DB

#Mobile Workplace -
The mobile workplace for smartphone & tablet!

DB Systel
Digital bewegen. Gemeinsam.

Table of contents

1 Welcome to the DB world: Enter the digital DB world!

Glad you decided to go with a DB smartphone/tablet!

With this guide, we'll help you get set up and give you an overview of all the topics related to your smartphone/tablet to get you started.

The most important app for the initial setup is the **Welcome App!** There you will find all the important information about your smartphone/tablet, for example:

- ▮ How to set up and restore your smartphone/tablet for the first time
- ▮ Information about your device
- ▮ Useful links for working in the DB world
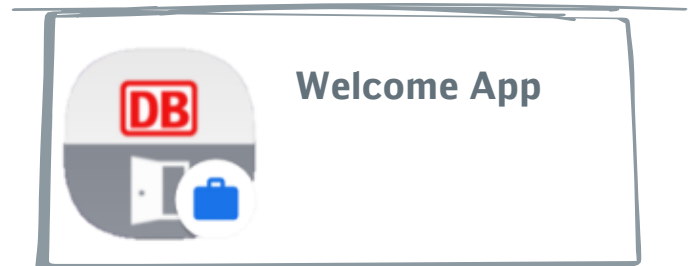
So check it out and keep up to date!

Note: If your smartphone/tablet is not yet set up, ask a colleague to open the Welcome App on their device.

2 First steps

Have you received your new smartphone/tablet? First check whether your name is on the package and that you have received the correct package. Compare the order - if the allocation is not correct, ask your mobile phone manager.

Do you have everything?

- ❚ Smartphone or tablet
- ❚ SIM card letter (sent by Vodafone, ask your mobile phone manager if necessary)
- ❚ Instructions, warranty card, handover document, terms of use and the tool for inserting the SIM card
- ❚ If ordered: Accessories such as charging cable, protective cover and powerbank

The first steps - We help!

Together with your smartphone/tablet you will receive a printed flyer. This will help you with the initial set-up! Further information is also available here: **>** http://www.db.de/ae.
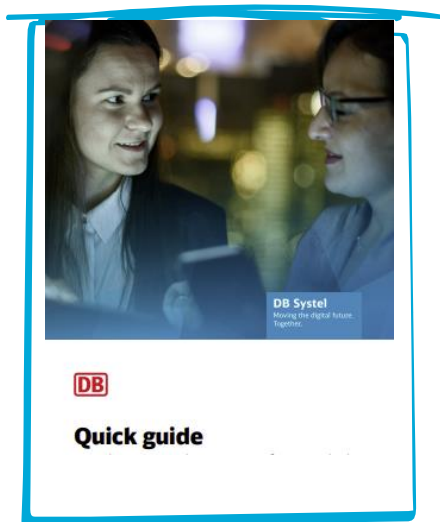
- ❚ **>** db.de/mobile-setup
- ❚ **>** db.de/mobile-restore

Here we go
Since the setup of your smartphone/tablet differs slightly depending on the model, we have described the initial setup separately in the next part.

Choose the instruction that suits you:

- ❚ Samsung/Nokia/Gigaset (p. 7)
- ❚ iPhone/iPad (p.14)

3 Requirements for the initial setup

3.1 DB User - the user account at DB

An activated DB user is required to set up your smartphone/tablet.
The DB User provides free access to many Group applications.

What is the DB User?

The DB User is the user account for all employees in the DB Group. It consists of a self-selected password and an automatically generated login name. You will receive the login name after successfully activating your DB User account.

How do I activate the DB User?

The DB User is activated once **together with a sponsor.** At the same time, you set a password. You can see how this works and who your sponsor is here:
> https://db-planet.deutschebahn.com/pages/db-user/apps/content/konto-aktivierung

After successful activation, you will receive a PDF document with your DB User login name.

How do I change my DB User password?

If you don't remember your password, you can change it **>** here. Or follow the instructions on **page 49**.

4 Initial Setup Samsung/Nokia/Gigaset

4.1 Insert SIM card

There is a small pocket on the top or side of your smartphone/tablet.

- Open the compartment with the tool. You will find it in the packaging of your device.
- Pull out the card holder and insert the SIM card.
- Put the card holder back into the smartphone/tablet.

Gigaset:
- Open the back of your device.
- Then insert the SIM card in the top right-hand corner.

4.2 Switch on

Connect your smartphone/tablet to the power supply using the power supply unit.
- Press the "on" button.
- When the device has booted up, it will ask you for a PIN. This is the PIN for the SIM card you just inserted into the device.
-

You can get the PIN like this:
- Open your SIM card letter from Vodafone.
- Pull off the foil. Underneath is a PIN and a SuperPIN.
- Enter the PIN in the input field of your smartphone/tablet and confirm with "OK".

The SIM PIN always remains the same. Keep the Vodafone SIM card letter with the SIM PIN and the Super PIN in a safe place.
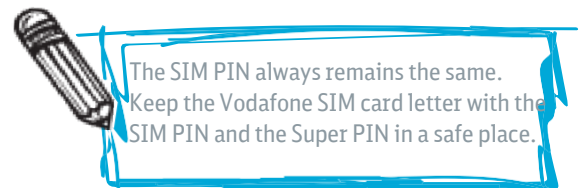
4.3 Unlock

Next, unlock the smartphone/tablet:
- Swipe your finger once across the screen.
- Enter the following password: DB-Device2019
- Confirm the entry, you will now see the start screen of your smartphone/tablet.

Attention: Hurry up when entering the password, otherwise the screen will switch off after a short time.

4.4 Change screen lock

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

In the next step, change the screen lock and set a new password or number combination. Pay attention to the data protection and usage information in chapter 8.

In addition, a so-called "**biometric security**" can be set up. This unlocks the smartphone/tablet by fingerprint or facial recognition.

Passwords must have at least 12 characters and contain at least 3 out of 4 of the following: Upper case letters, lower case letters, numbers, special characters.

A **PIN** must have at least 6 digits long and must not represent an ascending or descending sequence of digits.

In the next section, we will show you how to set up the screen lock, first for the smartphone and then for the tablet.

Samsung/ Nokia Smartphone
▌ Go to the "Settings" area.
▌ Tap on the "Settings" app in the "Personal"/"Private" section.
▌ Or swipe your finger once from the top edge of the screen downwards. A bar with symbols opens.
▌ Tap the cogwheel at the top right.
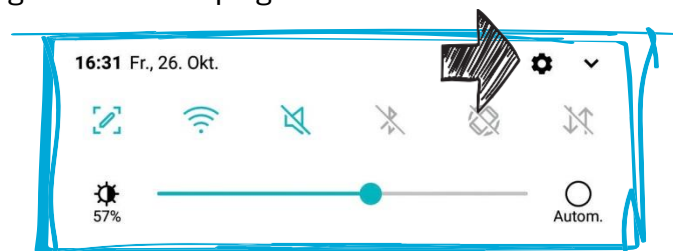
▌ You see a menu with different choices.
▌ Tap "Lock screen" and select "Lock screen type".
▌ Enter your current screen lock. This is the password from step Unlock 4.3 (DB-Device2019) the first time.
▌ Select "PIN" or "Password".
▌ Enter a new password or PIN. Remember it well!

▌ If you want to set up biometric security:
▌ Under "Biometric data", select "Fingerprints" or "Face".
▌ Scan your fingerprint or face. Follow the instructions displayed on the screen.

Gigaset Smartphone & all Tablets
▌ Go to the "Settings" app in the "Personal"/"Private" section.
▌ Tap on "Security" and then on "Screen lock".
▌ First enter your current device password. This is the password from step 3 (DB-Device2019) the first time.
▌ Select "No, thank you" in the following selection and tap on "Next".
▌ Enter a new password or PIN. Remember it well!

If you want to set up biometric security:

▋ Tap on "Biometric data and security":
▋ Select the "Face recognition" field here.
▋ Enter your current device password/PIN.
▋ Follow the instructions. The device will now scan your face (note: if you wear glasses, you must remove them during the scanning process).
▋ When face recognition is set up, a notification appears.
▋ Confirm the message "Quick face recognition" with "OK".

4.5 Notes for the daily switch-on

When switching your smartphone/tablet on and off, you must always do the following in future:

▋ Unblock the SIM card with the SIM PIN from the SIM card letter from Vodafone.
▋ Unlock the smartphone/tablet with your personal password/PIN. Or the device recognises you via your fingerprint/face.
▋

If you have already switched on the device, unlock it in between using only your fingerprint or facial recognition.

4.6 Activate

To use all DB apps, first activate your smartphone/tablet via the **Welcome app.** You only have to do this once.

Important: To activate a tablet, first establish a VPN connection. We show how to do this in **chapter 7.5.**

To activate the Welcome App, proceed as follows:

▋ To do this, go to the home screen and swipe upwards with your finger.
▋ Tap "Work/Business" at the bottom right or top right.
▋ Tap on the "Welcome App".
▋ Confirm the following messages with "Next" and "Start".
▋ Tap on "Start activation".
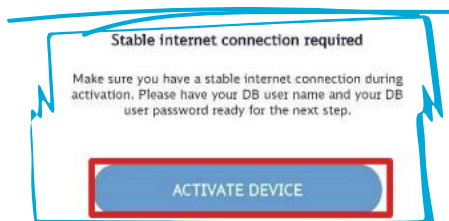
▋ Enter your DB User login details. This is your DB user login name and your DB user password.
▋ Forgotten your password? Change it **>** Password Self-Service.
▋ Enter both in the two empty fields and tap on "Log in".

Wait about 30 minutes.
Note: Sometimes it takes a little longer or a very long time to activate your smartphone/tablet. Be patient here.
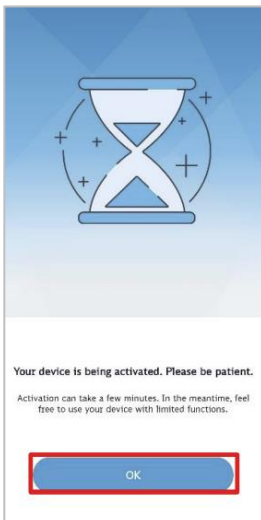
Your device is activated!
Congratulations! You can see that the activation was successful by the message in the "**Info**" tab in the Welcome app and by the fact that DB apps are visible on your device.

If the following message appears, the activation was successful. You can exit the app.
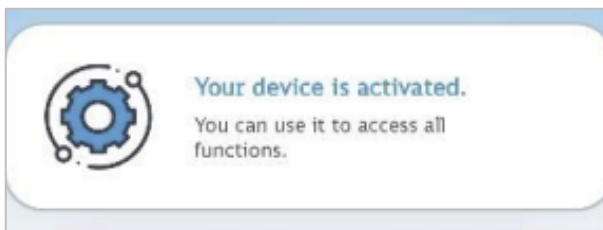
Activation failed?
- Activate the device again.
- To do this, go to the Welcome App and select the "Help" tab at the bottom right.
- Then tap on "Activate the terminal again".
- Only then can you download and work with all other necessary DB apps.

4.7 Activate MTD App

The Mobile Threat Defence (MTD) app is automatically installed on your smartphone/tablet after recovery. To enable it to detect security vulnerabilities on your device, proceed as follows:
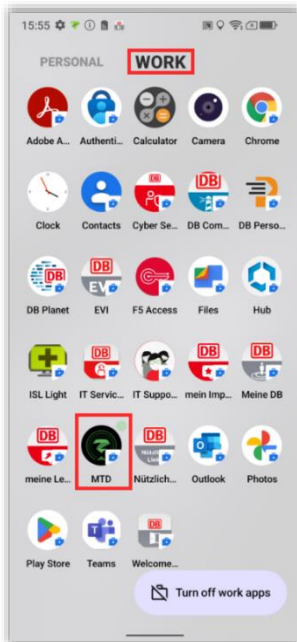
■ Tap the app icon in the "Work"/"Business" area.
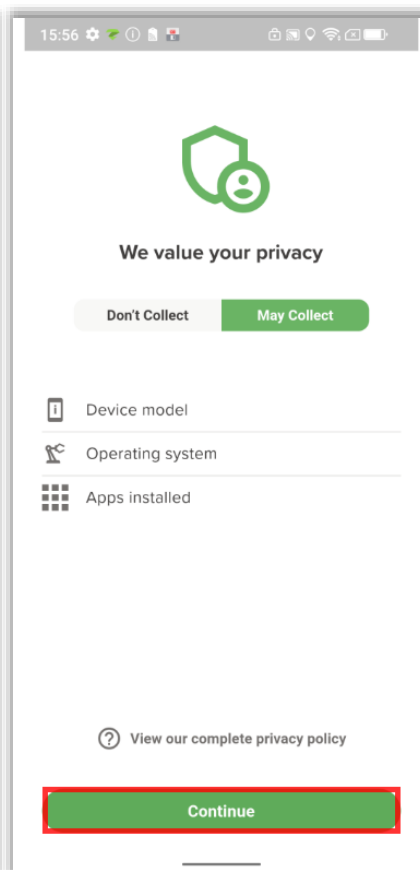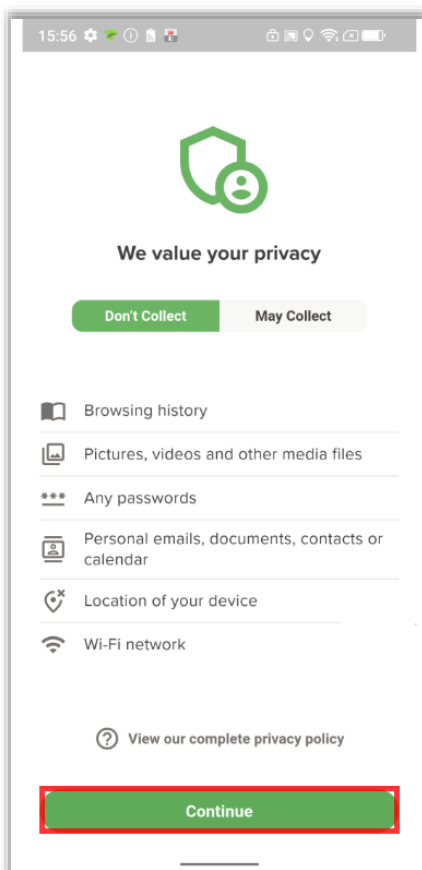
You will now see the "Privacy" settings. This screen is for information only. No action is required by you.

▊ **Don't Collect:** Here you can see which data the MTD app is not allowed to collect.

▊ **May Collect:** Here you can see what data the MTD app is allowed to collect.

▊ Tap "*Continue*".
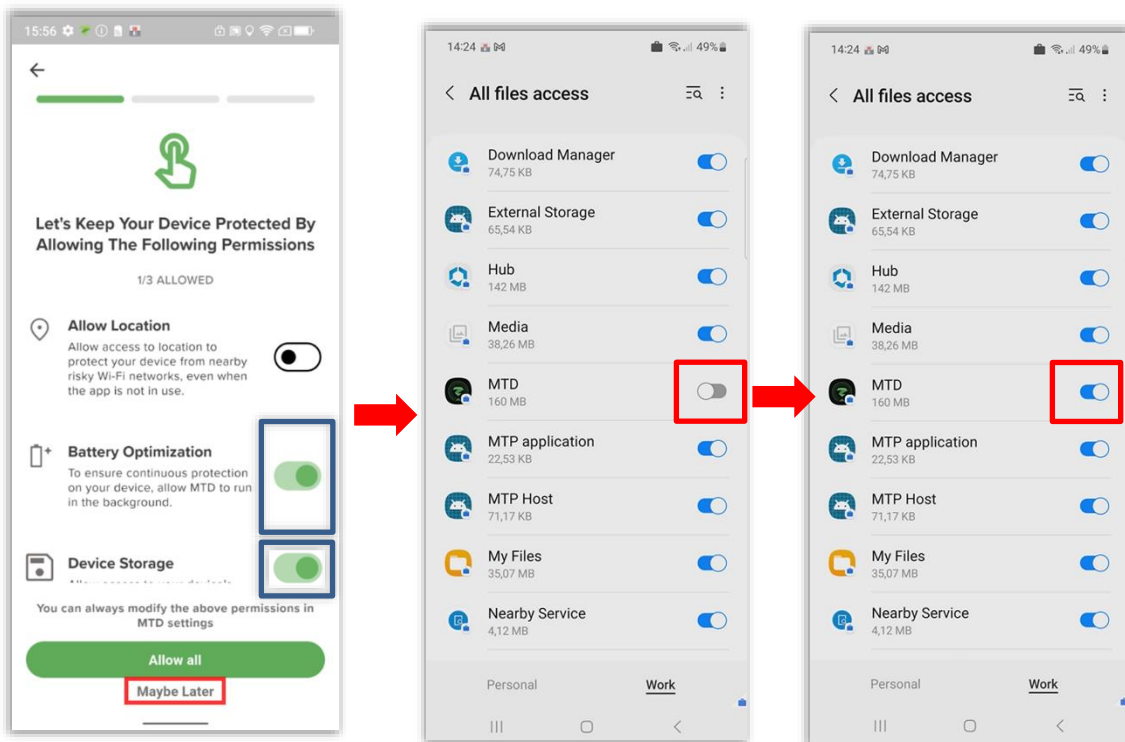
In the next step, you will be asked to set up some permissions for the MTD app.

▊ **Allow Location:** Leave slider to left (not activated).

▊ **Battery Optimisation:** Move slider to right (activated).

    o This option is **mandatory** for the MTD app to provide continuous protection in the background. The tested Battery consumption is minimal.

▊ **Device Storage:** Move slider to right (activated).

    o This option is **mandatory** for the MTD app for the detection of Malware which could spread on your device. This is the only way to provide a thorough protection.

▊ Then tap **"Maybe Later"**

You will now see the following screen:
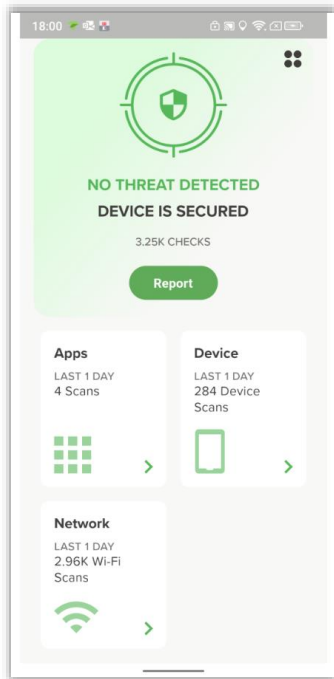
▌ The activation is now complete. The MTD app will now detect threats on your smartphone/tablet.

▌ Detailed step-by-step instructions: **>** Setup MTD.

▌ More information about MTD on the DB Planet page of **>** Endpoint Security.

5 Initial Setup iPhone/iPad

5.1 Switch on

Connect your iPhone/iPad to the power supply.
- ❚ Press the On button.
- ❚ After a short moment, the iOS setup wizard starts and "Hello" appears on the screen.
- ❚ Swipe your finger upwards across the screen to start.
- ❚ Select a language and the country.
- ❚ Tap on "Configure manually".
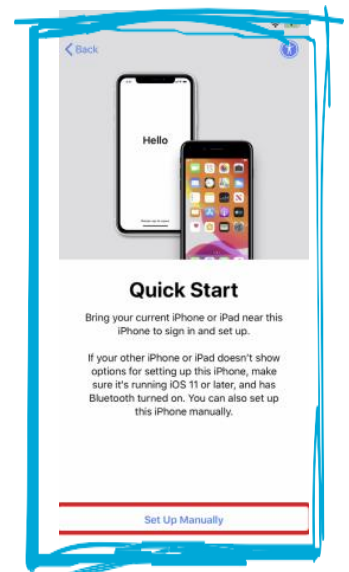
5.2 DB User

Connect to the Internet:
- ❚ Select a WLAN for this. If you are in a DB building, select "dbs4public".
- ❚ To use the WLAN, enter your DB User login data for authentication. These are your DB User login name and your DB User password.
  On **page 6** we explain what the DB User is and how to activate it.
- ❚ Forgotten your password? Change it here: Password Self-Service
- ❚ Enter both in the two empty fields.
- ❚ The unit is now activated and managed remotely.
- ❚ In the next step, tap on "Next":
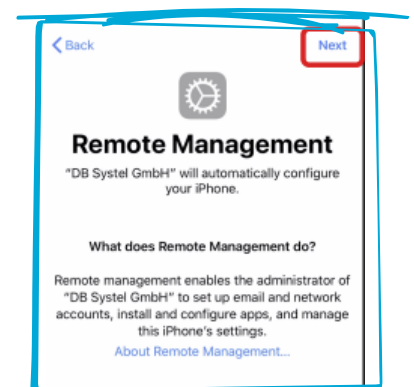
- ❚ Select the login method. To do this, tap on the small red arrow pointing downwards and select "Login data and SMS one-time password" as the login method.
- ❚ Enter your DB user login details:

5.3 SMS one-time password received

In the next step, you will be asked to enter the one-time SMS password. This has been sent to the mobile phone number associated with your DB User. To retrieve the one-time SMS password, proceed as follows:

- ❚ Insert your SIM card into another smartphone. Use your old or private device or that of a colleague.
- ❚ You will receive the one-time password by SMS.
- ❚ Enter the SMS one-time password into your new iPhone/iPad and tap "Sign in".
- ❚ The iPhone/iPad is now configured.

   Note: To receive the SMS, your mobile phone number must be linked to your DB user. You can check whether the correct mobile phone number is stored here and change it if necessary: **>** https://itsdapp.extranet.deutschebahn.com/selfservice/dbUserPhone/logIn

- ❚ If the link does not work on your iPhone/iPad, try it on a colleague's device.

If the correct mobile phone number is stored and you still do not receive a password via SMS, you probably entered your login data incorrectly in the *DB User* step (Chapter 5.2). Then go back to *DB User* (Chapter 5.2) and try again.

5.4 Insert SIM card

Take the SIM card from the other (old) smartphone and insert it into your new iPhone/iPad. Proceed as follows:

- ❚ At the top or side of your device is a small compartment that you open with the tool provided.
- ❚ Insert the SIM card there.

5.5 Create screen lock

The screen lock is the code you will use to unlock your iPhone/iPad in the future. You will now be asked to secure your iPhone/iPad. Think of a new six-digit code for it.

- ❚ Type the code twice in succession.
- ❚ Tap on "Next".
- ❚ In future, always use this personal code when switching on and unlocking your iPhone/iPad.

After activating the iPhone/iPad, set up unlocking with FaceID if required:

- ❚ Tap on "Settings" and select "FaceID & Code".
- ❚ Enter your personal code.
- ❚ Tap "Add FaceID" and follow the on-screen instructions.

5.6 Activate location services

In the next step, activate the location services. This is necessary so that the exact time is displayed on the iPhone/iPad. Tap on "Activate location services".

You can set the location services separately for each app after completing the installation!
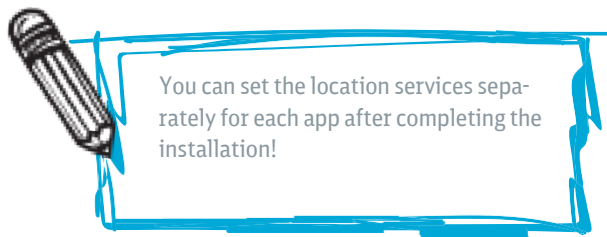
5.7 Check for Update

In the next step, check whether an iOS operating system update is available.
- ❚ Open the "Settings App".
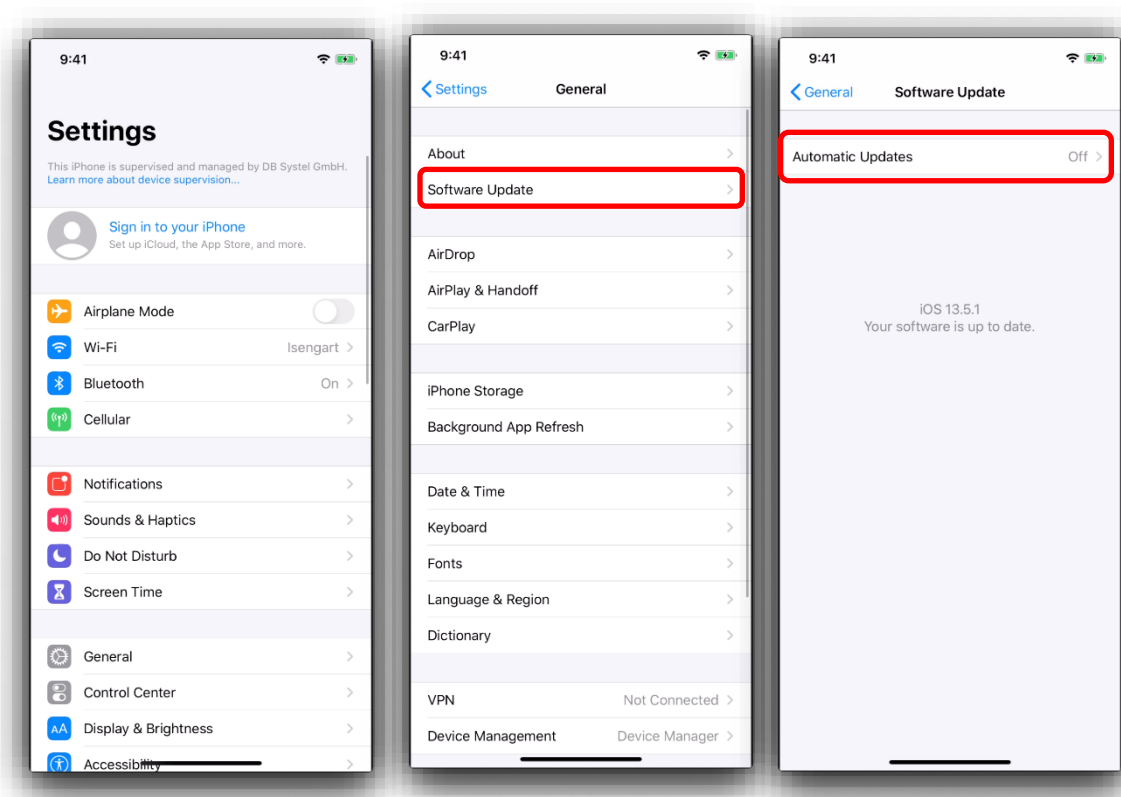
- ❚ Tap on "*General*".
- ❚ Then tap on "*Software updates*". If a new software version is displayed here, install it.
- ❚ To keep your iPhone/iPad up to date, activate the "automatic updates" function.

5.8 Activate

To use all DB apps, first activate your smartphone/tablet via the **Welcome app.** You only need to do this once.
Proceed like this:

- ▮ Open the Hub app. It is installed on your iPhone/iPad by default.

- ▮ Select "*I understand*" after reading the privacy policy.
- ▮ Tap "*Not now*" in the following queries.
- ▮ Tap "*Do not submit*" in the user experience prompt in the Data Sharing dialogue box.
- ▮ Give the Hub app permission to send you messages.
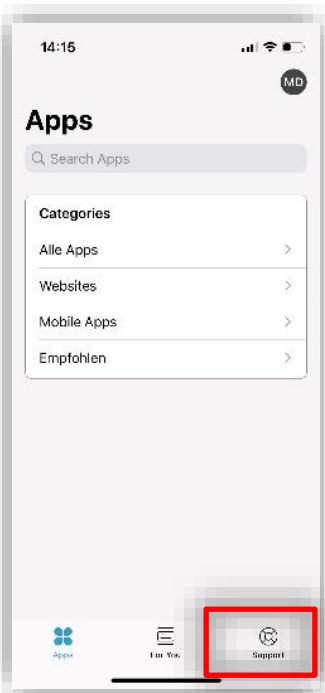
- The app overview is then displayed.
- To synchronise your device: Tap on "*Support*" at the bottom right of the menu bar.
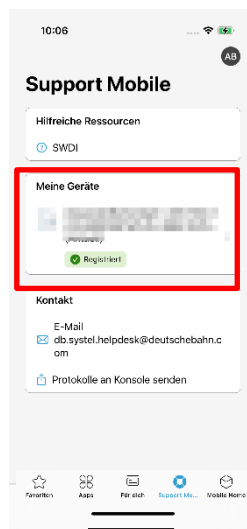
- Tap on your iPhone/iPad under "*My Devices*".
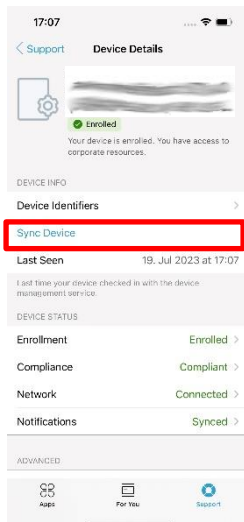
- Then tap on "Sync Device" to register your iPhone/iPad in the DB.

After activation, the device begins to install the corresponding apps. This process may **take a few minutes** as the installation depends on the network connection.

5.9 **Activate MTD App**

The Mobile Threat Defence (MTD) app is automatically installed on your iPhone/iPad after recovery. This enables it to detect security vulnerabilities on your device. Proceed as follows:
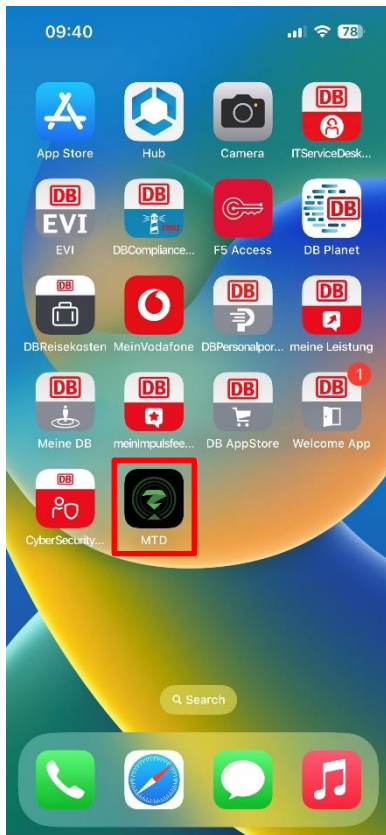
❚   Start the app by tapping on the app icon.
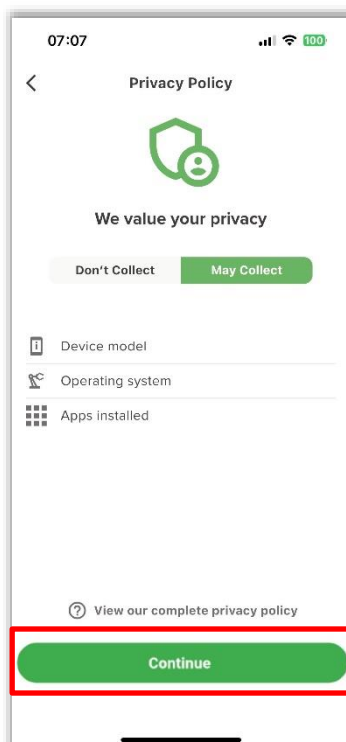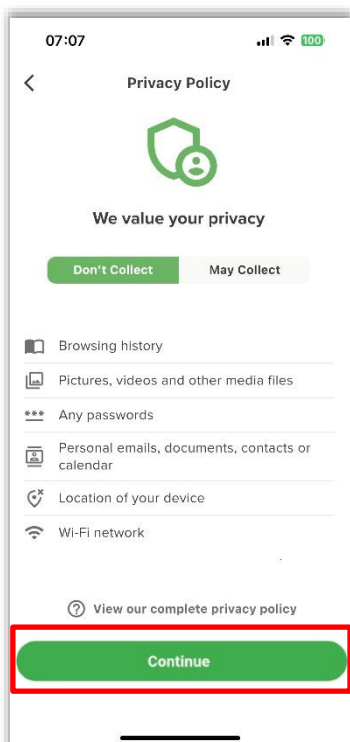
You will now see the "Privacy" settings. This screen is for your information only, you do not have to do anything here.

- **Collection not permitted:** Here you can see which data the MTD app is not allowed to collect.

- **Collecting allowed:** Here you can see what data the MTD app is allowed to collect.

- Tap on **"Continue"**.
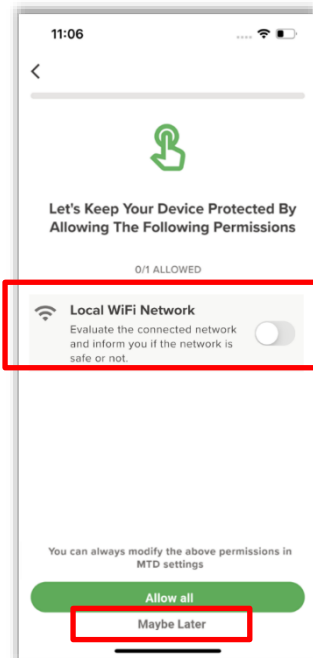
In the next step, you will be asked to set up some authorisations for the MTD app.

- **Local WLAN network:** Leave the slider on the left (deactivated).
- Then tap on "*Maybe late*r".

You will now see the following screen:
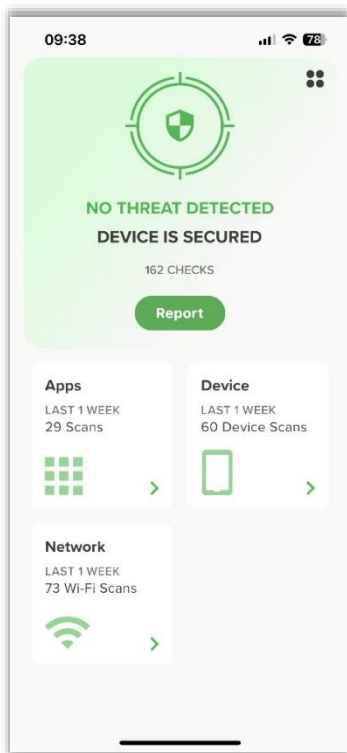
Activation is complete. The MTD app now recognises threats on your smartphone/tablet.

▐
▐ Detailed step-by-step instructions: **>** Setting up MTD
▐ More information about MTD on the DB Planet page of **>** Endpoint security.
▐

6 Official and private contents

These instructions are intended for all smartphone/tablet models. Therefore, we distinguish in some places between:

- Samsung/Nokia/Gigaset
- iPhone/iPad

The biggest difference is how private and business content is separated on the smartphone/tablet:

- With **Samsung/Nokia/Gigaset,** business content and apps are stored in a separate "Work/Business" area. You can recognise business apps by a suitcase icon on the app icon and a g 💼 suitcase icon at the top right of the battery icon.
- With **iPhone/iPad** there is no visible separation of business and private content. Therefore, observe a few rules (page 23).

In this guide, we have compiled some tips on the use of apps to ensure that business and private data do not get mixed up. Always follow the rule:

Use only official apps for official work!
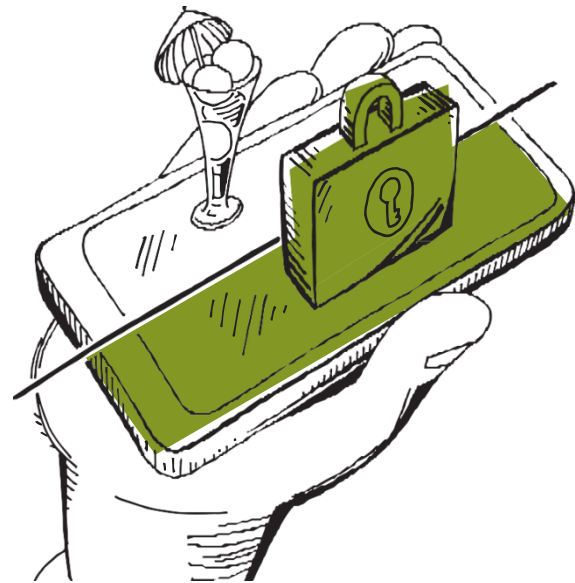
6.1 What is official and what is private?

It is **official use** when you
- start your service via an app
- or open the current duty roster

Private use is
- watch Netflix
- listen to Spotify
- create Google Account

Note: It is not always possible to make a clear distinction between business and private use. Therefore, always think carefully about the purpose for which you are using your smartphone/tablet.

Samsung/Nokia/Gigaset

This is how you switch to the "Work/Business" area:
- Swipe upwards with your finger on the home screen.
- Tap on "Work" or "Business" at the bottom right.
- You can now see all the apps that are in use.

The only exception: The phone app may be used for both business and private calls. For business calls, tap on your business "Contacts" app, select a business contact and tap on the handset icon.

iPhone/iPad

On your iPhone/iPad, private and business data are only separated in the background. There is **no visible separation of** business and private content. Therefore, when using apps, follow these instructions to avoid mixing business and private data:

E-mail: The "Outlook" app is used exclusively for business purposes. For private use, use other services such as Gmail, etc.

Messenger: Use the apps from the Hub app (e.g. Teams) for official communication. WhatsApp is not provided via the Hub app. Use it only for your private contacts.

Camera: For business photos, use the OneDrive app, which saves photos directly to OneDrive. The camera app is for private use only.

6.2 Download new DB Apps

Download business apps with the DB icon via the **Hub app in** the "Work" or "Business" area.

Only apps that you can download from the Hub app comply with DB's security regulations. With **Samsung/Nokia/Gigaset,** they are automatically stored in the service area when they are installed.

Apps for private use can be installed if required. Use **your private Google/Apple account** or create a new one and observe the terms of use of the device.

7 More settings

In the next step, we will show you how you can set up your smartphone/tablet individually so that it supports you in your everyday work in the best possible way.

7.1 The operating system

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

Your **Samsung/Nokia/Gigaset** runs on the Android or Android-One operating system. You can see which operating system version your smartphone/tablet has here:

- Open the "Settings".
- Scroll to "Phone info"/ „About the Phone".
- Tap on "Software information". The currently installed Android version is now displayed here.

Your **iPad/iPhone** runs on the iOS operating system. You can see which operating system version your iPhone/iPad has here:

- Open the "Settings".
- Tap on "General".
- Tap on "Info". The currently installed iOS version is now displayed here.

7.2 Quick access/ Control centre

Samsung/Nokia/Gigaset
Change the brightness, switch off the WLAN or open the settings of your smartphone/tablet? You will find these functions in the so-called "quick access":

- Swipe your finger once from the top edge of the screen downwards.
- A bar with icons opens - the quick access:
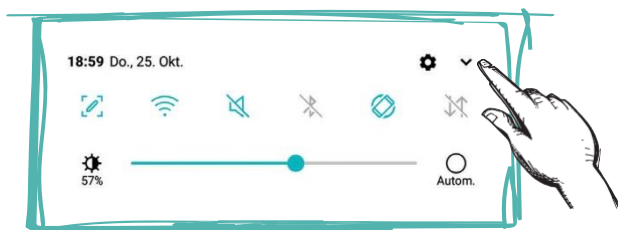
Here you can switch functions of your smartphone/tablet on and off by tapping, for example:

WLAN   Mobile data   Sound

Adjust the brightness of the screen:

▌ Tap the bar in quick access and slide the item to the desired brightness.

▌ Do you want the screen brightness to adjust automatically? Put a tick next to "Auto" or tap on the small sun symbol with the A next to it.

There are even more functions in the quick access. To see them, swipe your finger across the screen again from top to bottom. More icons appear, e.g. the torch.
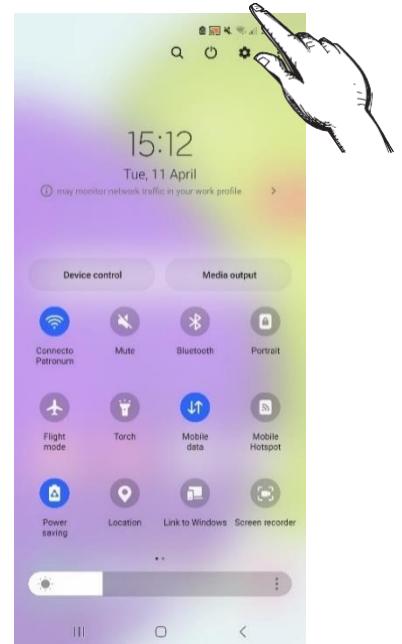
You can find more settings via the "Settings" app. This is located in your "Personal"/"Private" section.

iPhone/iPad

Change the settings via the so-called "**Control Centre**":

❚ Swipe down from the top right corner of the screen (note: on some models, you may need to swipe up from the bottom instead).
❚ The control centre opens.
❚ Now you can adjust the brightness or volume, among other things.
❚ To close the control centre again, swipe upwards from the bottom edge of the display or tap on the display.
❚

You can find more settings via the **Settings** app.

Design the start screen:

On your smartphone/tablet, you can move apps and folders within a screen view or from one side of the screen to the other:

▮ Tap on the app and hold it down a little longer.

▮ Then drag the app to where you want it and release.

Samsung/Nokia/Gigaset **Smartphone**:

▮ Tap and hold from an app

▮ Drag apps directly from the "Work"/"Business" area to the home screen.

▮

Samsung/Nokia/Gigaset **Tablet**:

▮ All apps are displayed on a general overview, dragging apps directly from the folder is not possible.

▮ To do this, swipe once across the centre of the screen and then to the left.

▮ Then you will see all the service apps.

▮ From there you can move them anywhere.
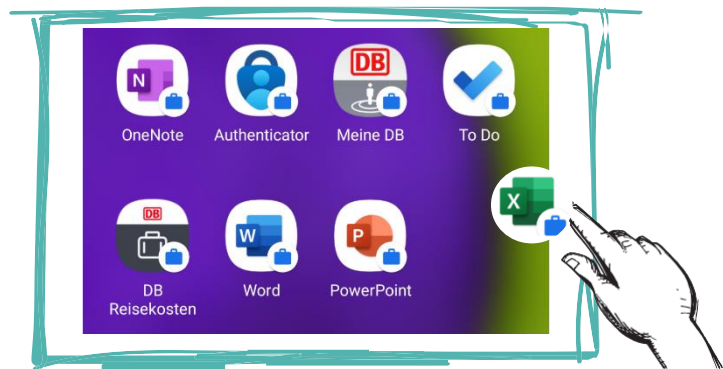
7.4 Connect to the internet

DB-WLAN

- Connect to the DB WLAN (dbs4mobile) at DB locations.
- This protects your data flat rate and at the same time establishes a secure network connection.
- Select the correct DB WLAN.
- Then activate Wi-Fi in the quick access menu of your smartphone/tablet.
- Enter the DB user login data, the next time the device connects automatically.
- Note: To use the DB WLAN, the product "WLAN for mobile devices" must first be ordered via the Service Portal.
-

Public WLAN

The data security of your smartphone/tablet is a particular problem wherever a public WLAN is offered.

- Log in only via DB WLAN or your private WLAN at home.
- avoid the use of unsecured Wi-Fi networks.
- Also, when choosing, make sure you use the right WLAN
- always observe DB's general safety requirements.

Mobile data - your data flat rate

If there is no DB WLAN nearby, use the internet via mobile data. Depending on your contract, Deutsche Bahn will provide you with a data volume that allows you to use the internet free of charge.

- As soon as 80 per cent of this data volume has been used up in the current month, you will receive an information message by SMS.
- You will be asked if you want to add more data volume.
- Note that this will incur additional costs for DB.

Your Vodafone Contract - Elfe (Electronic Telecommunications Invoice)

Once a month, you will receive a statement for the Vodafone contract for your smartphone/tablet. You will receive it by e-mail from the sender ELFE@deutschebahn.com. To open the statement, you need an extra password. You will receive this password once by e-mail. Keep the password in a safe place. **Important:** You do not have to pay anything, the statement is only for documentation purposes.

The offline mode (flight mode)

In the quick access of your smartphone/tablet you have the option of activating offline mode or flight mode. Please note, however, that this deactivates all communication functions. This also means that no updates will be carried out and you will not receive any DB messages. Hereford, think carefully when you set the flight mode.

7.5 F5 Access - Establish VPN connection

VPN is the abbreviation for **Virtual Private Network** and describes an internet connection that cannot be viewed by unauthorised persons. At DB, we use "**F5 Access**" to establish a VPN connection. This gives you secure access to the Deutsche Bahn corporate network. In addition, some apps can only be used with an active VPN connection, e.g. the staff portal or ASES and e-Time.

Set up the VPN connection:

▌ Open the app "F5 Access" in the area "Work/Business".

▌ If applicable, agree to the terms and conditions and allow messages to be sent.
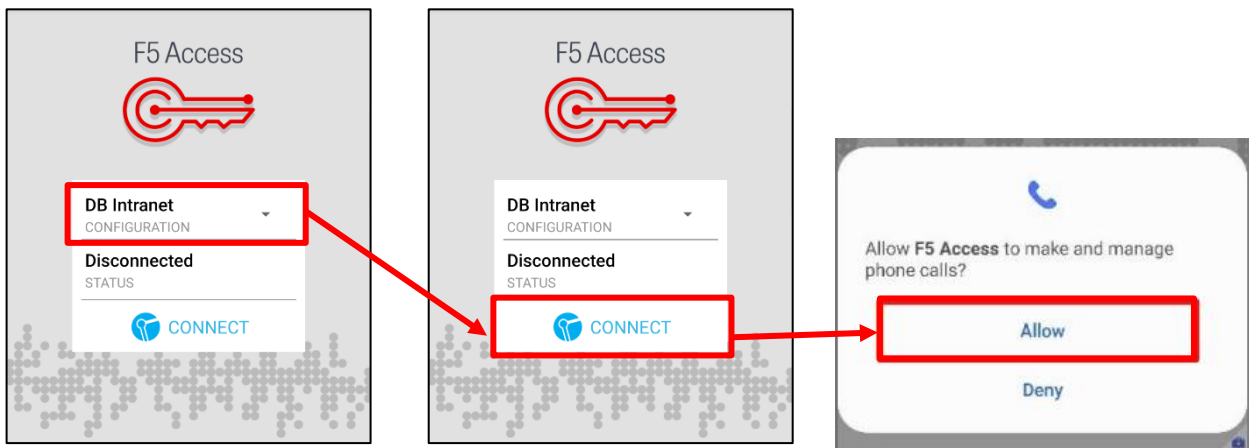
▌ Tap on "DB Intranet" in Configuration and then on "Connect". A VPN connection to the DB network is established.

▌ In the next dialogue, allow calls to be made and managed - Select "Allow" for this.
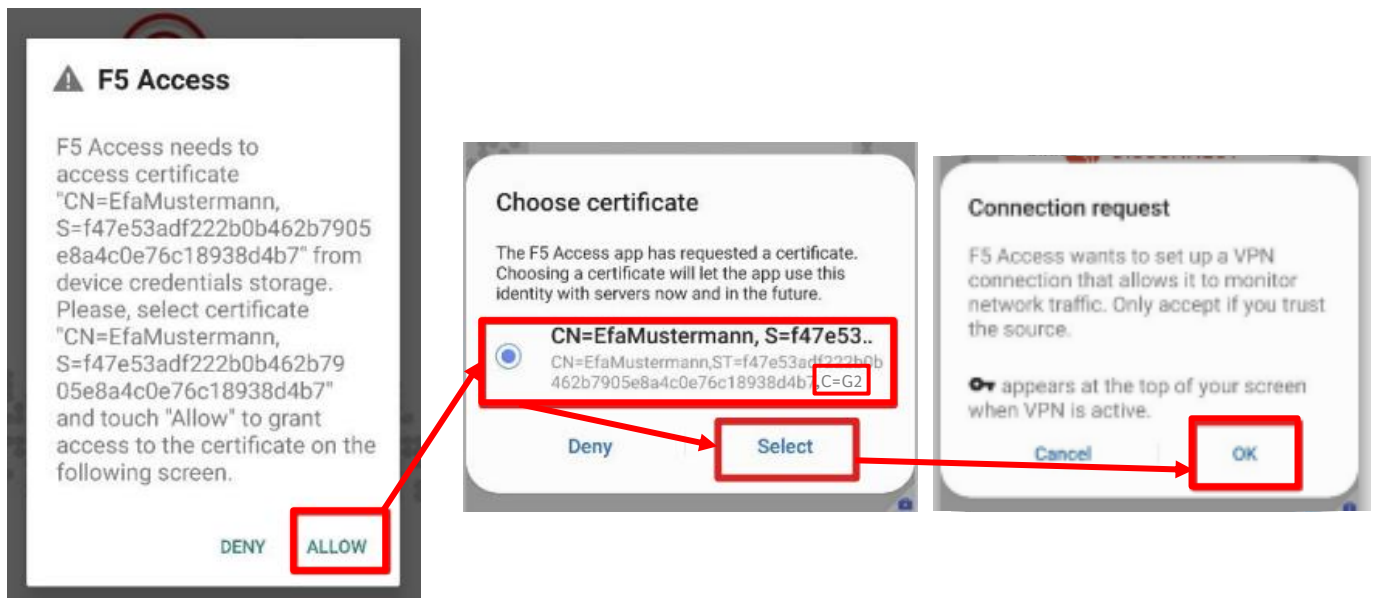
▌ Then allow the F5 Access Certificate by tapping on "Allow".

▌ Tap on the certificate that ends with C=G2.

▌ Then tap on "Select".

▌ Then confirm the connection request with "OK".

▌ The VPN connection is now set up. Tap on "Disconnect" as soon as the connection is no longer needed and close the app.

Note: A permanently active VPN connection leads to high battery consumption. Therefore, only switch it on when you really need it.

7.6 Improve the battery life of your smartphone

❚

❚ Updates can only be installed on your smartphone/tablet when the battery is charged more than 20%.

❚ If updates are not installed, you may eventually not be able to use your smartphone/tablet.

❚ Therefore, always charge the battery sufficiently!

This is how you save your battery:

❚ Switch off services that are not used all the time, e.g. Bluetooth, VPN (F5) and the GPS function.

❚ Do not charge the unit overnight.

❚ Do not expose it to extreme - too cold or too hot temperatures.

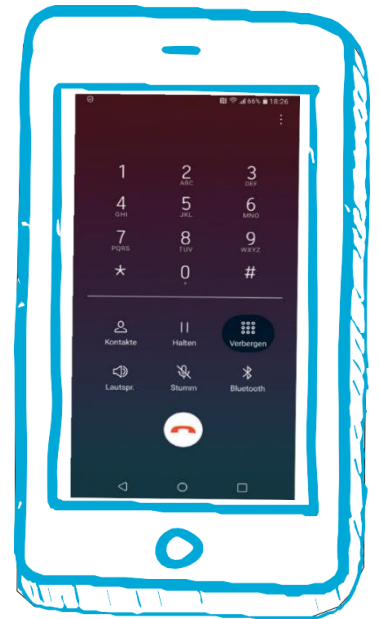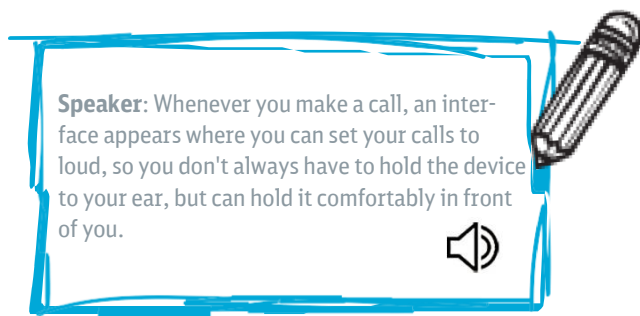## 7.7 Set up your answering machine

Your smartphone/tablet has an answering machine (mailbox), you set it up like this:

- ▌ Tap the phone app.
- ▌ Tap Contacts.
- ▌ Call your mailbox. To do this, tap on "Mailbox" in the contact list under M.
- ▌ A voice menu tells you exactly what to do and in what order.
- ▌ Record your own greeting text.

As soon as someone has left you a message on your voicemail, it will be displayed in your call list. Tap the handset to see them.

Speaker: Whenever you make a call, an interface appears where you can set your calls to loud, so you don't always have to hold the device to your ear, but can hold it comfortably in front of you.

7.8 Deactivate advertising ID

This note only applies to Android smartphones/tablets.

Google creates a so-called advertising ID for every Android smartphone/tablet by default. Google uses the advertising ID to create a profile from your behaviour on the internet and your preferences. In this way, personalised advertising can be displayed on your smartphone/tablet.

Group Privacy recommends **deactivating** this **advertising ID**. This is the only way to prevent a profile from being created.

To do this, proceed as follows:

- ▌ Open the settings on your smartphone/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, and profiling is no longer possible. More information about the advertising ID is available on DB Planet here: #MobileWorkplace

8 Apps - The important applications for the start

8.1 Hub app – Download new apps

The most important apps are already installed on your device.

Service apps: Download via the **Hub app**. DB-specific apps such as DB FASSI-MOVE or DB Baudoku and many others are only available for download there.

You can download **private apps** on your **Samsung/Nokia/Gigaset** via the **PlayStore** in the private area.

On your **iPhone/iPad,** download private apps from the **AppStore.** Note that you must first set up an Apple ID.

8.2 The Welcome App

In the Welcome App, you will find instructions for setup and recovery, regulations and other links related to your smartphone/tablet. More information about the Welcome App and its functions can be found here: <u>DB Planet</u>

It is also possible to take screenshots via the Welcome app. We show you how to do this here:

Take screenshots

A screenshot is a photo of your screen. This means that the content that is currently displayed on your screen is captured and saved as an image.

iPhone/iPad: Take screenshots as usual by pressing the side button and the volume up button at the same time.

Samsung/Nokia/Gigaset: You can take a screenshot with the usual key combination by pressing the "Silent" key and the "On/Off" key together for a few seconds. However, this picture will then end up in your private picture gallery on your smartphone/tablet.

To take screenshots in the in-office area that will be saved in your in-office picture gallery, use the Welcome app!
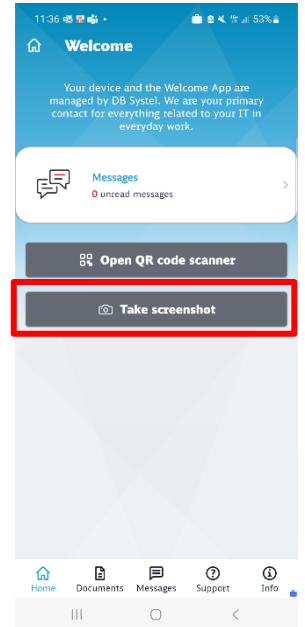
Activate screenshot function

When using the screenshot function for the first time, the app needs some permissions. We explain how to set these in the following or in the video tutorial (<u>Enable screenshots</u>):
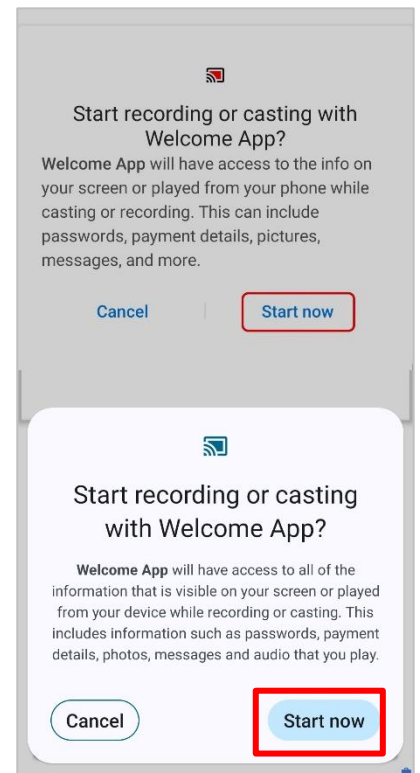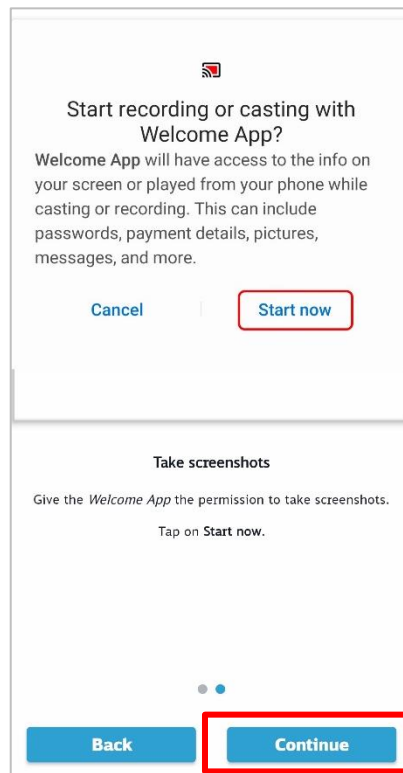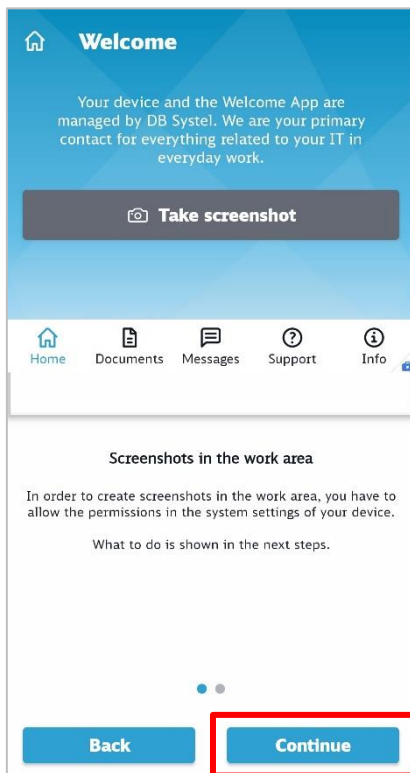
- Open the Welcome app and tap "Take screenshot"/"Take screenshot" on the start page.
- Tap "Continue" on the first query.
- In the next step, give permission for the Welcome app to access photos, media and files. This is the only way to save the screenshots. To do this, tap on "Continue" at the bottom right and then on "Start now" in the dialogue that opens.

- In the next step, the Welcome app needs permission to display itself over other apps. To do this, tap on "Continue" at the bottom right.
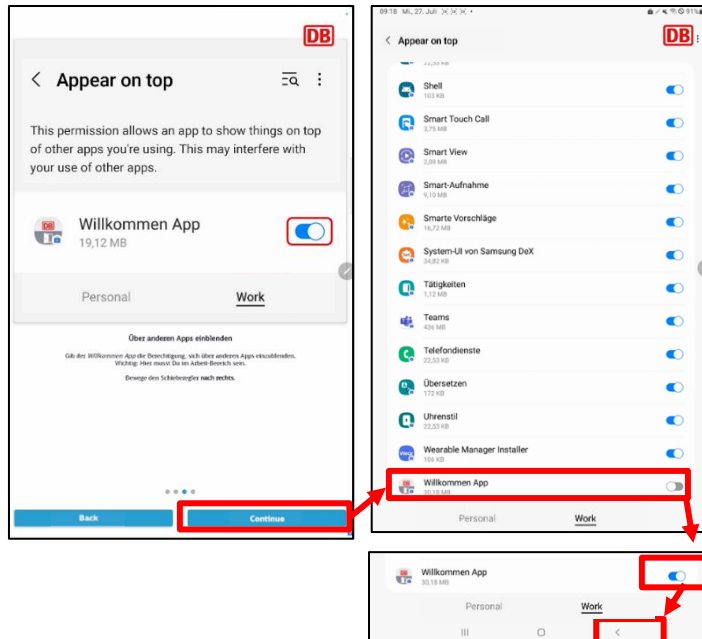
- A list of your apps opens. Scroll to the Welcome app and move the slider to the right.
- Then tap the system arrow at the bottom right to return to the Welcome app.
- Again, tap on "Continue" at the bottom right and then on "Start now" in the dialogue that opens:
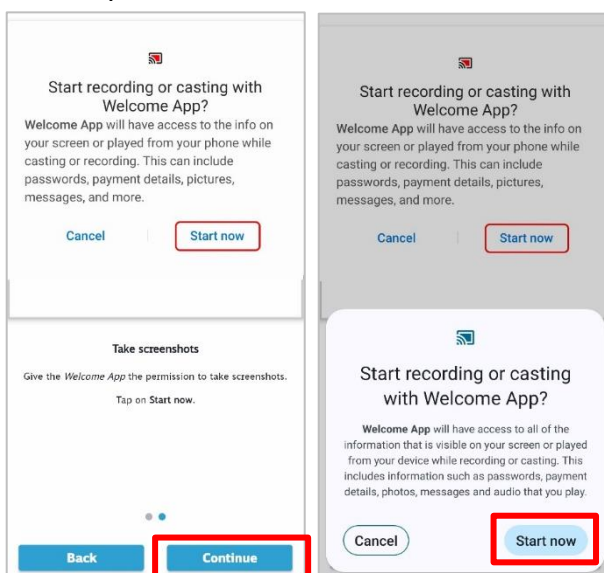
You can now take screenshots:
- After tapping the "Take screenshot" button, the red camera button appears on your screen.
- Press and hold the camera button to take the screenshot.
- The screenshot is saved in the on-duty picture gallery

Push notifications

For new software updates or anything that affects your device, you will receive **push notifi-cations** via the Welcome app. For example, we will inform you about the distribution and automatic installation of software on your smartphone/tablet. **So check it out and keep yourself up to date**!

All information about the Welcome App is available here: #MobileWorkplace.

You can find your messages here:
- ▌ Open the Welcome App. On the home page, you will see the message area.
- ▌ If you have a new message, you can see it by the small red number next to "unread messages".
- ▌ To read messages, either tap on the "Messages" area in the top centre or on the "Messages" tab at the bottom:
- ▌
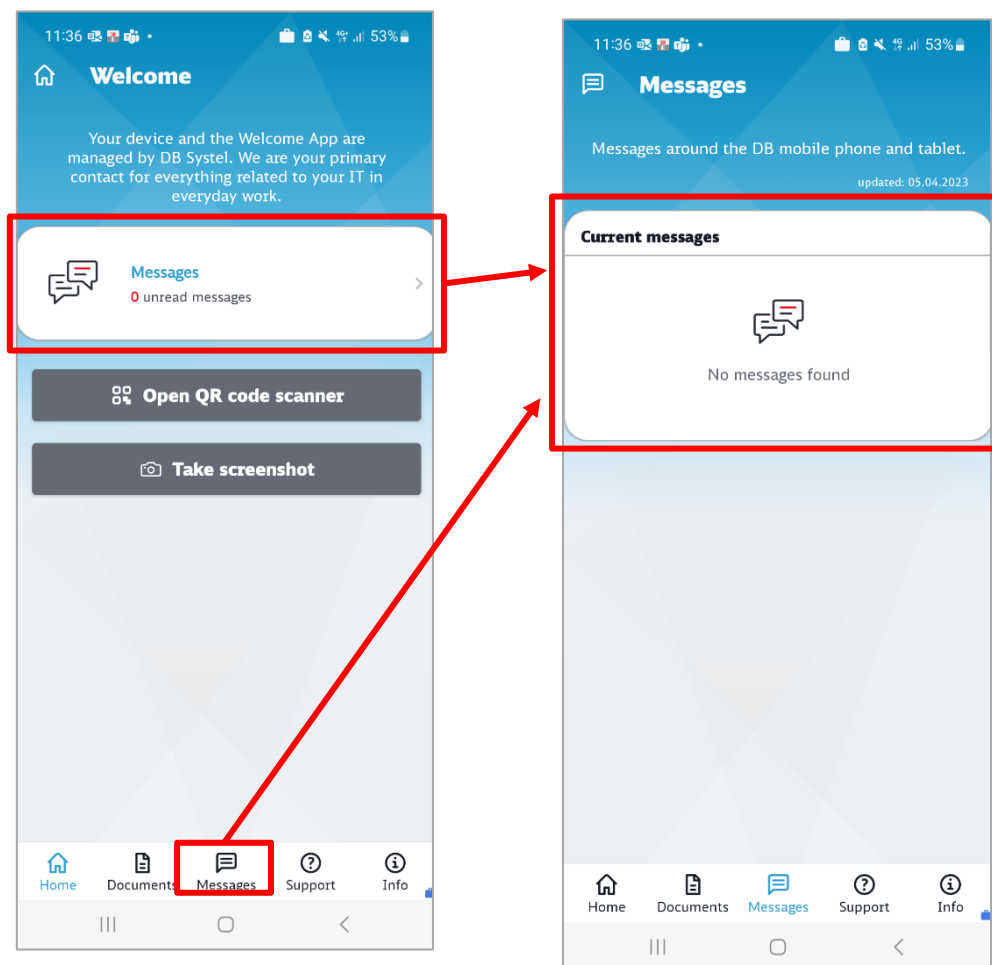
Scan QR Codes

QR codes are black and white squares. They are electronically readable codes. A special reader decodes this code and leads you directly to an application or to further information.

You can scan official QR codes via the **Welcome app** on your smartphone/tablet:

▌ Open the Welcome App.

▌ Tap on "Open QR code scanner" and allow the app to take pictures and videos.

▌ A small window opens with which you can scan the QR code. Position the QR code in the rectangle.

▌ After the code has been scanned, you will be redirected to the website.

8.3 Microsoft Authenticator App

The Microsoft Authenticator app enables **two-factor authentication**. With the app, you can prove your identity by confirming it in the app.

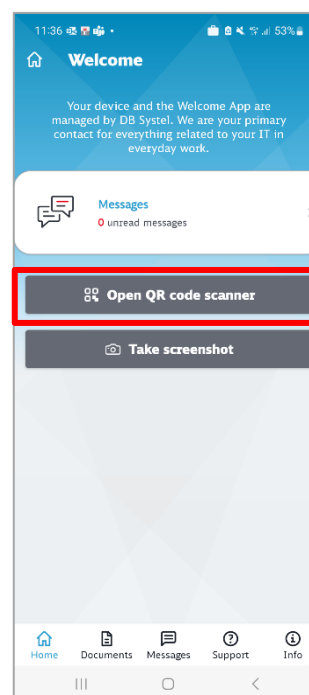After setting up your smartphone/tablet for the first time, the app is already installed and your account is set up. If your account is not stored in the app, you can set it up yourself in the **activation portal: >** https://db.de/authenticator.

Note: If you already owned a DB smartphone/tablet and now want to set up the Microsoft Authenticator app on your new device, follow these steps:

▌ Do not take the old device out of service yet! You still need it to set up the Authenticator app on the new device.

▌ Open **>** https://aka.ms/Setupmfa on your old device or a laptop.

▌ Log in with your DB email address and select your certificate.

▌ You will be shown a number.

▌ Open your Authenticator app on your old device and confirm the login by entering the number.

▌ Once you have logged in, select the "Authenticator app" option via the "Add login method" button.

▌ Now proceed with your new smartphone/tablet and follow the instructions.

▌ You can then use the Authenticator on your new smartphone/tablet and reset your old smartphone/tablet.

8.4 Sending and receiving e-mail s with the Outlook app

With Outlook, you can receive and send your business e-mails. Before you can get started, you need to make a few settings.

Set up Outlook

❚ Go to your "Work/Business" area and tap on the Outlook app there.

❚ Your email account should already be automatically stored - then tap on "1 account found".

❚ If your email account is not registered, tap on "Create new account".

❚ In the next step, select your email address by tapping on it so that a tick appears behind it and then tap on "Next".
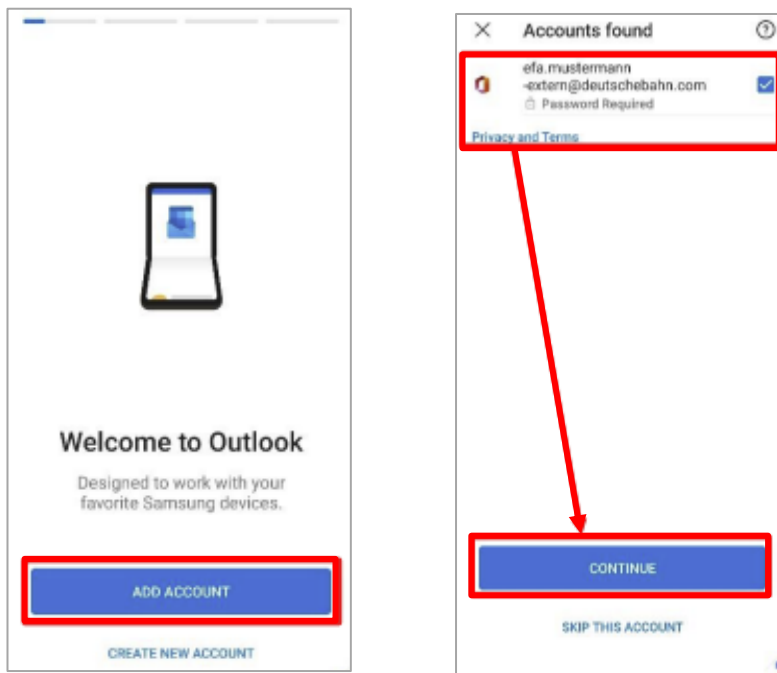
Samsung/Nokia/Gigaset:

❚ Select the correct certificate* in the query. This begins with CN and your first and last name and contains "Office 365", i.e. CN=FirstNameLastName- Office356, ...

❚ Tap on the certificate and then on "Select".
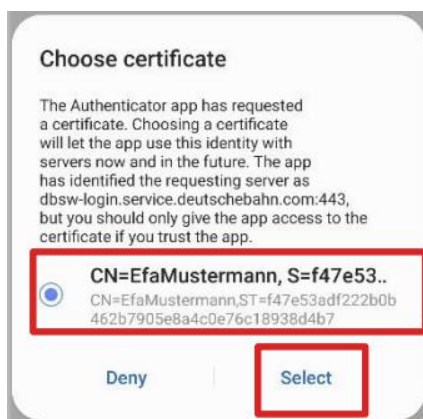
❚ Your email account is now set up.

❚ You can confirm the next two windows with "Maybe Later" and "Skip".

iPhone/iPad:
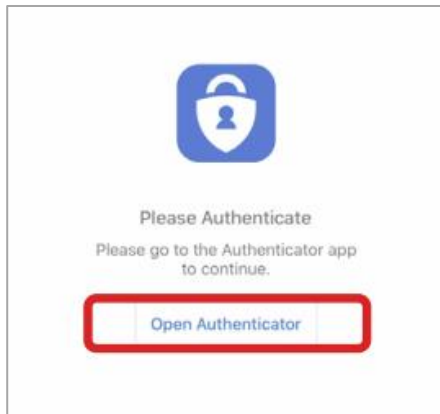
▮ Tap on "Open Authenticator" for authentication.

▮ Next, select the "Office365" certificate.

▮ Confirm the two queries with "Switch on" (so that the e-mail synchronisation can work) and with "Allow".

▮ You will then be asked for another account. Tap on "possibly later" and close the last query with "Skip" until you reach your inbox.

▮ Your emails will now be loaded. This process can take a few minutes. After that you can read and write emails.

Do you have questions about writing and sending emails? On **>** ITfit you will find useful tips and instructions on how to use Outlook.

Set up e-mail signature

An e-mail signature is a mandatory part of official e-mail communication. It appears at the end of an e-mail and must, by law, contain certain information, such as the company name and the official headquarters of your DB company.
You can find the text for your e-mail signature in the DB's central telephone book, the so-called **"EVI".**

How to get your email signature from EVI:

❚ Open the EVI app in your "Work"/"Business" area.
❚ You will now see the mobile EVI view.
❚ Tap on the menu at the top left and then on "Classic EVI view".
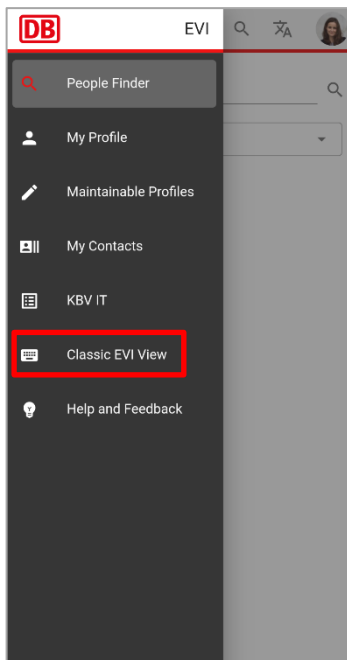
The classic EVI view opens. Then tap under "My EVI" on "My email signature".
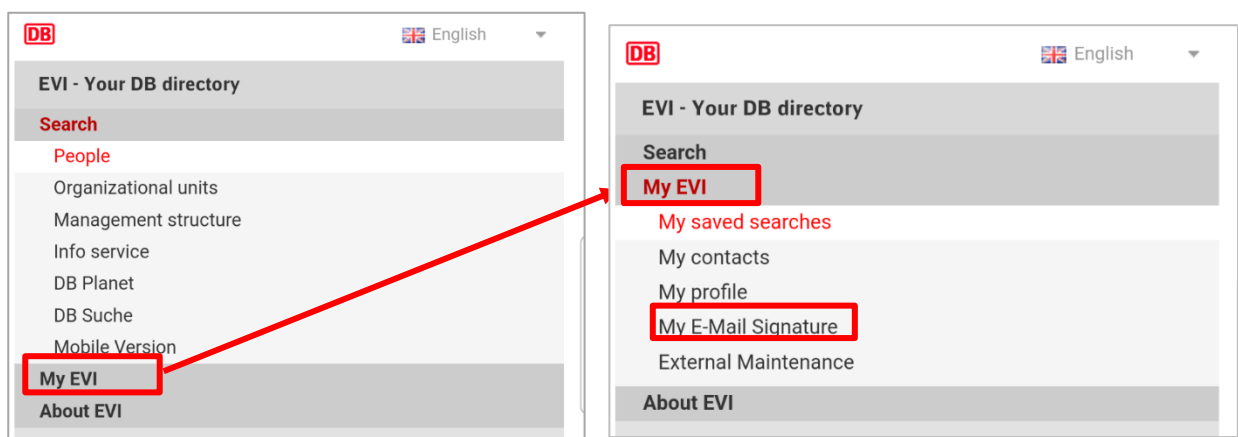
❚ A field with the heading "My email signature" appears. Below this is your personal email signature.
❚ Copy the signature by tapping on the "Copy signature to clipboard" field below.
❚ Then close EVI.
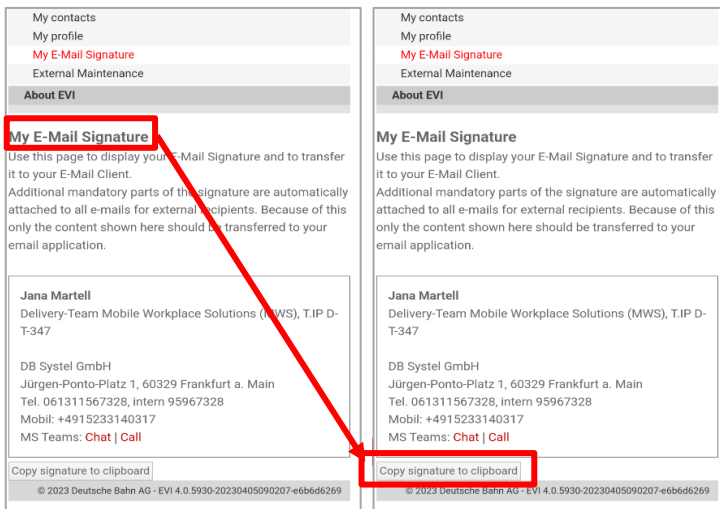
Paste the signature into Outlook:

▌ Open the Outlook app in the "Work"/"Business" area

▌ At the top left is a small circle with an icon or your profile picture. Tap on this.

▌ An overview of your email folders opens on the left-hand side.

▌ Tap the cogwheel at the bottom left⚙ .

▌ The settings will open. Tap on "Signature" under "E-mail".

▌ A field for the signature opens. If there is already an entry there, delete it with⊗

▌ Now tap on the empty field until the "Insert" field appears and tap on it.

▌ Your copied signature from the EVI is inserted.

▌ Close the window - your signature will now be automatically inserted in all emails you write.
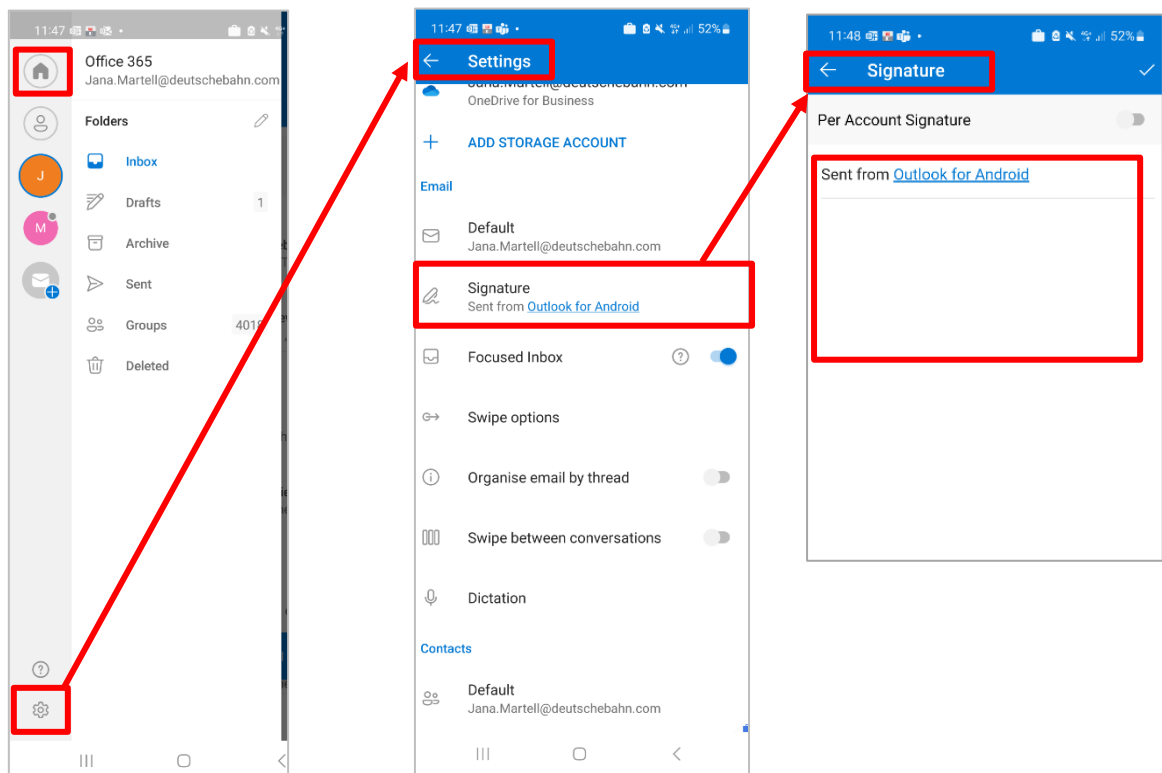
▌ **Note:** If you have set up several e-mail accounts, you can use the "Signature per account" slider to set up a separate signature for each account. Otherwise, the stored signature is used for all your e-mail accounts.

Encrypt emails

E-mails that you send within the DB Group are encrypted by default. This is sufficient for most concerns - so you don't need to do anything else!

When you send an e-mail, however, always keep these two rules in mind:
- ▌ the e-mail contains only as much personal data as necessary.
- ▌ the subject of the e-mail does not contain any confidential information.

Set up additional encryption:
If you want to send particularly sensitive data (e.g. personal data) by e-mail, you must also encrypt the content of the e-mail.
DB provides the so-called S/MIME encryption for this purpose. To use it, you need your personal certificate. You can install this yourself via the Welcome App.

- ▌ To do this, open the Welcome App.
- ▌ Select the Help tab in the Welcome App.
- ▌ Then tap on Encrypted e-mails.
- ▌ Follow the steps in the instructions.

After successful installation, you can read and send encrypted emails on your smartphone/tablet.

You can find detailed step-by-step instructions here: **>** Encrypted communication by e-mail

Synchronisation - Everything always up to date

All your emails are automatically backed up in the Outlook app and synchronised with your connected Office account. This means no matter which device you log in from, you're always up to date.

Synchronise contacts

If you create a new contact in the "Work"/"Business" area on your smartphone/tablet via the Contacts app, it is advisable to release them for synchronisation with Outlook. You do this like this:
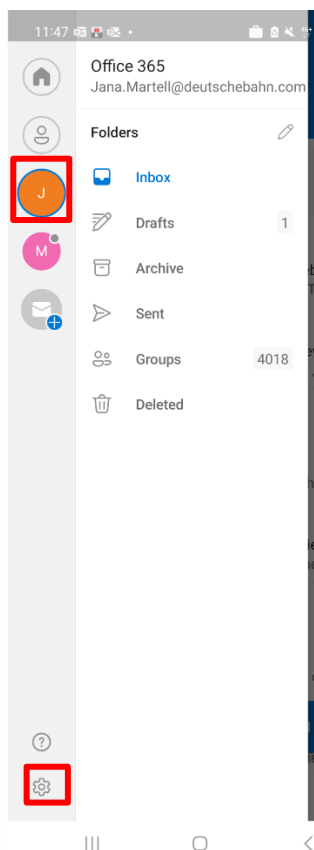
▮   Open the Outlook app in the "Work"/"Business" area.

▮   In the app, there is a small circle with an icon in the top left-hand corner. Tap this.

▮   An overview of your e-mail folders opens on the left-hand side.

▮   Select the cogwheel ⚙ at the bottom left.

▮   The settings open.

▮   Select your Outlook account under "Email accounts" and then tap the small slider next to "Synchronise contacts".

▮   Confirm the subsequent access request with "Allow".

▮   After you have activated synchronisation, exit the Outlook app.

Create new contacts

▮   Open the Contacts app.

▮   Tap the "+" to create a new contact

▮   Select "Outlook" in the top left corner via the small arrow. The new contact is saved in Outlook.

8.5 MS Office

You can also open and read Word, Excel, PowerPoint files or PDF files on your smartphone/tablet. To do so, download the corresponding apps from the Hub App:

❚ Open the Hub app.

❚ Search for the respective app via the search bar, for example Word, Excel, Power-Point or the PDF Reader).
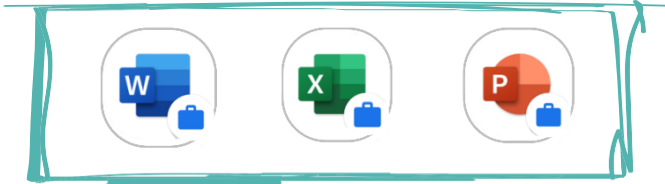
❚ Then tap on "Install". The app will now download and appear in your "Work"/ "Business" area and on your iPhone/ iPad on the start page.

❚ When you open a file, the app opens automatically.

Note: You can only open one file at a time. It is therefore not possible, for example, to open and edit several Word files at the same time.

9 Back up your data

9.1 Back up business data in OneDrive

In order to save photos and other documents, such as PDF or Word files, you need the app "OneDrive". With this app, you can save all your work data in a cloud and then access it at any time with all your work devices. For example, you can also access your data from your work PC.

Set up OneDrive

To set up OneDrive, Outlook must already be installed on your smartphone/tablet and the user account must be set up.

- Download the app "OneDrive" from the Hub app.
- After installation, the app is displayed as an icon in the "Work"/"Business" area and on your iPhone/ iPad on the start page.
- Open the OneDrive app by tapping on the icon.
- Confirm that the app can send you notifications.
- Select "Log in".
- Enter your DB email address - you will be automatically registered.
- You can now see all your files in OneDrive.
-
- **Note**: When you set up OneDrive again, it can take a few minutes until all your data is synchronised.
-

Save settings

If you ever reset your smartphone/tablet to factory settings, back up your settings as well. Take screenshots or notes of your individual settings and DB apps. Save them to OneDrive so you can use them as notes when you restore.

9.2 **Automatically save photos**

▮

Samsung/Nokia/Gigaset

Set up synchronisation

▮ Tap the "Me" icon at the bottom right of the bar and then select "Photos".

▮ The message "Camera upload is deactivated" appears at the top.

▮ Select "Turn on" in the menu.
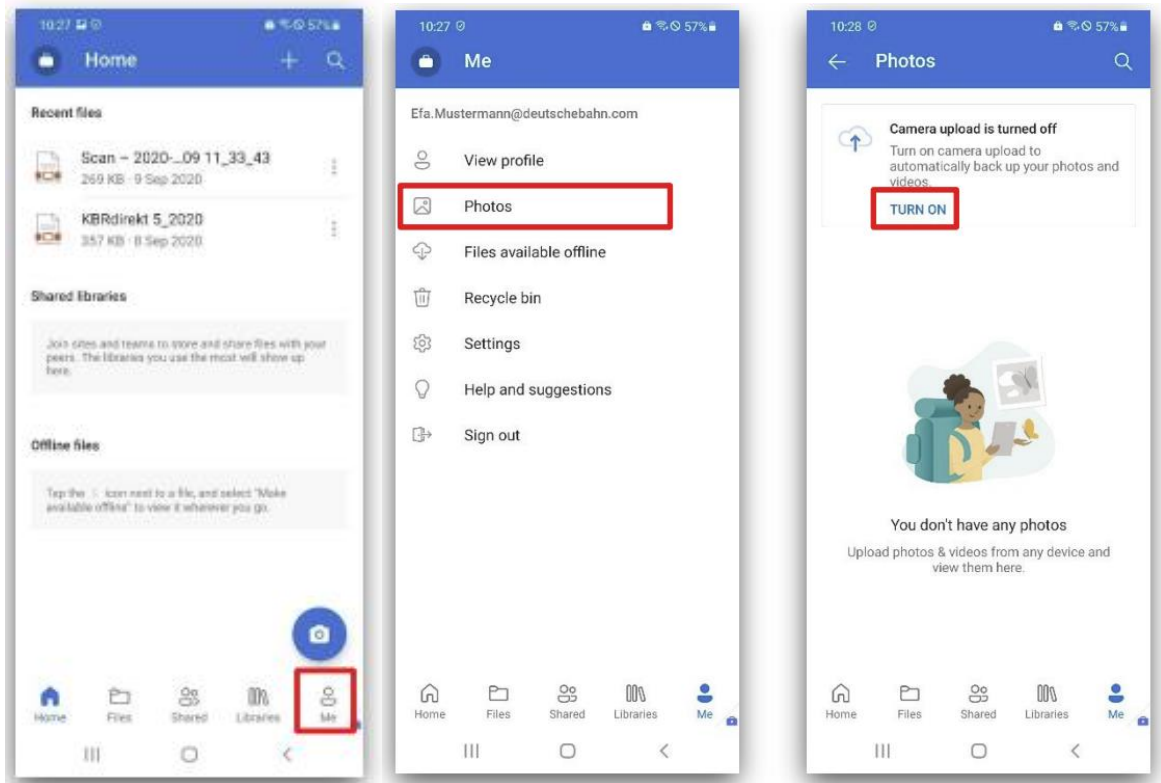
▮ Tap "Confirm" in the dialogue asking whether pictures and videos should be synchronised with OneDrive.

▮ Activate the camera backup: Select "Allow".
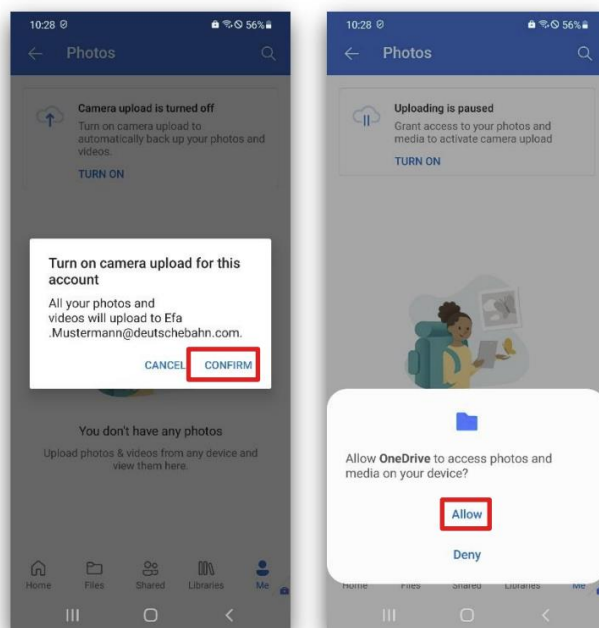
- ▌ Select "Permissions" and tap on "Files and Media".
- ▌ Select "Allow access to media files only" to give OneDrive access to videos and photos.
- ▌ Tap the arrow at the top left.
- ▌ Then select "Camera" and tap "Allow access only while in use".
- ▌ Tap the arrow at the top left several times to return to the OneDrive app.

9.3 Save PDF files

PDF files are usually saved in the download directory in the "Work"/"Business" area. To save them to OneDrive, proceed as follows:

- ▌ Open the My Documents app.
- ▌ Tap on "Downloads", long press on the PDF file until a tick appears in front of the name.
- ▌ Tap "Send" at the bottom of the menu bar and then select "OneDrive".
- ▌ Select the folder in which the PDF is to be saved and then tap on the white tick at the top right.
- ▌ The file is now uploaded to the OneDrive.

iPhone/iPad

Set up synchronisation

- ▌ Tap on the round symbol in the top left corner or on your profile picture.
- ▌ Then select the item "Photos" in the menu.
- ▌ The message "Camera upload is deactivated" appears at the top.
- ▌ Tap the "Activate" button to the right and activate the slider next to your email address.
- ▌ Tap "Confirm" in the dialogue asking whether pictures and videos should be synchronised with OneDrive.
- ▌ Activate the camera backup: Tap on the "Open settings" app button.
- ▌ You are now in the settings of your smartphone/tablet.
- ▌ Tap on "Photos" and then tick "All photos" to allow OneDrive to save the photos and videos.
- ▌ Return to the OneDrive app.

Save PDF files

PDF files can be saved directly in OneDrive, proceed as follows:

- ▌ Open the file.
- ▌ Tap the share icon in the top right corner.
- ▌ Select "OneDrive" from the menu at the bottom.
- ▌ Select the folder in which the PDF is to be saved and then tap on the white tick at the top right.
- ▌ The file is now uploaded to the OneDrive.

After synchronisation has been set up, every photo taken via the camera is synchronised with OneDrive.

9.4 Back up private data

If you have stored private pictures, contacts, files and documents on your smartphone/tablet, it is necessary that you back them up independently and regularly. If you reset your smartphone/tablet, your private data will also be deleted.

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

10 Data protection and usage information

When you use a DB smartphone/tablet on the move, there is always a security risk that unauthorised persons will gain access to the smartphone/tablet. Even a brief access then offers many opportunities to tap into data worthy of protection.

Therefore, stick to the following basic rules:

- Don't just leave the smartphone/tablet lying around, always make sure it is within your control.
- Do not give your smartphone/tablet to anyone else, even for a quick look, unless it is a group device.
- Always secure your smartphone/tablet with a PIN or a secure password, and even better with biometric security such as your fingerprint or face.
- Always use passwords and PINs only once!
- Passwords and PINs should not be guessable, so do not use telephone numbers, birthdays, car registration numbers or names.
- A PIN must be at least 6 digits long, contain at least 4 different characters and must not be an ascending or descending sequence of digits.
- Passwords must always have at least 12 characters and contain at least 3 out of 4 of the following: Upper case, lower case, number, special characters.
- Never save passwords, PINs and user names for the smartphone/tablet or the DB user on the device. Not even disguised as a telephone number, everyone knows that trick.
- Back up your business and private data promptly and regularly. You can do this by saving them in your OneDrive or by sending them as soon as possible by e-mail to the respective recipient for whom they are intended. Only then are they secured. This is because DB IT can access them if your end device breaks down or is lost.

Terms of use "mobile data communication
By accepting the smartphone/tablet and these Terms of Use, the employee confirms compliance with the Terms of Use:

1. The mobile devices are personal work equipment. Passing on the device or the access data/passwords/PINs to third parties (e.g. family members or superiors) is not permitted.
2. The mobile terminal remains the property of DB Systel for the entire period of use. The end device must be returned at the end of the period of use. It must always be kept free of third-party rights; in particular, it may not be lent or sold to third parties.
3. The consumption, use and dissemination of insulting, defamatory, pornographic, sexist, racist, anti-constitutional, immoral or criminal content and applications are prohibited.
4. The terminal must be handled with care and attention. The end device may only be charged using chargers/cables provided by the manufacturer (included in the scope of delivery). Charging during working hours is permitted.
5. Any loss, theft or function-impairing damage must be reported immediately to the superior.*
6. The data use of the mobile terminal device should, if available and usable at the employer, primarily take place via WLAN/WiFi networks.
7. The security settings of the unit (policies, virus scanner, terminal configuration, etc.) must not be changed or deactivated.

---

[1] See also Annex 1 to KBV IT General and Special Terms of Use, A (1).
[2] See also DB Asset Protection Guideline, 136.01.03

11 Help - When something doesn't work

You have forgotten the password for your screen lock or don't remember your DB user password? Outlook always crashes? You get error messages you don't understand? Don't worry, you'll find help here.
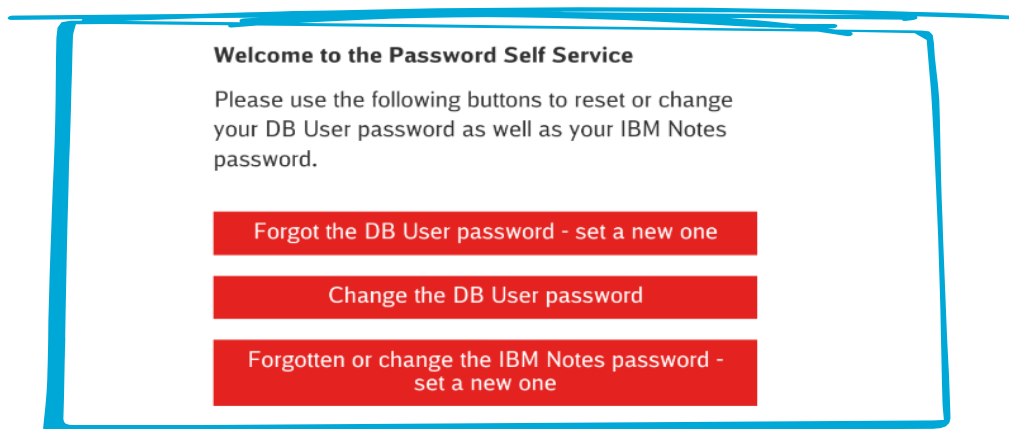
11.1 Help via the Welcome App

The Welcome App is the first point of contact for questions about your smartphone/tablet.

In the "Documents" tab and in the "Help" tab you will find the most important instructions, links and telephone numbers. For example, the instructions for initial set-up and for recovery. If your device is not working at the moment, use the device of a colleague. Alternatively, you can find all important instructions here: db.de/ae.

Forgotten DB user login data?

If you don't remember your DB user login details or you want to change them, you can do so like this:

▌ Select the "Help" tab in the Welcome App.

▌ The help area opens. Tap in the middle on the box "Reset DB User Password".

▌ The self-service opens. Choose between the three options and follow the instructions:

Welcome to the Password Self Service

Please use the following buttons to reset or change your DB User password as well as your IBM Notes password.

> Forgot the DB User password - set a new one

> Change the DB User password

> Forgotten or change the IBM Notes password - set a new one

Note: To receive a new password, you need a mobile phone number that is stored in the DB phone book (EVI) or in DB User Selfservice.

11.2 Help via the IT ServiceDesk App

The IT ServiceDesk app is the central technical contact point for questions. From error analysis to technical support for hardware and software problems on your device - here you can ask your questions and get access to helpful instructions and important links.

This is how you get to the IT ServiceDesk app:

▌ Open the "IT ServiceDesk App" in the "Work/Business" area.

▌ Or access it via the link: **>** www.db.de/itservicedesk

▌ In the top left corner of the app you will find the menu

▌ Click on "New service request" and then select the method you would like to use to report your request.

In addition, in the IT ServiceDesk app under "Self Services & Links" you can, among other things:

▌ Update your DB User password

▌ Update your DB User mobile number
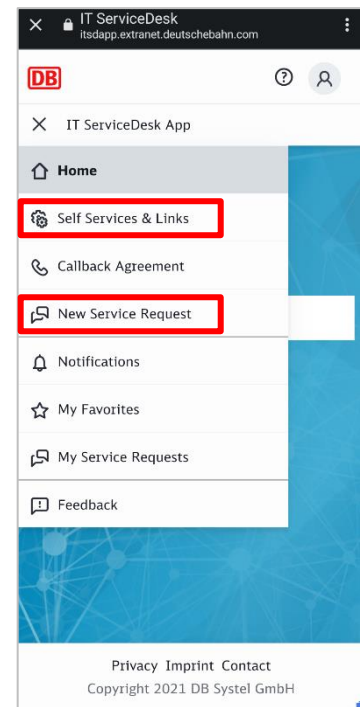
11.3 Lost smartphone/tablet - what now?

Call the **DB Systel helpdesk** immediately:

▌ Report the loss or theft.

▌ Make sure that your official data is deleted, i.e. a so-called "remote wipe" is carried out. You can find the instructions here: **>** www.db.de/ae.

Inform your **mobile phone manager** immediately.

▌ Report the loss or theft.

▌ Ask him to block your SIM card! Then no one will be able to make calls at company expense.

▌ Discuss with him the next steps to get a new smartphone/tablet.

Report the loss in the **>** **service portal:**

▌ Report a loss or theft via the Service Portal: Report mobile phone lost

▌ Click on "Mobile devices/services" in the main menu under "Inventory data".

▌ Select your device from the list and click on "Report loss/theft" in the drop-down menu.

▌ If you have any questions, please contact your mobile phone manager!

11.4 The smartphone/tablet has a total loss?

Inform your **mobile phone manager** immediately.
- ❚ Report the total loss.
- ❚ Discuss the next steps with him or her on how to get a new terminal.

Log off the smartphone/tablet in the **>** service portal:
- ❚ Open the service portal
- ❚ In the main menu, tap on "Mobile devices/services" under "Inventory data".
- ❚ Select your smartphone/tablet from the list, tap "unsubscribe" in the drop-down menu.
- ❚ If you have any questions, please contact your mobile phone manager!

11.5 Return old smartphone/tablet?

Important: Back up your data in advance. This is because your smartphone/tablet will be completely deleted by the recycler after it is returned. This means that all data (business and private) will be lost.

You can back up your work data to OneDrive. This way the data is stored in the cloud and you can access it at any time from any of your devices (smartphone/tablet/PC). We show you how to set up OneDrive in chapter 8.6 (OneDrive).

Log off the smartphone/tablet in the **>** service portal:
- ❚ Open the service portal
- ❚ In the main menu, tap on "Mobile devices/services" under "Inventory data".
- ❚ Select your smartphone/tablet from the list, tap "unsubscribe" in the drop-down menu.
- ❚ If you have any questions, please contact your mobile phone manager!

Simply return the smartphone/tablet yourself via the **>** recycler portal:
- ❚ Log in to the portal.
- ❚ Order a free return.
- ❚ You can choose whether you only need the return note for the return or whether you would also like to receive a cardboard box.
- ❚ You will receive the label by e-mail and the box by post to your specified address.

Prepare smartphone/tablet for dispatch
- ❚ Remove the personal accounts on your smartphone/tablet
- ❚ For Android: your Google account. You can find instructions here: db.de/ae.
- ❚ For iPhone/iPad: the "Find my iPhone/iPad" function. Also deactivate the iCloud lock. You can find instructions here: Apple support page.
- ❚ Remove your SIM card and memory cards.
- ❚ Pack your smartphone/tablet well so that it is not damaged during transport and include any accessories (power supply, USB charging cable, etc.) in the return box.
- ❚ Stick the return label on the box and take it to the post office.

Congratulations!

You have now successfully set up your smartphone/tablet.
To ensure that you can always use it reliably in the future, always carry out the latest updates!
We hope you enjoy using it!