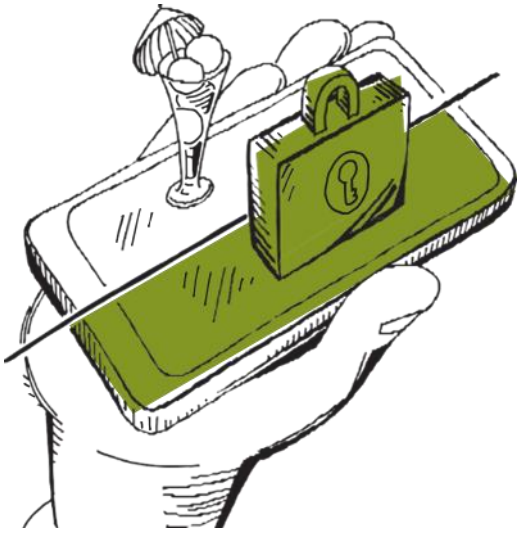
5 Work and personal content

An Enterprise version is installed on your DB smartphone/tablet; you can tell this by the fact that personal and work content are kept separate:

- On Samsung/HMD devices, work-related content and apps are stored in a separate 'Work/Business' section. You can recognise work apps by a briefcase icon on the app icon and a grey briefcase icon in the top right-hand corner next to the battery icon.

In this guide, we've put together some tips on using apps to ensure that work and personal data don't get mixed up. Always stick to this rule:

Only use work apps for work-related tasks!



5.1 Distinguishing between work and personal use

Work-related use is when you

- Start your shift via an app
- Or open the current duty roster

Personal use includes, for example:

- Watching Netflix
- Listen to Spotify
- Create a Google account

Please note: It is not always possible to draw a clear distinction between work and personal use. You should therefore always consider carefully what you are using your smartphone or tablet for.

Here's how to switch to the 'Work/Business' section:

- Swipe up with your finger on the home screen
- Tap 'Work' or 'Business' in the bottom right-hand corner
- You will now see all your work apps

The only exception: the Phone app may be used for both work and personal calls. For work calls, tap your work 'Contacts' app, select a work contact and tap the telephone receiver icon.

5.2 Downloading DB apps

Download work apps with the DB icon via the **DB Google Play Store** in the 'Work' or 'Business' section.

Apps for personal use can be installed as required. To do this, use **your personal Google account** or create a new one, and please note the device's terms of use.

5.3 Managing items on the home screen

You can drag DB apps that you use every day, such as the work camera app, onto the home screen. Here's how:

Create a folder

- Tap an app or shortcut
- Press and hold it until the app starts to wobble
- Drag the app or shortcut onto another one → Let go → A folder has been created
- If you want to add more apps to the folder, drag them onto it

Rename a folder (group)

- Tap the folder you want to rename
- Tap the suggested folder name
- You can tap a suggested name at the top of the keyboard or enter the name of your choice

Moving apps/folders

On your smartphone or tablet, you can move apps and folders within the screen or from one screen to another:

- Tap and hold the app for a few seconds
- Then drag the app to where you want it and let go

> You can find more useful tips for apps on the Samsung Support page

5.4 Take-Off: Separating personal and work use + grouping apps

Your smartphone or tablet is what's known as an enterprise device. You can find apps for your work on Samsung/HMD in the 'Work/Business' section.

Only use work apps for work-related tasks! Some apps are available for both work and personal use. Make a conscious decision about which ones to use for your specific needs.

You can drag DB apps that you use every day onto the home screen. You can also group apps together to get a better overview of your DB apps.

6 Further settings

In the next step, we'll show you how to customise your smartphone or tablet to suit your needs, so that it supports you as effectively as possible in your day-to-day work.

6.1 Android operating system Install updates

The operating system forms the basis of your smartphone or tablet. It is the user interface on which apps and software are then installed.

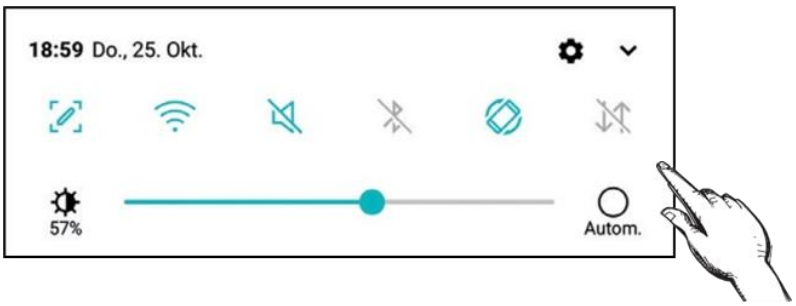
Your Samsung/HMD runs on the Android operating system. You can check which version of the operating system your smartphone or tablet is running here:

- Open Settings
- Scroll to 'Phone info' or 'About phone'
- Tap 'Software information'
- The currently installed Android version will now be displayed here

6.2 Quick Access/Control Centre

Want to adjust the brightness, turn off Wi-Fi or open your smartphone or tablet's settings? You'll find this feature in the 'Quick Access' menu:

- Swipe down once with your finger from the top edge of the screen
- A bar with icons will open – this is Quick Access



Here you can enable or disable functions on your smartphone or tablet by tapping them, for example:

Adjusting the screen brightness:

- Tap the bar in Quick Access and slide the slider to the desired brightness
- Want the screen brightness to adjust automatically? Tick the ‘Auto’ box or tap the small sun icon with the ‘A’ next to it

There are even more functions in Quick Access. To view them, swipe down from the top of the screen again with your finger. More icons will appear, such as the torch. The torch app is also hidden here

You can find more settings via ‘Settings’ (the cog icon). You can access this by swiping down from the top of the screen.

6.3 Connecting to the internet

6.3.1 DB Wi-Fi

- Connect to the DB Wi-Fi network 'dbs4public' at DB locations as described in section 4.5, 'Setting up Wi-Fi in DB buildings'
- To use the DB Wi-Fi, order the *"DB Secure Network Access Mobile Device"* service via the Digital Shop

6.3.2 Public Wi-Fi

Data security on your smartphone or tablet is a particular concern wherever public Wi-Fi is available.

- Only log in via DB Wi-Fi or your private home Wi-Fi
- Avoid using third-party, unsecured Wi-Fi networks
- Also, when selecting a network, make sure you're using the correct Wi-Fi network
- Always follow DB's general security guidelines

6.3.3 Using mobile data – your data allowance

If there is no DB Wi-Fi nearby, use the internet via mobile data. Depending on your contract, Deutsche Bahn provides you with a data allowance that allows you to use the internet free of charge.

- As soon as 80 per cent of this data allowance has been used up in the current month, you'll receive a text message
- You'll be asked whether you'd like to top up with additional data allowance
- Please note that this will incur additional costs for DB

6.3.4 Your Vodafone contract – Elfe (electronic telecoms bill)

Once a month, you'll receive a statement for your smartphone/tablet's Vodafone contract. You'll receive it by email from the sender ELFE@deutschebahn.com.

Important: You do not need to pay anything; the statement is for documentation purposes only.

6.3.5 Disable data warning

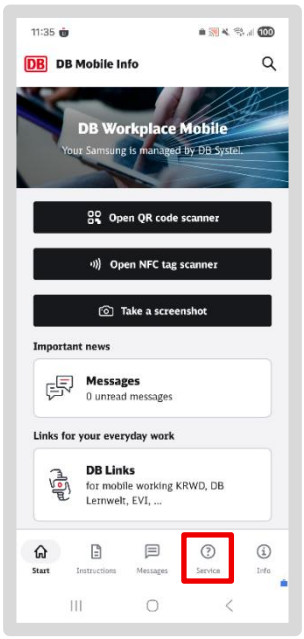
The Android operating system automatically sends you a warning as soon as you have used 2 GB of data in a month. This helps you keep track of your data usage.

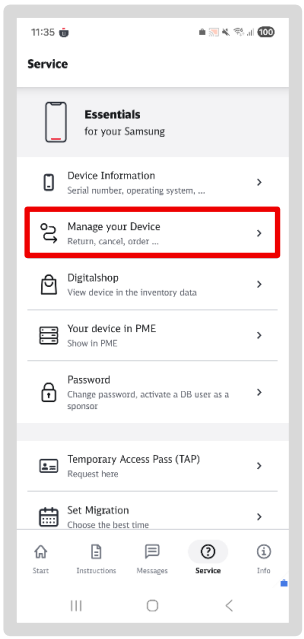
At the same time, all Vodafone users on the DB network have 6 GB of base data allowance and the automatic 2 GB top-up pack (= 8 GB total allowance). So if you don't want to be warned after using just 2 GB of data, you can deactivate the data warning in a few simple steps. Or you can increase the default threshold.

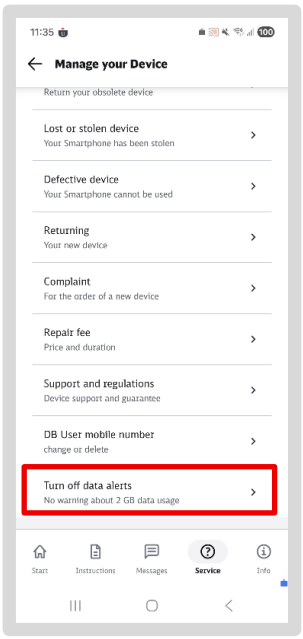
The good news is that you don't need to worry about unexpected costs! Vodafone will automatically notify you by text message as soon as you've used 80 per cent of your data allowance (i.e. 80 per cent of 6 GB or 8 GB) – no matter which mobile phone you're using.

For Samsung smartphones/tablets, follow these steps:

- Open the *DB Mobile Info* app
- Tap the ‘Service’ tab → then tap ‘Everything about your device’ → and finally tap ‘Disable data warning’

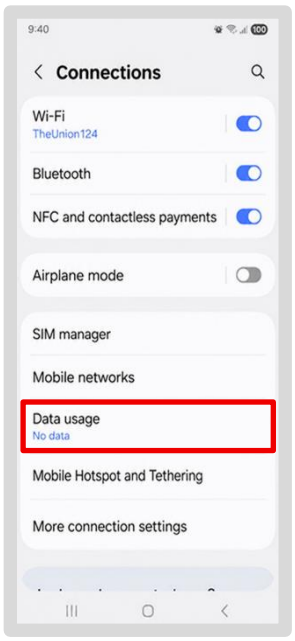


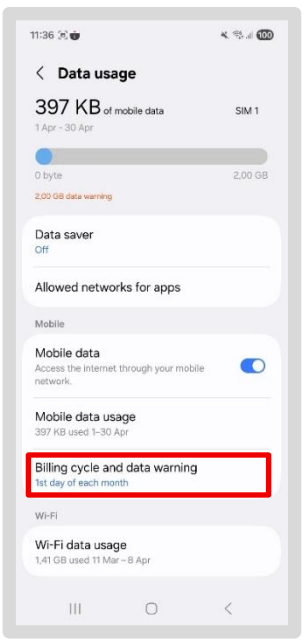


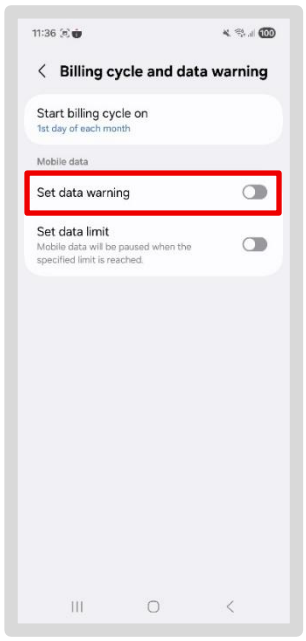


The ‘Connections’ screen will open in the system settings

- Tap ‘Data usage’ ❼ then ‘Billing cycle & data warning’ ❼ under ‘Set data warning’, swipe the screen to the left

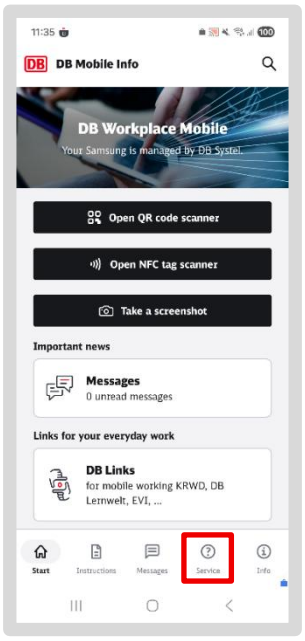


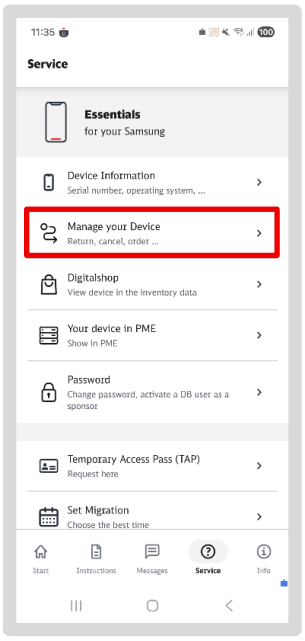


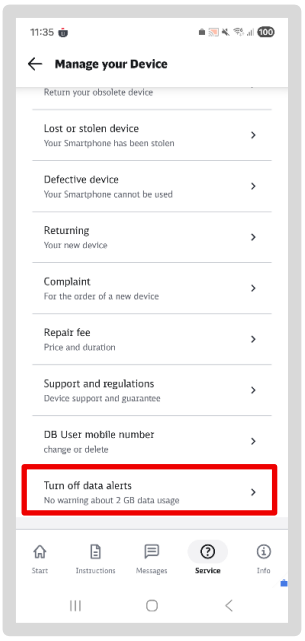


For Nokia/HMD smartphones and tablets, follow these steps:

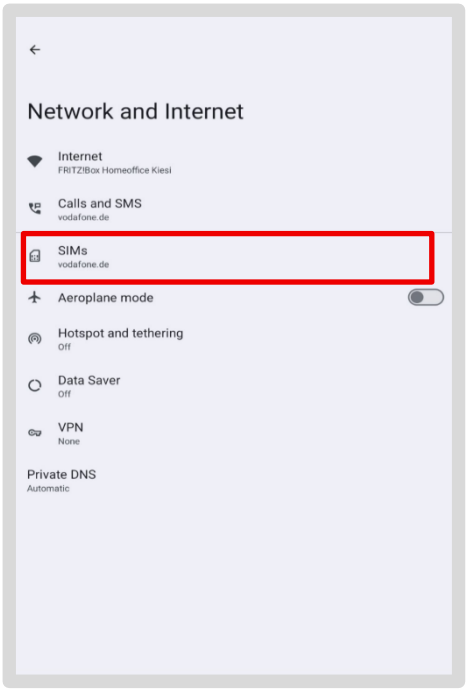
- Open the *DB Mobile Info* app
- Tap the “Service” tab → then tap “Everything about your device” → and then tap “Disable data warning”

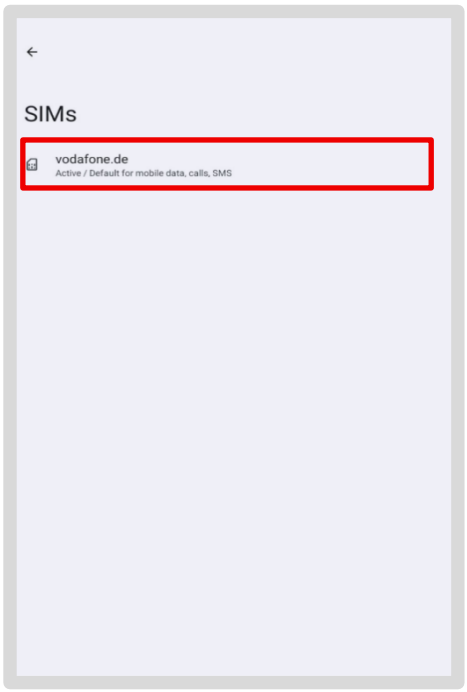


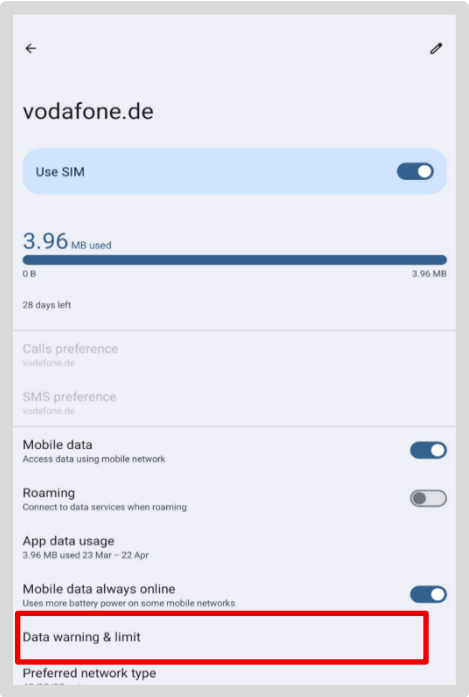


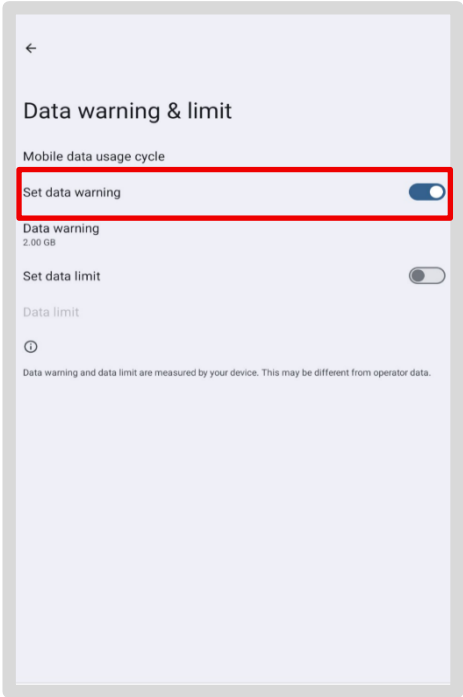


- *This opens the ‘Network & Internet’ screen in the system settings*
- Tap ‘SIM cards’ ❼ Tap the active SIM card (in this case, ‘vodafone.de’❽ ❼ Tap ‘Data warning and limit’ ❼ Under ‘Set data warning’, swipe the screen to the left









6.3.6 Offline mode (Airplane mode)

You can enable Offline mode or Airplane mode via the quick settings panel on your smartphone or tablet. Please note, however, that this will disable all communication functions. This means that no updates will be carried out and you will not receive any DB messages.

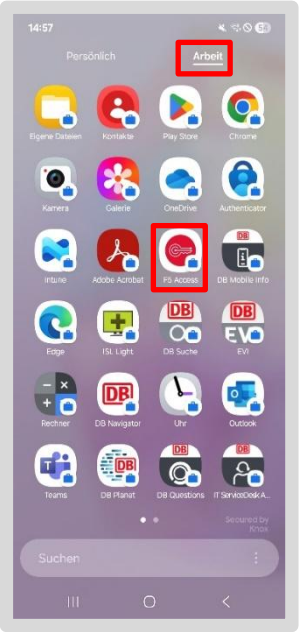
So think carefully about when you switch to flight mode.

6.4 F5 Access – Establishing a VPN connection

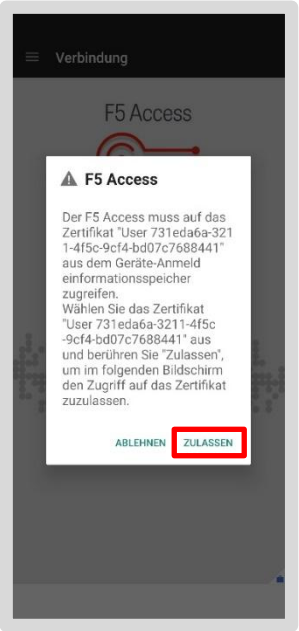
VPN stands for **Virtual Private Network** and refers to an internet connection that cannot be viewed by unauthorised third parties. At DB, we use **'F5** Access' to establish a VPN connection. This gives you secure access to Deutsche Bahn's corporate network. Furthermore, some apps can only be used with a VPN connection, e.g. the staff portal, ASES and E-Time.

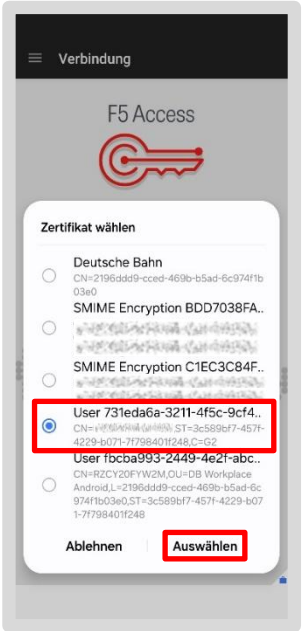
6.4.1 Set up the VPN connection

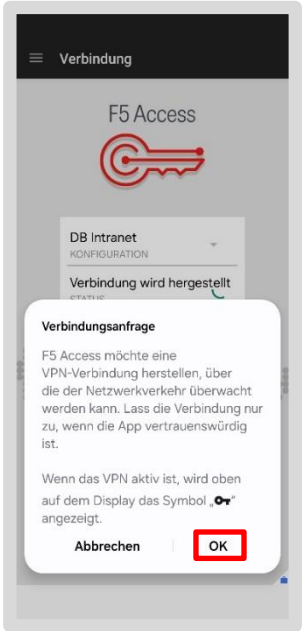
- Open the *F5 Access* app in the 'Work/Business' section
- If necessary, accept the terms and conditions and allow notifications to be sent
- Under 'Configuration', tap 'DB Intranet' and then 'Connect'
- Then allow you to make and manage calls – to do this, select 'Allow'



- Then tap ‘Allow’ for the F5 certificate
- Tap on the certificate ending with C=G2
- Then tap ‘Select’
- Then confirm the connection request by tapping ‘OK’







- To disconnect, tap ‘Disconnect’

Note: A permanently active VPN connection uses a lot of battery power. You should therefore only switch it on when you really need it.

6.5 Take-Off: Certificates & VPN connection

Why do I need a certificate on my smartphone/tablet?

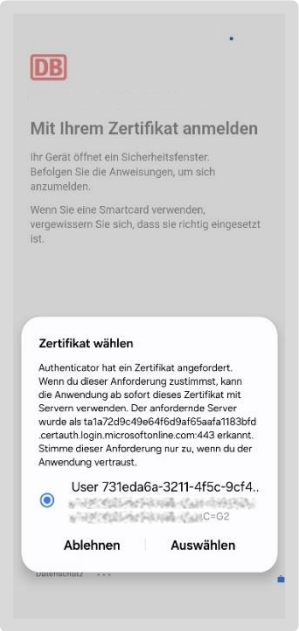
To access certain DB apps and websites on your work smartphone or tablet, you need to identify yourself. This is done using what is known as a certificate. The certificate tells the app or website that you are authorised to access it.

How do I get the certificate?

Certificates are automatically stored on your device. When you open an app for the first time, you'll need to select the certificate once, after which you'll be logged in.

In Outlook, for example, it looks like this:

The certificate always contains your first name and surname



What is the F5 Access app?

The *F5 Access app* is automatically installed on your smartphone or tablet. On Samsung/HMD devices, you'll find it in the 'Work/Business' section

The *F5 Access app* establishes a secure VPN connection between your smartphone or tablet and the DB intranet. This is because certain mobile apps and websites require this access in order to connect.

6.6 Improving battery life

- Updates can only be installed on your smartphone or tablet if the battery is more than 20% charged
- If updates are not installed, this may eventually mean you can no longer use your smartphone or tablet (so always make sure your battery is sufficiently charged!)

How to conserve your battery:

- Switch off services that aren't needed all the time, e.g. Bluetooth, VPN (F5) and the GPS function
- Do not charge the device overnight
- Do not expose it to extreme temperatures – whether too cold or too hot

6.7 Disable the advertising ID

By default, Google creates a so-called advertising ID for every smartphone or tablet.

Google uses this advertising ID to create a profile based on your online behaviour and preferences. This allows personalised adverts to be displayed on your smartphone or tablet.

The Group Data Protection Office recommends disabling this advertising ID. This is the only way to prevent a profile from being created.

To do this, follow these steps:

- Open the *Settings* on your smartphone or tablet
- Tap on Google and then on Work/Business
- Select 'Ads'
- Tap 'Delete advertising ID'
- Confirm by tapping 'Delete advertising ID'

The advertising ID is now deactivated; profiling is no longer possible.

More information about the advertising ID is available on DB Planet here:

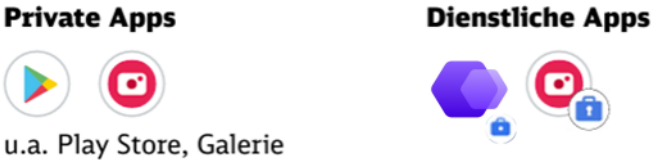
> #MobileWorkplace

7 The most important apps to get you started

The most important DB apps are already installed on your smartphone or tablet.

7.1 Download new DB apps

If you'd like to install more **DB apps**, download them from the **DB Google Play Store**. DB-specific apps, such as Meine DB or DB Planet and many others, are only available for download there.



You can download **private apps** onto your **Samsung/HMD** via the **Google Play Store** in the private section.

7.2 The DB Mobile Info app

Have you forgotten your screen lock password or can't remember your DB user password? Does *Outlook* keep crashing? Are you getting error messages you don't understand? Don't worry – you'll find help here.

The **DB Mobile Info app** is your first port of call for any questions about your smartphone or tablet.

Features on the home screen:

- Take a screenshot and save it automatically to the work gallery or photos app
- Read NFC tags and use them in the work area
- Use the QR code scanner for work-related information
- Tap the magnifying glass to go straight to the DB Search, where you can ask questions about DB-related topics

In the 'Guides' tab, you'll find the most important guides. In the 'Service' tab, you'll find important work-related links and all the personal links you need for your work at DB, as well as the IT ServiceDesk telephone number.

If your device isn't working at the moment, use a colleague's device.

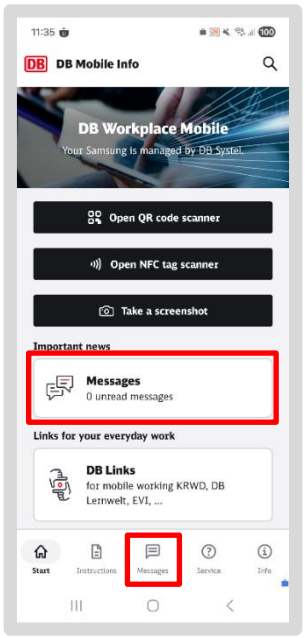
> Alternatively, you can also find all the key guides at: db.de/ae

7.2.1 Push notifications

You'll receive **push notifications** via the *DB Mobile Info* app for new software updates or anything else relating to your smartphone or tablet. For example, this is how we'll keep you informed about the distribution and automatic installation of new software on your smartphone or tablet.

You can find your messages here:

- Open the *DB Mobile Info* app
- On the home screen, you'll see the notifications area
- If you have a new message, you'll see a small red number next to 'Unread messages'
- To read your messages, tap the 'Messages' section
- Alternatively, you can tap the 'Messages' tab at the bottom



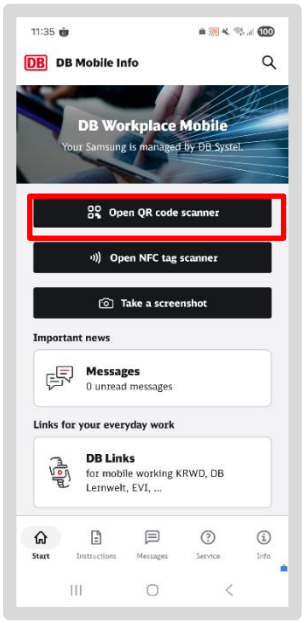
> For more information, see: DB Mobile Info app: Receiving messages

7.2.2 Scan QR codes

QR codes are black-and-white square patterns that can be scanned using your smartphone or tablet's camera. A scanner decodes the code and automatically redirects you to the app or a website containing further information.

You can scan official QR codes using the *DB Mobile Info app*:

- Open the *DB Mobile Info app*
- Tap on 'Open QR Code Scanner'



- Then allow the app to take photos and record videos
- A small window will open, allowing you to scan the QR code
- To do this, position the QR code within the rectangle

Once the code has been scanned, you'll be redirected to its content

7.3 Outlook

With *Outlook,* you can receive and send your work emails. Before you can get started, you'll need to configure a few settings.

Do you have questions about writing and sending emails? On ITfit, you'll find useful tips and guides on using *Outlook*.

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

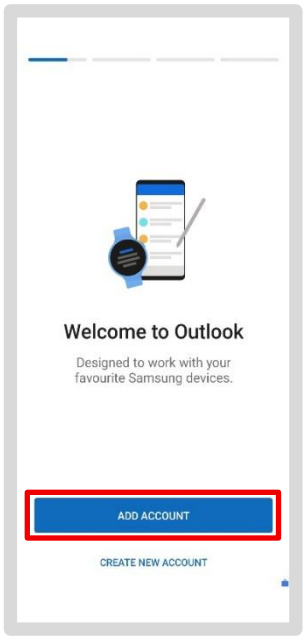
> **Note:** You can find a video tutorial at db.de/mobile-videoanleitung

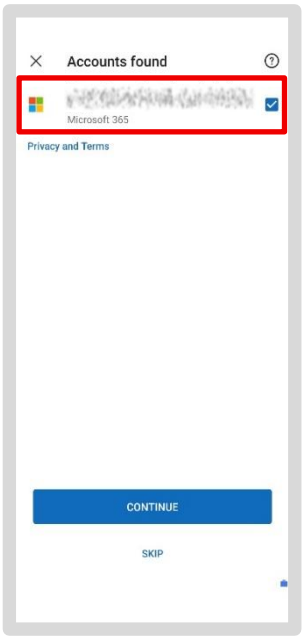
- Go to your 'Work/Business' section and tap the *'Outlook'* app
- Your email account is automatically set up – tap *'Add account'*
- In the next step, select your email address and tap *'Next'*

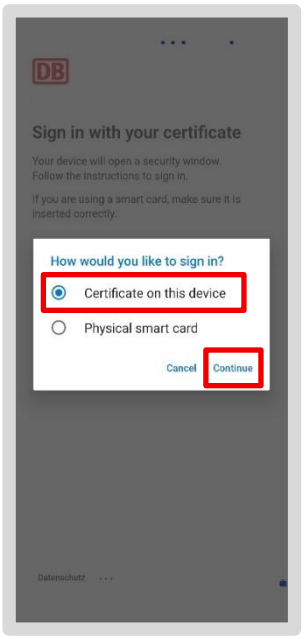
When prompted to log in, you may be asked for a temporary access pass (TAP):

- If your temporary access pass is still valid, enter it here or create a new one as described in Chapter 4.6 'Activate device – Create a temporary access pass (TAP)'

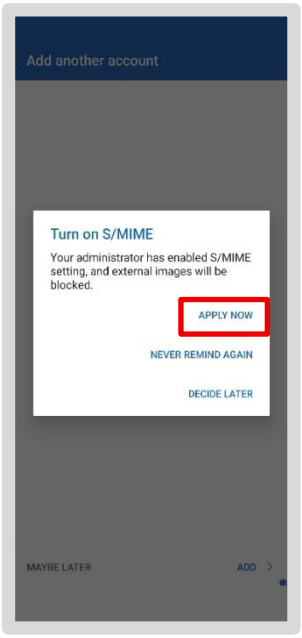
- Alternatively: under *'Select another login option'*, choose the option *'Certificate on this device'*
- Tap *'Select'* when prompted for the certificate







- 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 what is known as S/MIME encryption for this purpose
- Tap *'Apply now'* when asked whether you wish to enable S/MIME

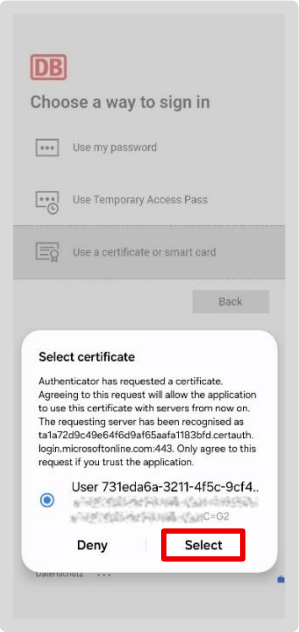


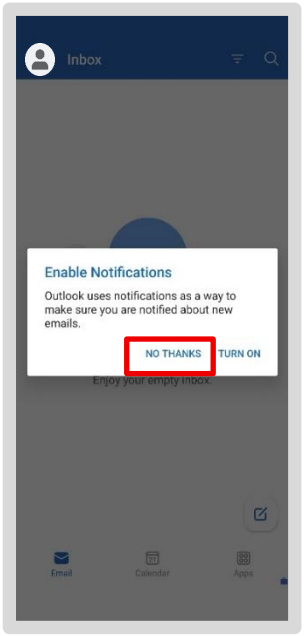
You will then be prompted to select a certificate. You can identify the certificate that applies to you as follows:

- 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 will now be set up:

- Tap ‘Maybe later’ when asked if you want to add another account
- And select ‘No, thanks’ when prompted to enable notifications





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

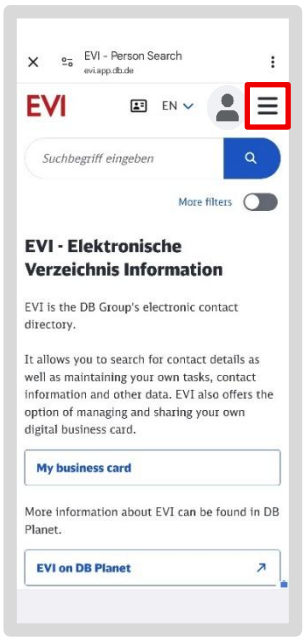
Android 16: On devices running Android 16, the step to enable S/MIME may be skipped. In this case, you must complete the *Outlook* setup and restart the app! The prompt to enable S/MIME will then appear.

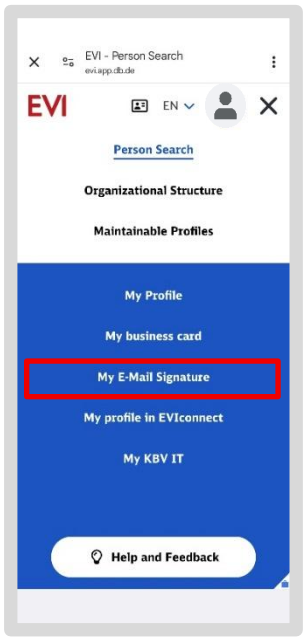
7.3.2 Setting up an email signature

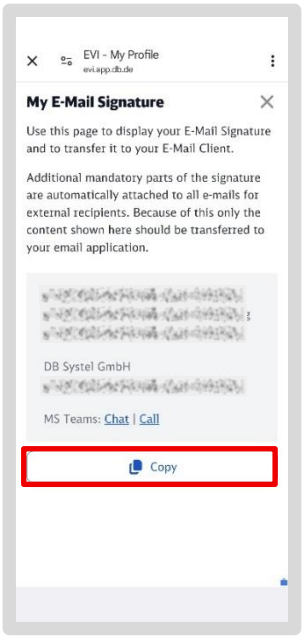
An email signature is a mandatory part of business communication. It appears at the end of an email and, by law, must contain certain information, such as the company name and the official registered office of your DB company. You can find the text for your email signature in DB’s central directory,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

Here's how to retrieve your email signature from the 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 field. Copy it by tapping 'Copy'

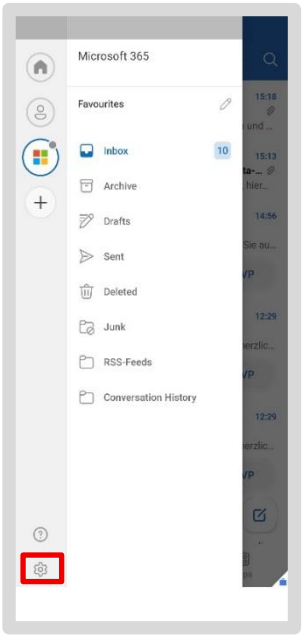


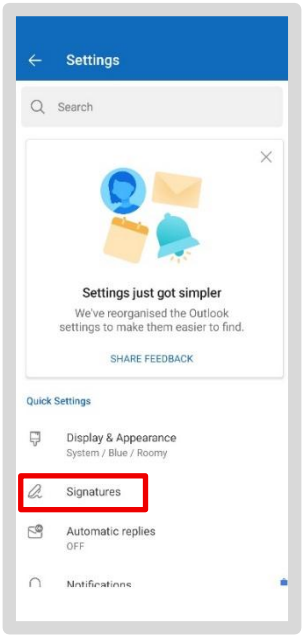


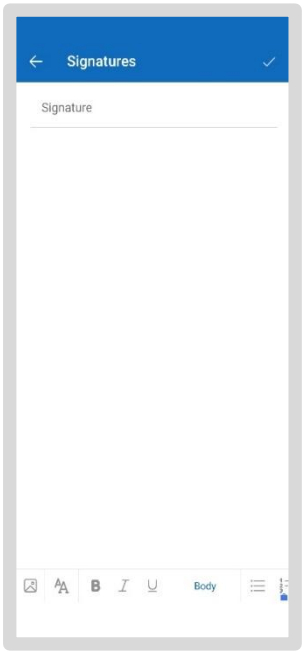


Paste the signature into *Outlook*:

- Open the *Outlook app*
- Tap your profile picture in the top left-hand corner
- Tap the cog icon in the bottom left-hand corner
- Now tap 'Signature'







- A field for the signature will open. If there is already an entry there, delete it
- Now long-press the field until the 'Paste' option appears, then tap it
- Your copied signature from *EVI* will be inserted

Close the window – your signature will now be automatically added to 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.

7.3.3 Email synchronisation – All your emails are 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 device you log in from – be it a smartphone, tablet or BKU/Basic Workplace computer – you'll always be up to date.

If you previously owned an old smartphone or tablet and wish to import your contacts, please refer to Section 8.5: Backing up contacts to OneDrive.

7.3.4 Creating new contacts in Outlook

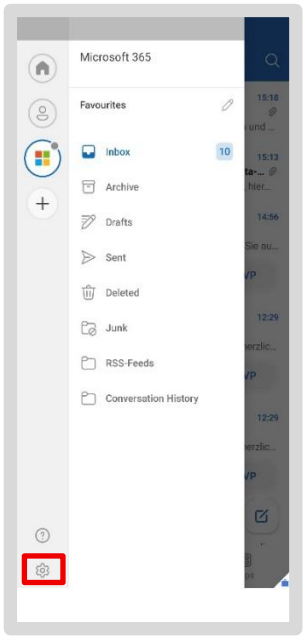
- Go to the 'Work' section and open the Contacts app
- Tap the '+' to create a new contact
- Select 'Outlook' in the top-left corner above the arrow
- The new contact will be saved in *Outlook*

7.3.5 Synchronising contacts in Outlook

If you create a new contact in the 'Work/Business' section on your smartphone or tablet using the Contacts app, it's a good idea to share it with *Outlook* for synchronisation. Here's how to do it:

- Open the *Outlook app* in the 'Work/Business' section
- In the app, there is a circle with an icon in the top-left corner. Tap this
- An overview of your email folders will open on the left-hand side

- Select the cog icon in the bottom left-hand corner
- The settings will open
- Under ‘Email Accounts’, select your Outlook account. Then tap the small slider next to ‘Synchronise contacts’
- Then confirm the access request by tapping ‘Allow’
- Once you’ve enabled synchronisation, exit the *Outlook app*



7.4 MS Defender app – must be opened

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

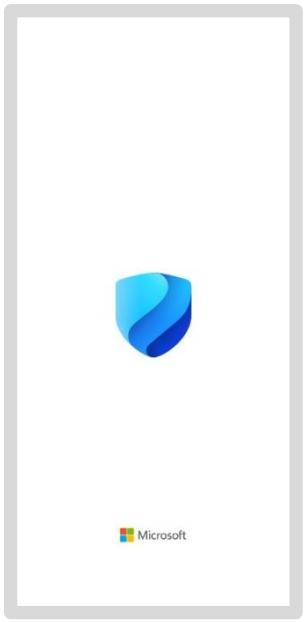
Due to the wide variety of different DB smartphones/tablets, there may be minor differences in the description of individual steps.

7.4.1 Setting up the MS Defender app

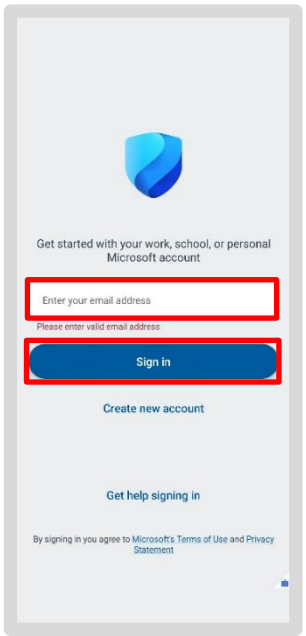
To set up the *MS Defender app* on your smartphone or tablet, you need to follow these steps:

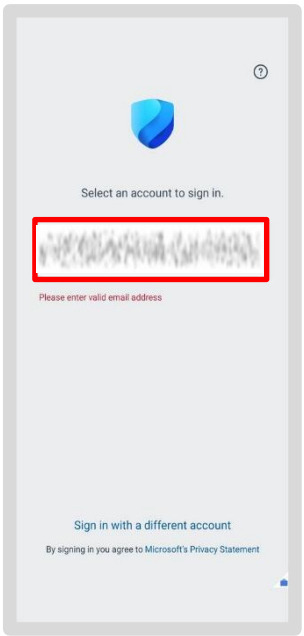
- Go to the ‘Work/Business’ section and open the ‘DB Google Play Store’
- Search for the app ‘Microsoft Defender: Antivirus’ and tap ‘Install’

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



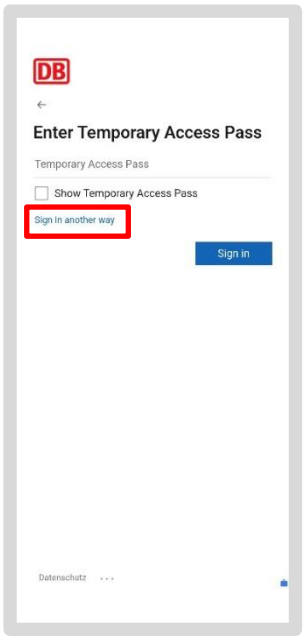
- You will be asked for your work email address
- Tap the ‘Sign in’ button, or the app will automatically take you to the next screen, where your email address will be displayed
- Tap your work email address

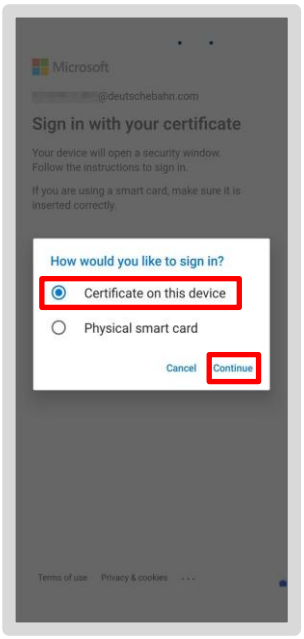


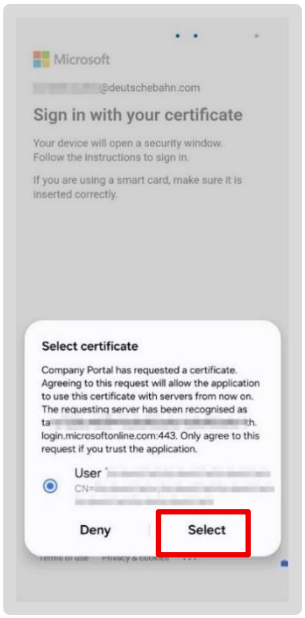


If you have activated your smartphone/tablet with the Intune app within the last hour, you may be asked here to enter your temporary access pass again.

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



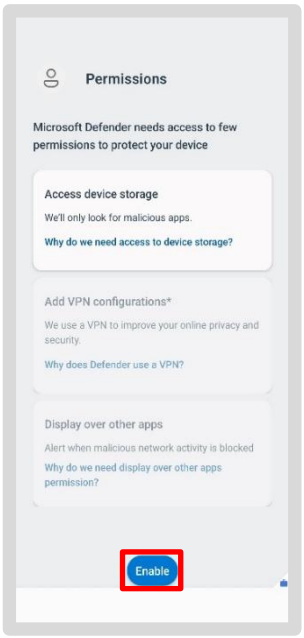


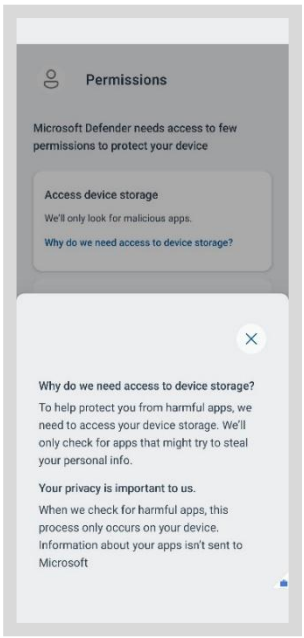


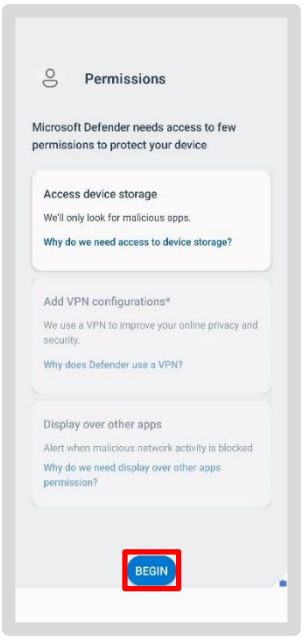
7.4.2 Grant permissions

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

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





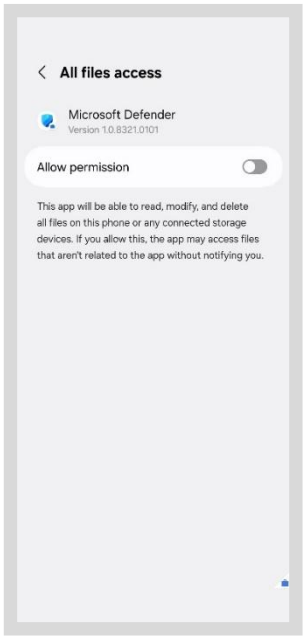


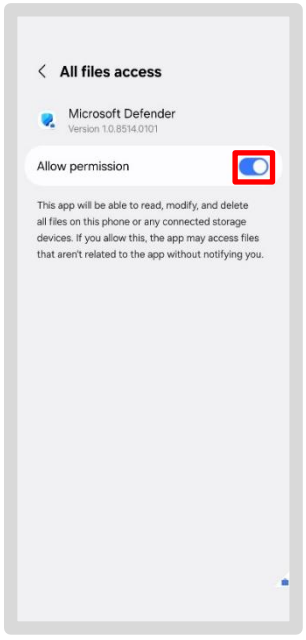
Background information on permissions:

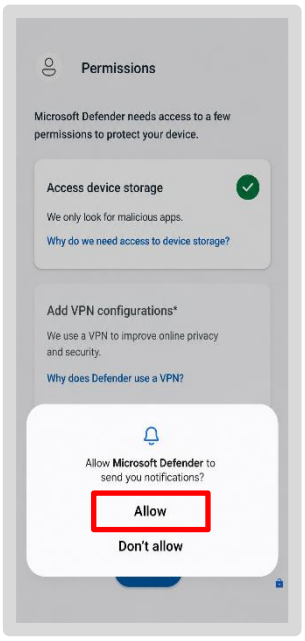
These permissions are required to ensure the app works properly and to maintain security on your device.

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 options 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 settings.

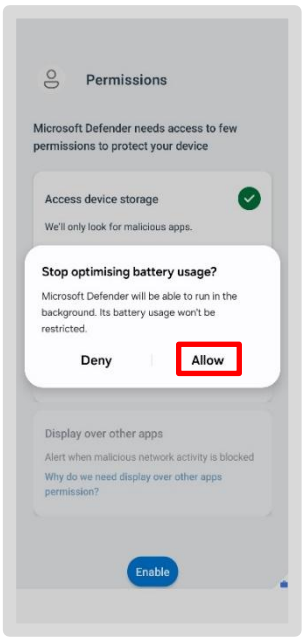
- Now slide the slider to the right to grant the permission
- When the subsequent prompt appears, tap ‘Allow’

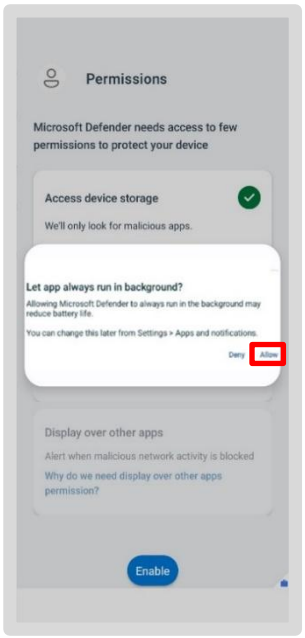






- Tap “Allow” for each of the following prompts

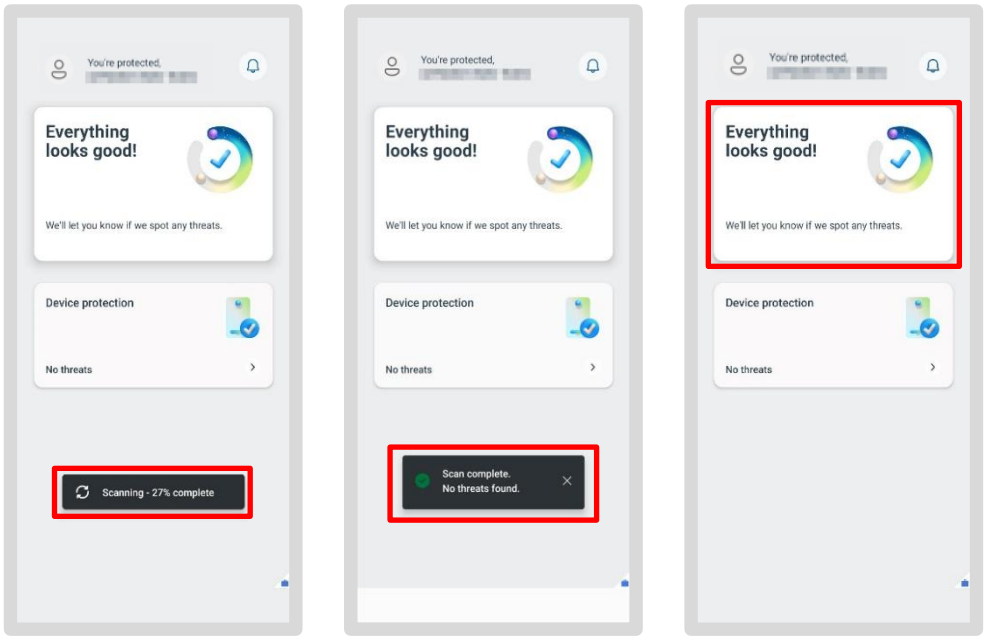




Please note: Depending on your device type, you may be asked for different permissions! As a result, you may only see one of the prompts shown here.

You will then be taken to the home screen of the *MS Defender app*. A scan for malware on your smartphone or 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.

7.5 DB M 365

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

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

- Then tap *'Install'*
- When you open a file, the app will open automatically

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

7.6 Microsoft Authenticator app

The Microsoft Authenticator app enables **multi-factor authentication (MFA).**

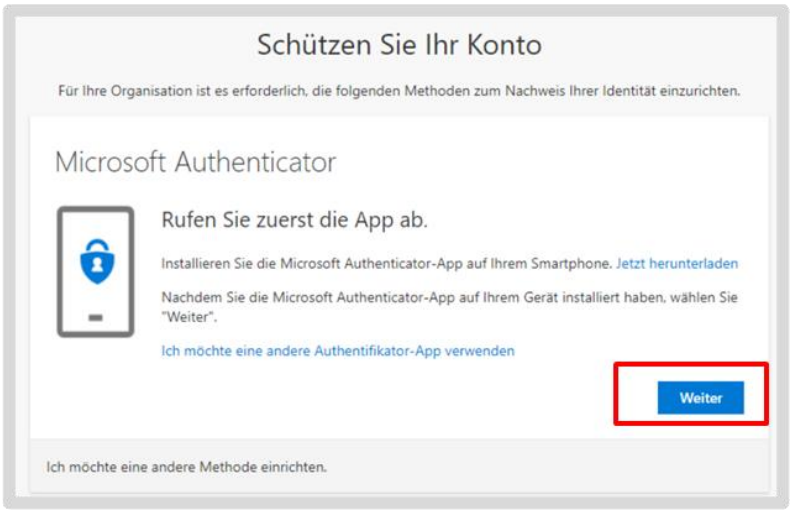
You'll need the Microsoft Authenticator app, for example, for:

- Connecting via VPN to Basic Workplace MAC
- Using the DB admin account
- Accessing specific applications, e.g. SAP

A distinction is made depending on whether you have already used the Microsoft Authenticator app on a DB smartphone or tablet, or whether you are using the app on your smartphone or tablet for the first time.

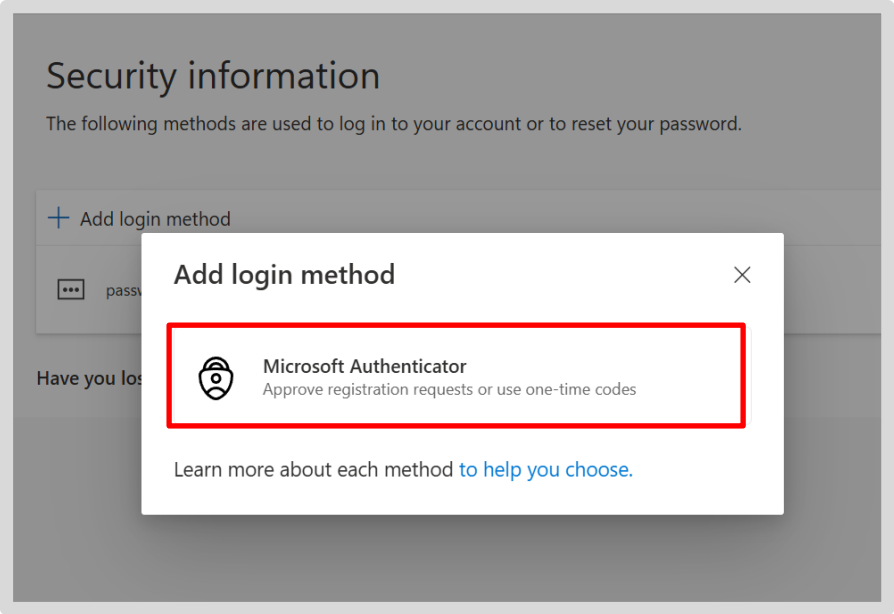
Using the Microsoft Authenticator app for the first time

When you tap on an app that requires the Microsoft Authenticator app, this dialogue box will open. Tap 'Next' and follow the step-by-step instructions; to do this, tap the 'MFA setup guide' button



Alternatively, you can launch the Microsoft Authenticator app yourself:

- Tap ondb.de/authenticator on your BKU or Basic Workplace computer
- Tap the 'plus icon' and the 'Add sign-in method' button
- A dialogue box will open; select "Microsoft Authenticator"
- Switch to your smartphone or 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 on your smartphone or tablet for authentication



Switching from an old to a new DB smartphone/tablet

If you have already been using the Microsoft Authenticator app, please note the following:

- If you need to use the Authenticator app whilst setting up your new smartphone or tablet, use your old smartphone or tablet to connect it to the Authenticator app
- Open this step-by-step guide, tap the 'MFA setup guide' button and follow the steps provided
- You can then use the Microsoft Authenticator app on your new smartphone/tablet and reset your old smartphone/tablet. If you have used the Authenticator app for websites or tools, re-activate the app on those websites
- **Tip**: If you have difficulty reactivating the connections in the Authenticator app after setting it up, use the self-service option: 'Reset Microsoft Authenticator app (MFA)':db.de/resetmfa and then follow the steps in this section from top to bottom

7.7 Key takeaway: DB Apps

Where can I find DB apps?

The most important apps are already installed on your work smartphone or tablet. If you wish to download further work apps, do so via the **DB Google Play Store**.

There you'll find, for example, *Outlook*, Word and OneDrive, as well as DB-specific apps such as Meine DB or DB Planet. You can download personal apps via the Google Play Store.

Where can I find information about my smartphone/tablet?

For any questions about your smartphone or tablet, use the *DB Mobile Info* app. You'll find instructions in the 'Guides' tab and useful information about your device in the 'Service' tab.

The app is installed on your smartphone or tablet by default.

8 Backing up data

8.1 Backing up work data to OneDrive

You have a smartphone or tablet running the Enterprise version. This means that work and personal documents are strictly separated when it comes to backups.

The process for backing up your work documents or photos/videos is described here:

> mobileworkplace.deutschebahn.com/mobile-daten-sichern

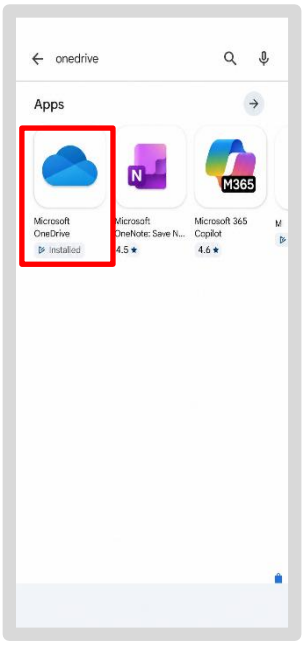
> **Note:** You can find a video tutorial at db.de/mobile-videoanleitung

To save photos and other documents, such as PDFs or Word files, you'll need the Microsoft 'OneDrive' app. With this app, you can store all your work data in the cloud and then access it at any time from all your work devices. This means you can, for example, access your data from your work PC as well.

8.2 Setting up OneDrive

Prerequisite: To set up OneDrive, first install the *Outlook app* on your smartphone or tablet and set up your work email account. You can find further information on the setup process in Chapter 7.3 Outlook.

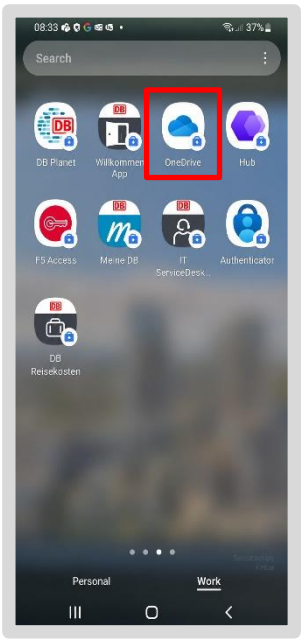
- Hold your tablet in portrait orientation to ensure that the screens match the layout shown in the instructions
- Download the 'OneDrive' app. To do this, open the Google Play Store
- Search for the 'Microsoft OneDrive' app

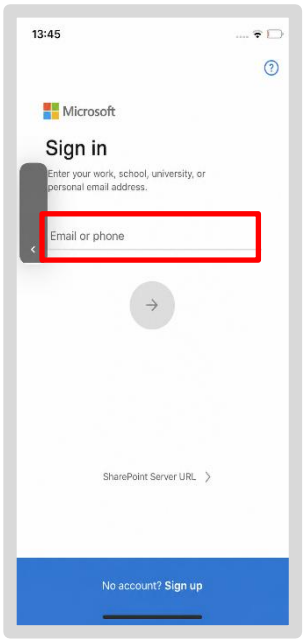


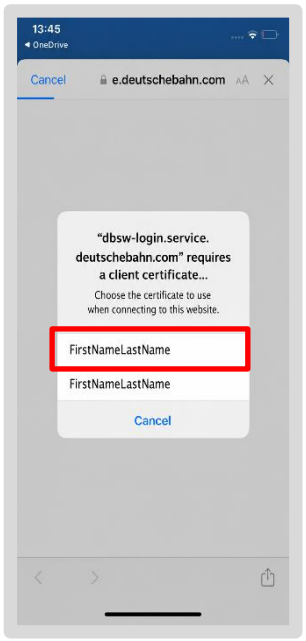
8.2.1 Android 15

Once installed, the app will appear as an icon (hint: a cloud) labelled 'OneDrive' in the 'Work/Business' section on the home screen of your smartphone or tablet.

- Open the OneDrive app by tapping the icon
- Confirm that the app is allowed to send you notifications
- Select '**Sign** in'
- Enter your DB email address – you'll be logged in automatically
- Select your DB user certificate
- You will now see all your files in OneDrive
- Enter your DB email address – you'll be logged in automatically
- Select your DB user certificate







Please note: If you're setting up OneDrive for the first time, it may take a few minutes for all your data to synchronise.

Backing up all system settings

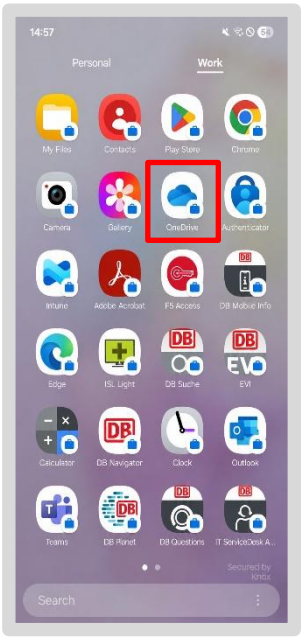
If you ever need to reset your smartphone or tablet to factory settings, make sure you also back up your system settings.

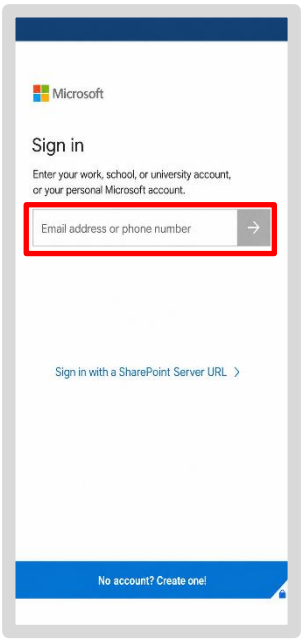
Take screenshots or make notes of your personalised settings and your specific work-related DB apps. Save these in OneDrive too, so you can refer to them as notes during set-up.

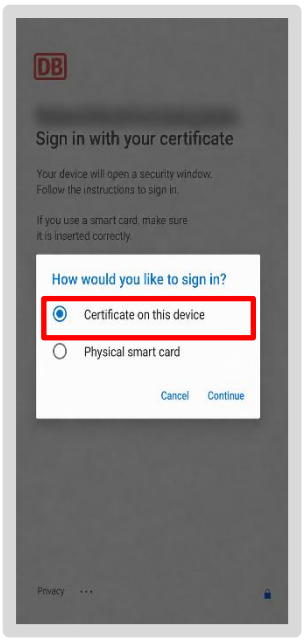
8.2.2 Android 16

Once installed, the app will appear as an icon (hint: a cloud) labelled ‘OneDrive’ in the ‘Work/Business’ section on the home screen of your smartphone or tablet.

- Open the OneDrive app by tapping the icon
- Confirm that the app is allowed to send you notifications
- Select ‘Sign in’
- Enter your DB email address and confirm by tapping the blue arrow
- Then select your DB user certificate from ‘Certificate on this device’
- Confirm by tapping ‘Select’







You will now see all the files you have stored in OneDrive.

Important: If you find yourself back at the login screen after selecting the certificate, re-enter your DB email address and try logging in again.

Please note: If you’re setting up OneDrive for the first time, it may take a few minutes for all your data to synchronise.

Backing up all system settings

If you ever reset your smartphone or tablet to factory settings, make sure you also back up your system settings.

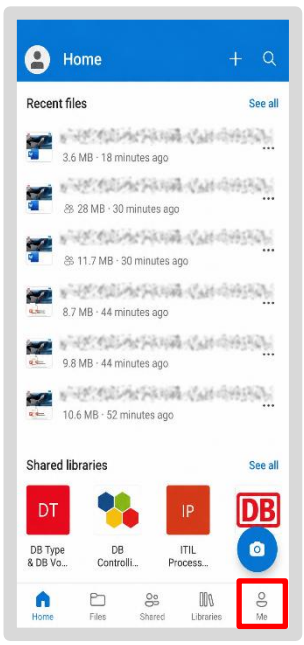
Tip:

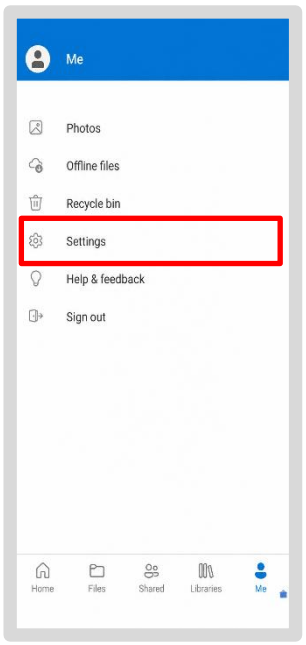
Take screenshots or make notes of your personalised settings and your specific work-related DB apps. Save these in OneDrive too, so you can refer to them as notes when setting up your device.

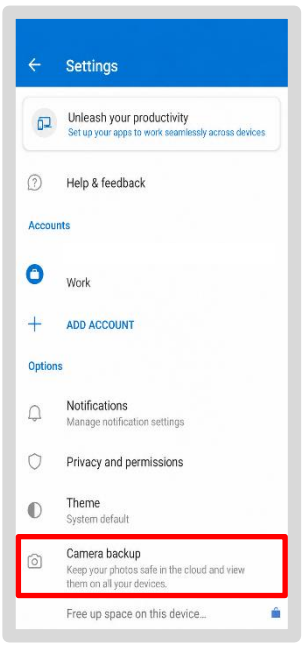
8.3 Backing up photos

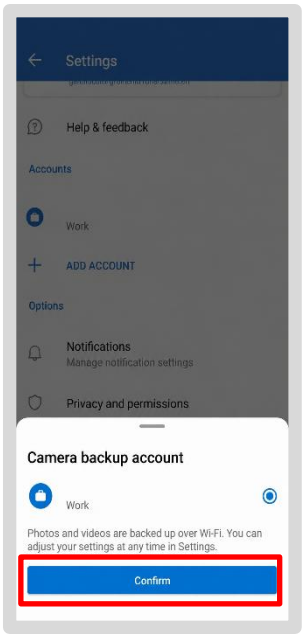
If you want to automatically save your photos to OneDrive, follow these steps:

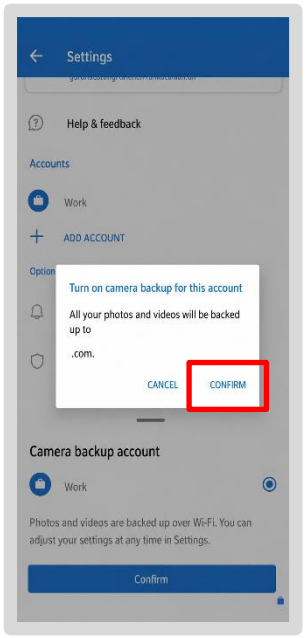
- Open the OneDrive app
- Tap the ‘Profile’ icon in the bottom right-hand corner, then select ‘Settings’
- Then select ‘Camera backup’
- Then tap ‘Confirm’ twice









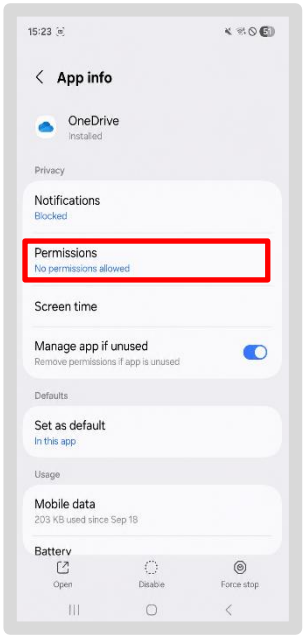


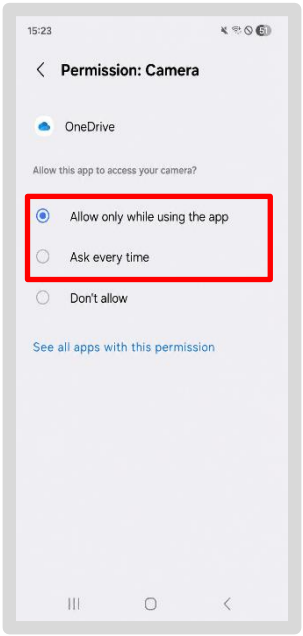
In the next step, you’ll need to grant OneDrive permission to access your photos and camera. To do this:

- An error message will appear stating that OneDrive lacks the necessary permissions
- Tap the ‘Adjust settings’ button on the right
- You’ll then be taken to the app permissions settings

If no error message appears, or if you’ve closed it:

- Go to the ‘Apps’ section under ‘Settings’
- Then, under ‘Work’, select the OneDrive app
- Tap ‘Permissions’
- Tap ‘Camera’ once, then tap ‘Photos and videos’ to grant OneDrive the necessary permissions
- Decide for yourself whether you want OneDrive to ask you each time or whether you want to grant permanent access whilst using the app
- Once synchronisation has been set up, every photo taken with the camera will be synchronised with OneDrive



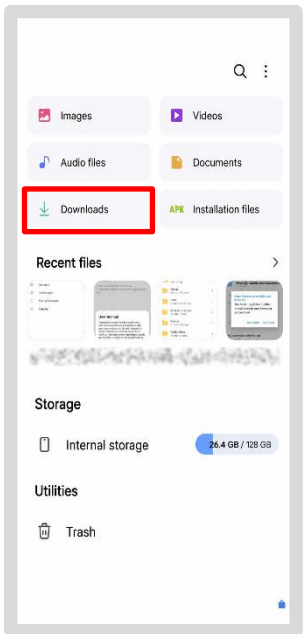


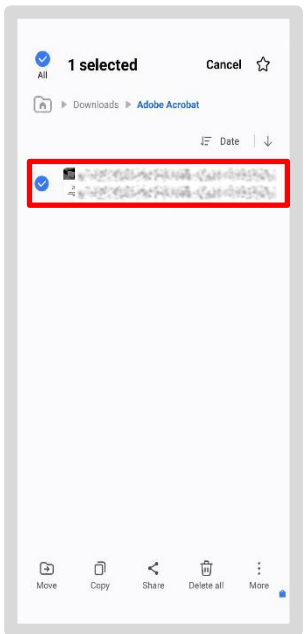
8.4 Backing up PDF files

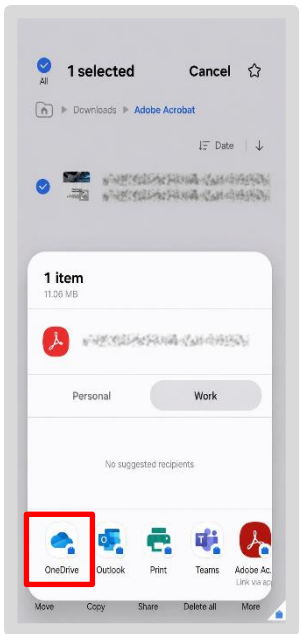
PDF files are usually saved to the Downloads folder in the ‘Work/Business’ section. To back them up to OneDrive, follow these steps:

- Open the Files app

- Tap ‘Downloads’
- Press and hold the PDF file until a tick appears next to its name
- Tap ‘Send’ at the bottom of the menu bar, then select ‘OneDrive’

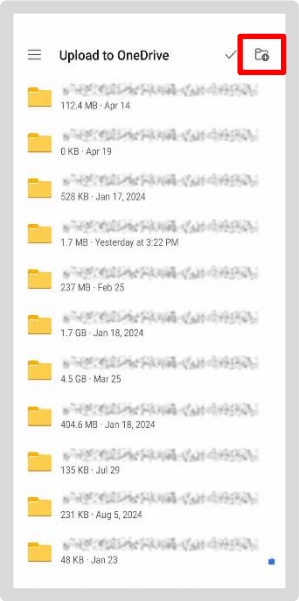






- Your personal folder in OneDrive will be displayed
- If this isn’t the right location: Tap the hamburger menu (three horizontal lines) in the top-left corner

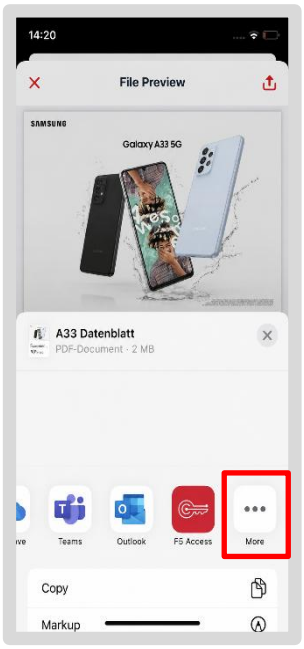
- Select the folder where you want to save the PDF file, then tap the white tick in the top right-hand corner
- The file will now be uploaded to OneDrive

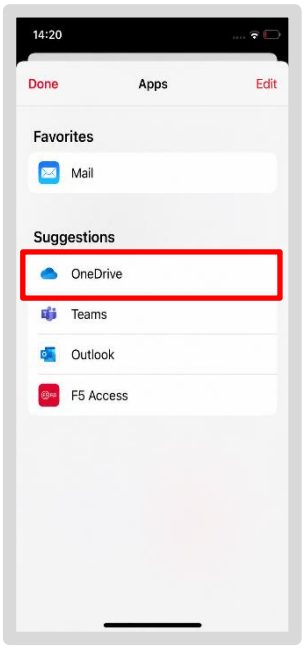


8.4.1 Save PDF files directly to OneDrive

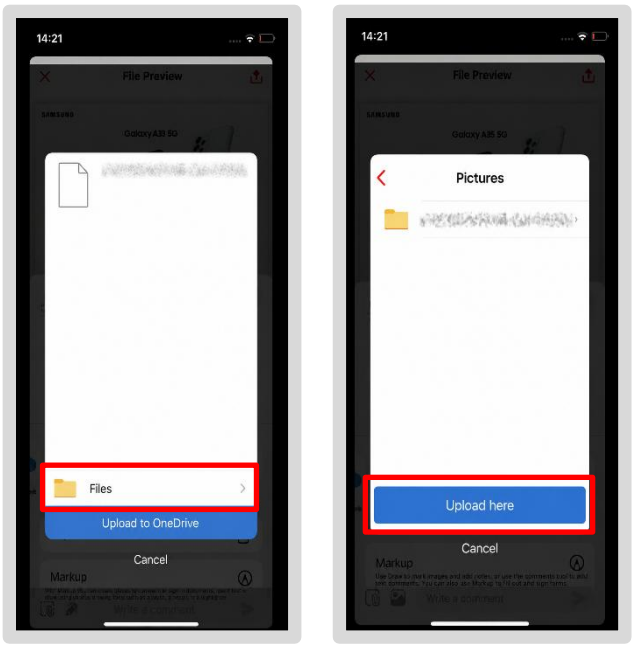
PDF files can be saved directly to OneDrive. Here's how:

- Open the file
- Tap the share icon in the top right-hand corner
- Select 'OneDrive' from the menu at the bottom (under the '...' dots)





- Select the folder where you want to save the PDF, then tap the white tick in the top right-hand corner

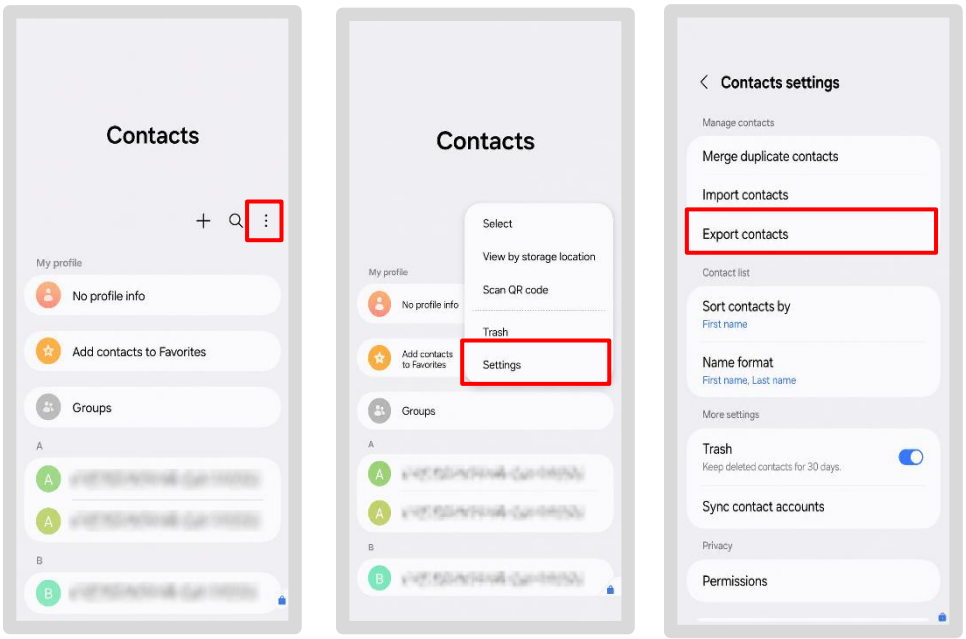


8.5 Backing up contacts to OneDrive

Want to switch to a new smartphone or tablet and take your contacts with you?

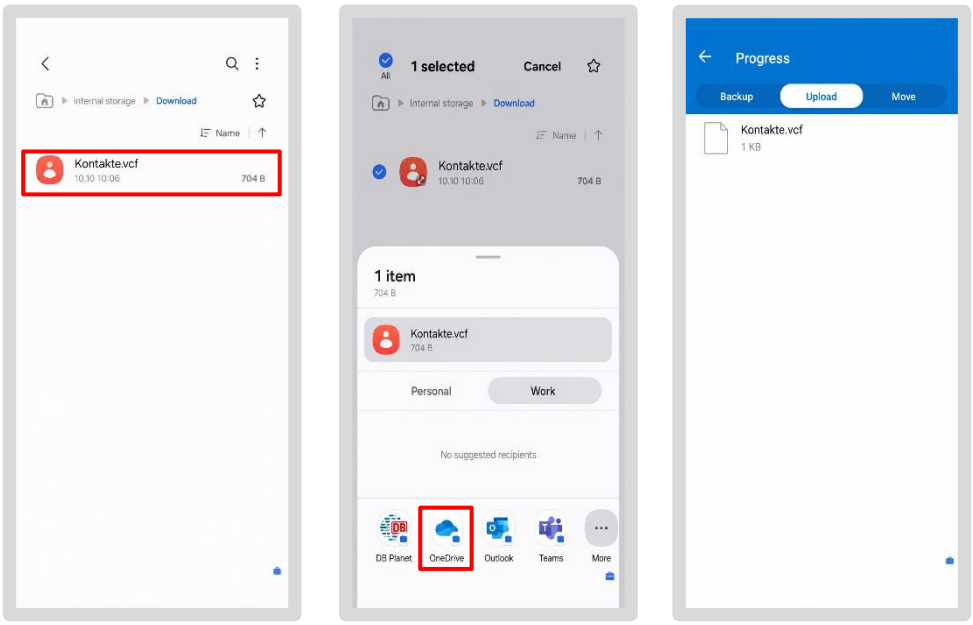
Then follow these steps:

- Open the Contacts app
- Tap ‘⋮’ (three-dot menu) in the top right-hand corner
- Select ‘Settings’
- Tap ‘Export contacts’
- First, save your contacts to ‘Internal storage’



You'll now find a .vcf file called "Contacts.vcf" in your Downloads folder.

- Select the "Contacts.vcf" file
- Tap 'OneDrive' at the bottom of the selection bar



Your contacts are now in your OneDrive folder.

8.6 Import contacts from OneDrive

To import your contacts back into the Contacts app on your new device, follow these steps:

- Swipe up on the home screen
- Tap 'Work' in the top right-hand corner
- Open the Contacts app

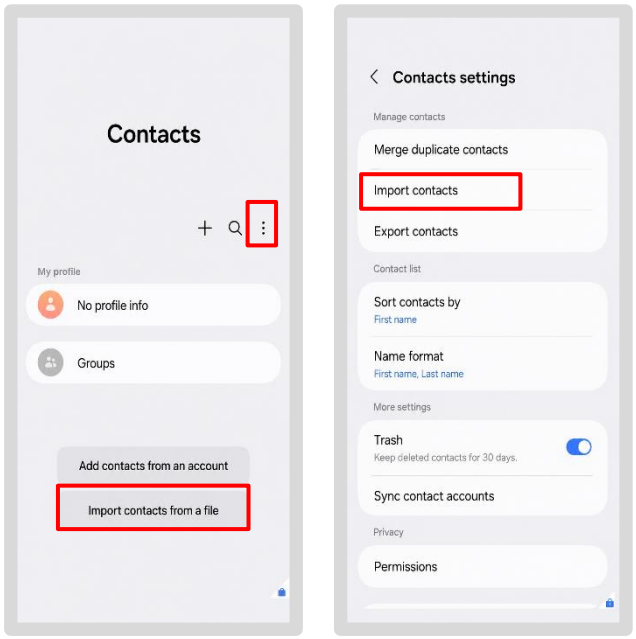
If you **don't** have **any new contacts** yet:

- Tap 'Import contacts from a file'
- Select 'Internal storage'
- Select the file "Contacts.vcf"
- Tap 'Phone (work profile)'
- Confirm by tapping "Import"

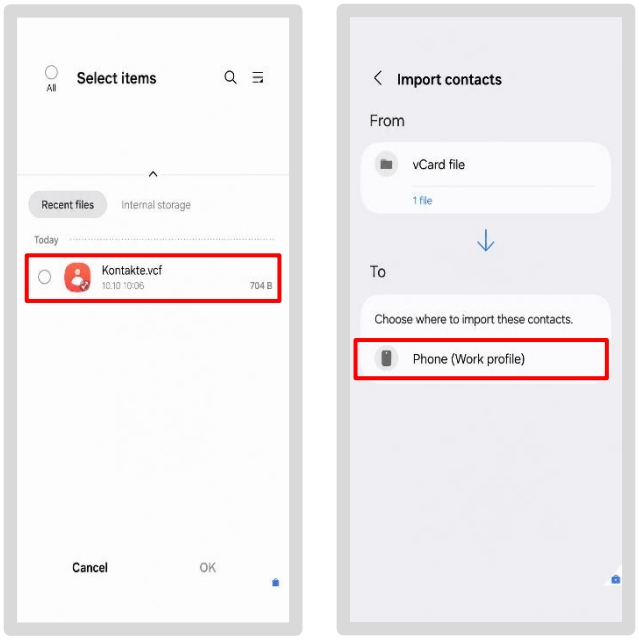
If you already have new contacts:

- Tap '⋮' (three-dot menu) in the top right-hand corner
- Select 'Settings'

- Tap on ‘Contact import’
- Select ‘Internal storage’

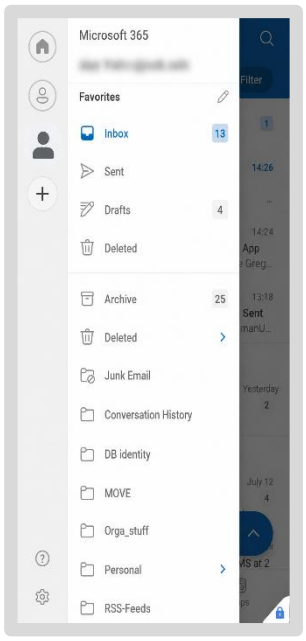


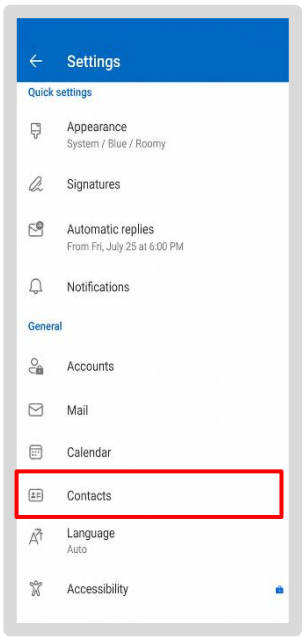
- Select the “Contacts.vcf” file
- Tap “Phone (Work profile)”
- Confirm by tapping ‘Import’

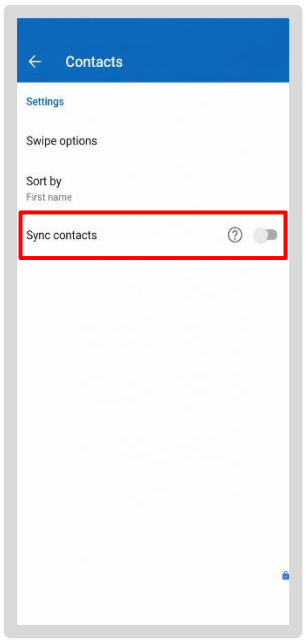


8.7 Backing up contacts via Outlook

- Always manage your contacts directly in Outlook **on every device**; that way, you'll have access to them from all your devices and won't need to back them up separately
- Tap the profile photo to the left of the word 'Inbox'
- Tap the settings icon in the grey area at the bottom, then tap 'Contacts' on the next screen
- Turn on the "Synchronise contacts" feature by tapping the slider







8.8 Backing up passwords

For smartphones and tablets running the Android operating system, the 'Keepass2Android' app is available. You can use it to store and access your passwords.

You can download the app from the work Google Play Store. You can find instructions on how to set up the app here:

> mobileworkplace.deutschebahn.com/Keepass2Android

8.9 Backing up personal data

If you have stored private photos, contacts, files and documents on your work smartphone or tablet, you must back these up yourself on a regular basis. This is because resetting your smartphone or tablet will also delete your private data.

To back up your personal data, you can, for example, use your **personal Google account or a personal OneDrive account**.

Instructions on how to back up your private documents or photos/videos can be found here:

> mobileworkplace.deutschebahn.com/mobile-daten-sichern

8.10 Take-Off: Where are your photos, files and documents?

- Your own work files are located in the ‘Work/Business’ section of the My Files app
- To back up work documents, you can use the OneDrive app, which you can open via the Intune app
- OneDrive will ask for your work email address; just enter it and your account will be activated straight away! To do this, you’ll need to have the *Outlook app* installed and your user account (email linked to a certificate) set up
- If you’re not yet receiving work emails or haven’t set up an email account for Outlook, please do so here.

> See section 7.3.1 Setting up Outlook/Creating an email account

Backing up PDF documents or Word files:

- Go to Documents or Downloads
- Press and hold a file until a tick mark appears
- Select the file(s) you wish to upload
- Tap ‘Send’
- Select ‘OneDrive’
- You’ll be taken to a view of all your folders
- Select a folder and tap the tick to upload the file
- Can’t see the folder? Tap the menu in the top left-hand corner
- Under ‘Libraries’, select additional folders and tap the tick to upload the file

Backing up photos and videos:

- Open ‘OneDrive’
- Tap ‘Photos’
- Enable Camera Backup/Camera Sync
- Then tap ‘Confirm’

9 Privacy and Terms of Use

If you use a DB smartphone or tablet whilst travelling, there is always a security risk that unauthorised persons may gain access to your device. Even brief access provides plenty of opportunities to access sensitive data.

Therefore, please follow these basic rules:

1. Do not simply leave your smartphone or tablet lying around; always ensure it remains within your sight.
2. Do not hand your smartphone or tablet to other people, not even to “just have a quick look”, unless it is a shared device.
3. Always secure your smartphone or tablet with a PIN or a strong password, and even better, with additional biometric security such as your fingerprint or facial recognition.
4. Only ever use passwords and PINs once!
5. Passwords and PINs should not be easy to guess; so do not use phone numbers, birthdays, car registration numbers or names.
6. A PIN must be at least 6 digits long, contain at least 4 different characters and must not consist of an ascending or descending sequence of digits.
7. Passwords must always be at least 12 characters long and must include at least 3 out of the following 4 elements: uppercase letters, lowercase letters, a number and a special character.
8. Never store passwords, PINs or usernames for your smartphone/tablet or DB User account on the device itself. Not even disguised as a phone number – everyone knows that trick.
9. Back up your work and personal data promptly and regularly. You can do this by saving them to your OneDrive or by emailing them as soon as possible to the intended recipient. Only then are they properly secured. This ensures that DB-IT can access them should your device break or go missing.

Terms of Use for ‘Mobile Data Communication’

By accepting the smartphone/tablet and these Terms of Use, the employee confirms compliance with the Terms of Use:

1. Mobile devices are personal work equipment. Passing the device or the access details/passwords/PINs on to third parties (e.g. family members or line managers) is not permitted.
2. The mobile device remains the property of DB Systel for the entire duration of its use. The device must be returned at the end of its useful life. It must at all times be free from any third-party rights; in particular, lending or selling it to third parties is not permitted.
3. The consumption, use and dissemination of offensive, defamatory, pornographic, sexist, racist, anti-constitutional, immoral or criminal content and applications are prohibited.
4. The device must be treated with care and respect. The device may only be charged using chargers and cables provided by the manufacturer (included in the scope of delivery). Charging during working hours is permitted.

5. Any loss, theft or damage that impairs the device’s functionality must be reported to your line manager immediately.*
6. Where the employer has Wi-Fi networks available and these can be used, data usage on the mobile device should primarily take place via these networks.
7. The device’s security settings (policies, antivirus software, device configuration, etc.) must not be altered or disabled.

[1] See also Annex 1 to the KBV IT General and Special Terms of Use, A (1).

[2] See also DB’s Asset Protection Policy, 136.01.03

9.1 Take-Off: Safety aspects

Your work smartphone/tablet is part of your job. It is the property of DB Systel GmbH and must therefore be treated with care.

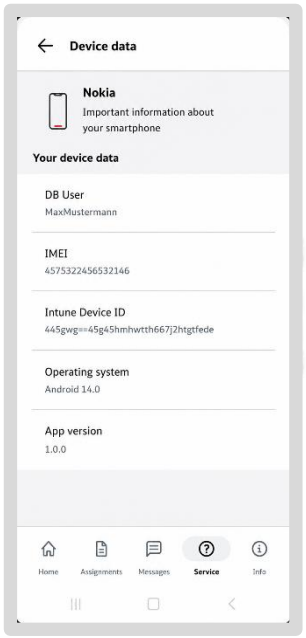
It is part of your job, so do not lend it out or sell it.

> If the smartphone/tablet needs to be returned for security reasons, please return it as described here

Don't give thieves a chance: use a strong password. For example, do not stick a note with your password on your monitor.

Data protection: Where can I find the details for my smartphone/tablet?

To do this, open the *Welcome app*, use the tabs at the bottom of the screen to go to the 'Help' tab and then select the 'Device details' sub-item. Here you'll see your smartphone/tablet's details, such as the serial number, IMEI or operating system version (e.g. Android 13 or iOS 17.5.1).



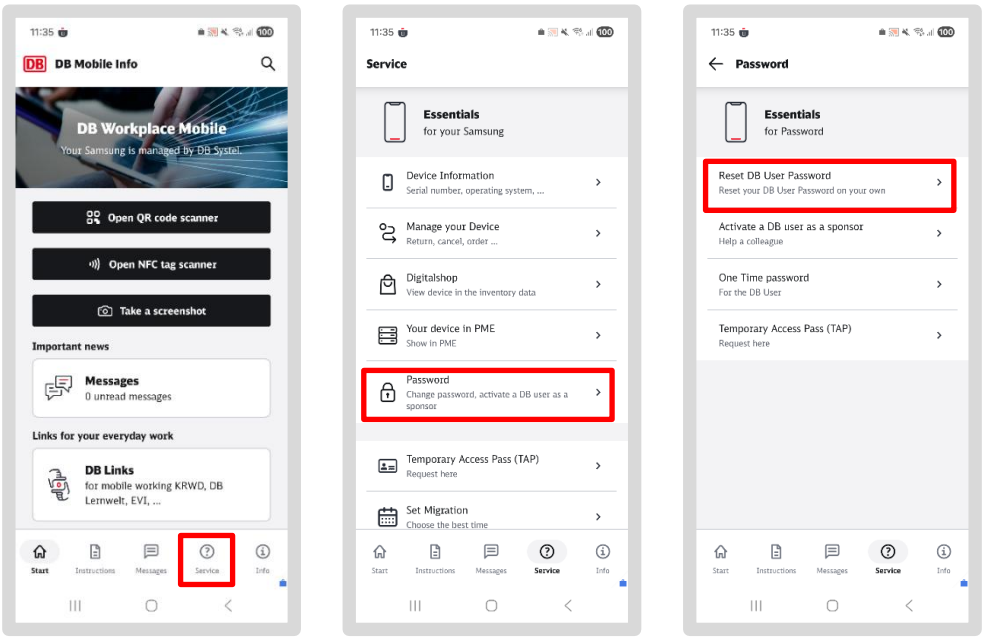
10 Forgotten your password, returning your device

Have you forgotten your screen lock password or can't remember your DB User password? Does Outlook keep crashing? Are you getting error messages you don't understand? Don't worry – you'll find help here.

10.1 Forgotten or changing your DB User password

If you've forgotten your DB User login details or want to change them, here's what to do:

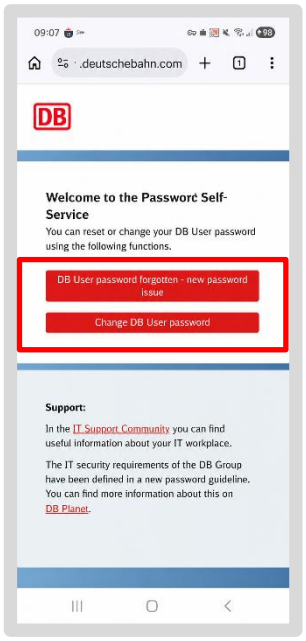
- In the *DB Mobile Info* app, select the 'Service' tab
- Tap 'Passwords'
- Then tap 'Reset DB User password'

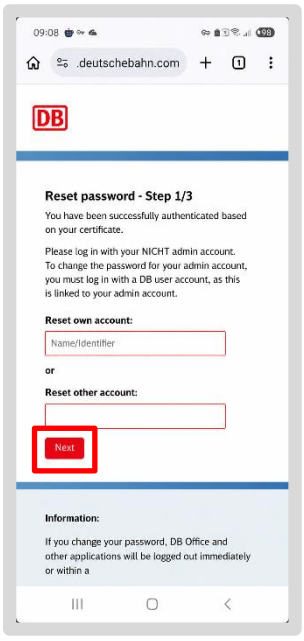


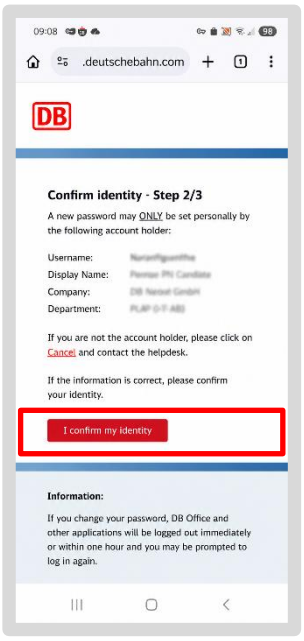
Please note: A connection to F5 Access will be established automatically at this point. This is necessary to carry out the following steps. If a connection to F5 Access has not been established, you must activate it manually to continue!

If you have done everything correctly, you will now be redirected to the password self-service website.

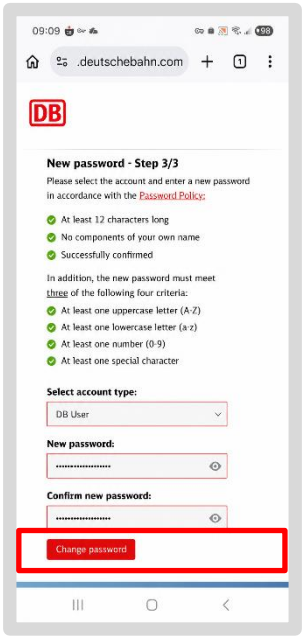
- Now select the button that applies to you
- Tap ‘Next’ without entering anything
- Then confirm your identity







- Now enter your new password, ensuring it complies with the password policy
- Confirm your entry by tapping ‘Change password’

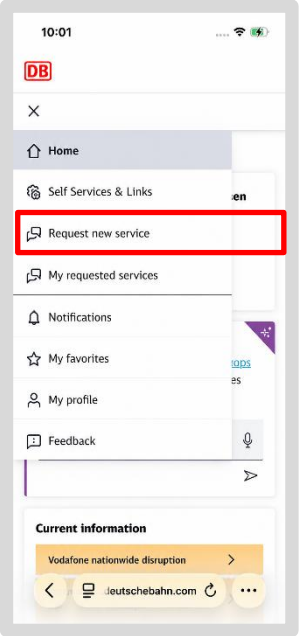


10.2 Help via the IT ServiceDesk app

The IT ServiceDesk app is the central technical point of contact for queries. From fault diagnosis to technical support for hardware and software issues on your device – here you can ask your questions and gain access to helpful guides and important links.

Here's how to access the IT ServiceDesk app:

- Open the *IT ServiceDesk app* in the 'Work/Business' section
- Or access it via the link: db.de/itservicedesk
- You'll find the menu in the top-left corner of the app
- Click on 'New Service Request' and then select the method you'd like to use to submit your request



You can also do the following in the IT ServiceDesk app under 'Self Services & Links':

- Update your DB user password
- Change or delete your DB user mobile number

10.3 Lost your smartphone or tablet?

Call the **IT ServiceDesk** immediately:

- IT ServiceDesk
  - Internal: Tel. 91-5555
  - External: Tel. 0361 430 8200
- IT ServiceDesk DB Cargo
  - Tel. 91 7777 (internal)
  - Tel. 00800 327 978 35 (external)
- Report the loss or theft

Notify your mobile phone administrator immediately:

- Report the loss or theft
- Ask them to have your SIM card blocked! That way, no one will be able to make calls at the company's expense
- Discuss the next steps with them to find out how to get a new smartphone or tablet

Report the loss via the Digitalshop:

- Report a loss or theft via the Digitalshop
- Open the Digitalshop at http://www.db.de/digitalshop
- In the main menu, under 'Inventory data', tap on 'Mobile devices'
- Select your smartphone or tablet from the list
- Tap 'Perform inventory action' on the left, then select 'Theft of mobile device' or 'Loss of mobile device' from the drop-down menu
- If you have any questions, please contact your mobile phone administrator!

10.4 Faulty smartphone/tablet

Inform your mobile phone administrator immediately:

- Report the total loss
- Discuss the next steps with them to find out how to get a new smartphone/tablet

De-register the smartphone/tablet in the Digitalshop:

- Open the digital shop at http://www.db.de/digitalshop
- In the main menu, under 'Inventory Data', tap 'Mobile Devices'
- Select your smartphone or tablet from the list
- Tap 'Perform inventory action' on the left, then select 'Mobile device – Cancel subscription' from the drop-down menu
- You can find instructions on how to replace your device at db.de/mobile-setup
- If you have any questions, please contact your mobile phone administrator!

10.5 Returning your smartphone or tablet?

If your smartphone/tablet is faulty, you'll find a quick guide to replacing smartphones/tablets atdb.de/ae under 'Set-up/Quick Guides'.

Important: Back up your data beforehand. This is because your smartphone/tablet will be completely wiped by the recycling company after you return it. As a result, all data (work-related and personal) will be lost.

You can back up your work data to OneDrive. This stores the data in the cloud, allowing you to access it at any time from any of your devices (smartphone/tablet/PC).

> We show you how to set up OneDrive in Chapter 8.2 'Setting up OneDrive' (OneDrive) or at mobileworkplace.deutschebahn.com/mobile-daten-sichern.

Log out of your smartphone/tablet in the Digitalshop:

- Open the Digitalshop at http://www.db.de/digitalshop
- In the main menu, under 'Inventory data', tap 'Mobile devices'
- Select your smartphone/tablet from the list
- Tap 'Perform inventory action' on the left, then select 'Mobile device – Deregister' from the drop-down menu
- You can find instructions on how to exchange your device at db.de/mobile-setup
- If you have any questions, please contact your mobile phone administrator!

Simply return your smartphone or tablet yourself via the IT Asset Management Portal:

- Log in to the http://www.db.de/itverwertung
- Order a free return
- When doing so, choose whether you only need the return label for the return or would also like a box sent to you
- You'll receive the label by email and the box will be delivered by post to the address you've provided

Prepare your smartphone or tablet for dispatch:

- Delete any personal accounts from your smartphone/tablet
- Remove your SIM card and memory cards
- Pack your smartphone/tablet securely so that it isn't damaged in transit, and include any accessories (power adaptor, USB charging cable, etc.) in the return box
- Stick the return label onto the box and take it to the post office

Congratulations!

You have successfully set up your work smartphone/tablet!

To ensure it always works reliably in future, make sure you install the latest updates! We hope you enjoy using it!

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

> You can find a brief guide to backing up your data at mobileworkplace.deutschebahn.com/mobile-daten-sichern