



Operating system version from Android 15

Samsung Recovery

DB Workplace Mobile

DB Systel GmbH | 15.10.2026

Table of Contents

1 Necessary steps before recovery	4
1.1 Back up data	4
1.2 Authenticator App – optional	4
1.3 Create a Temporary Access Pass (TAP) - Expert Mode	4
2 Start recovery: Reset smartphone/tablet	7
2.1 Reset your smartphone/tablet yourself	7
2.2 Reset smartphone/tablet via the IT ServiceDesk app	8
3 Set up again in Microsoft Intune	9
3.1 Select language	9
3.2 Agree to End User License Agreement	10
3.3 Set up Wi-Fi	11
3.4 Setting up Wi-Fi in the DB building	12
4 Log Samsung into the DB	13
4.1 Set up your work profile	14
4.2 Set screen lock	15
4.3 Installing DB Apps	16
4.4 Google Account – Not Necessary	16
4.5 Activate Google service	17
4.6 Complete setup - optional	18
5 Activate Device - Create Temporary Access Pass (TAP)	19
5.1 What is necessary for the creation of the Temporary Access Pass (TAP)	19
5.2 Create a Temporary Access Pass (TAP)	19
5.3 Create a temporary access pass for a colleague	22
6 Activate your device with the Temporary Access Pass (TAP)	24
6.1 Set up access to all DB apps and websites	25
6.2 DB Apps	26
7 Necessary settings	27
7.1 Install Android OS Updates	27
7.2 MS Defender App – Activation required	27
7.3 Setting up Outlook /creating an email account/setting up email encryption	32
7.3.1 Outlook: Setting up your e-mail signature	34
7.3.2 Outlook: Synchronize e-mail	35

7.3.3 Outlook: Create new contacts in	36
7.3.4 Outlook: Sync Contacts	36
7.4 DB M 365	37
7.5 Turn off the Bixby button	37
7.6 Re-enable the Microsoft Authenticator app	38

1 Necessary steps before recovery

If your work smartphone/tablet has problems such as slow performance, freezing, or frequent crashes, a factory reset is helpful. These steps are necessary:

1.1 Back up data

To do this, follow these steps:

- a) Back up your work data and settings
- b) Secure your private data and settings
- > For instructions, see mobileworkplace.deutschebahn.com/mobile-daten-sichern
- > You can find a video tutorial at: db.de/mobile-videoanleitung

1.2 Authenticator App – optional

Note: This information only applies to users who actively use the *Authenticator app*, e.g. for administrative access with the so-called 2-person account or for multifactor authentication, e.g. for VPN with a Basic Workplace MAC.

- **Note:** You won't be able to use the Authenticator app during the recovery process
- No further steps are necessary
- Once restored, the app needs to be re-enabled
- > Go to [Chapter 7.6 Re-enabling the Microsoft Authenticator app](#)

If it is necessary to use the *Authenticator app* during the recovery, use another smartphone/tablet to connect it to the *Authenticator app*. To do this, follow the step-by-step instructions:

- > [Set up multi-factor authentication \(MFA\)](#)

1.3 Create a Temporary Access Pass (TAP) - Expert Mode

After you've backed up your data, there are two options:

Your smartphone/tablet no longer works at all:

- > Go to [Chapter 2.2 Resetting your smartphone/tablet via the IT ServiceDesk app](#)

Smartphone/tablet still works partially:

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

Continue on the following page!

To create a Temporary Access Pass (TAP):

- Open your default browser and go to db.de/tap
- Enter your DB User Name and DB User Password
- Select For Myself and tap the blue button
- Now select "DB Workplace Mobile"
- You'll then see the Temporary Access Pass (TAP)
- Write down the Temporary Access Pass (TAP) on a piece of paper or notebook

Note: The TAP is now valid for 60 minutes and for multiple smartphones/tablets.

Important!

The **TAP** may only be used in the **Intune App** even if you are asked for it in another DB app or on another smartphone/tablet.

- You'll need it later after resetting your phone/tablet
- You have enough time to reset your smartphone/tablet
- > Go directly to [Chapter 2.1 Resetting your smartphone/tablet yourself](#)

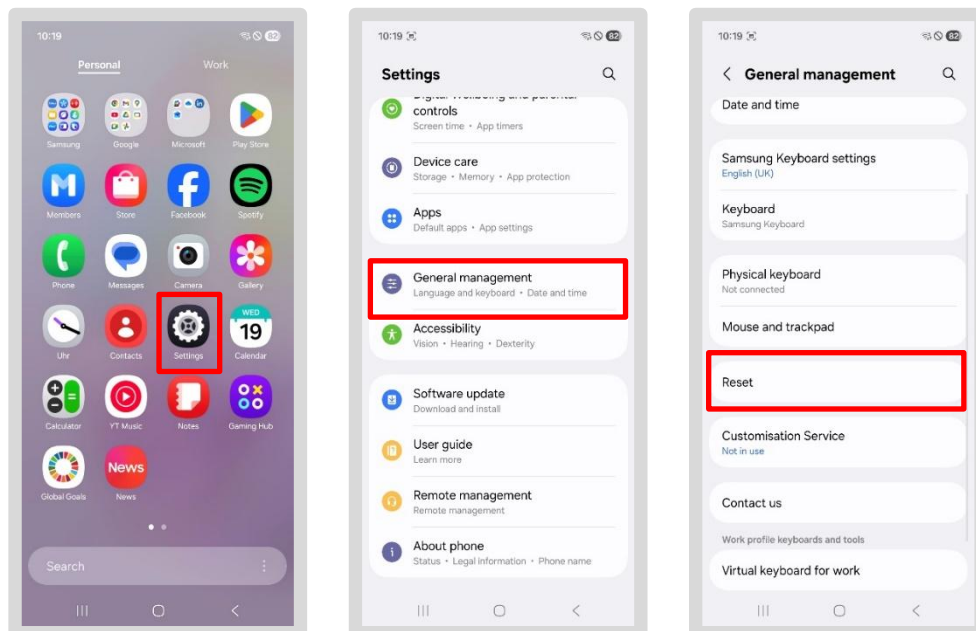
2 Start recovery: Reset smartphone/tablet

Note: The following screens may have a different display depending on the device model of the smartphone/tablet.

2.1 Reset your smartphone/tablet yourself

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

- On your phone/tablet, go to the Personal section
- Open the Settings app
- Tap General Administration
- Keep scrolling down and tap Reset



- Then select "Factory Reset"
- You'll see a hint about what the reset deletes
- Check whether you have backed up your work data (instructions: Backing up data)
- Then tap the "Reset" button, enter your screen lock and then "Erase everything"
- Wait a few minutes, your device will reset automatically

> Then go to [Chapter 3 Re-Setup in Microsoft Intune](#)

2.2 Reset smartphone/tablet via the IT ServiceDesk app

If your smartphone/tablet no longer works, then choose this step:

- Open the IT ServiceDesk app and enter your order for resetting your smartphone/tablet under "New service request"
- If you can't open the app, dial this number:
- IT ServiceDesk
 - Internal: Tel. 91-5555
 - External: Tel. 0361 430 8200
 - Select the menu item 0 here
- IT ServiceDesk DB Cargo
 - Tel. 91 7777 (internal)
 - Tel. 00800 327 978 35 (external)
 - Select the menu item 0 here
- If other things come up, think about it in advance:
 - Where did **problems arise?**
 - **Define the fault location;** to provide you with faster support
 - **In case of certificate problems:** Wait after registration **from 5 minutes to 24 hours** until all information and certificates have been transferred to the smartphone/tablet.

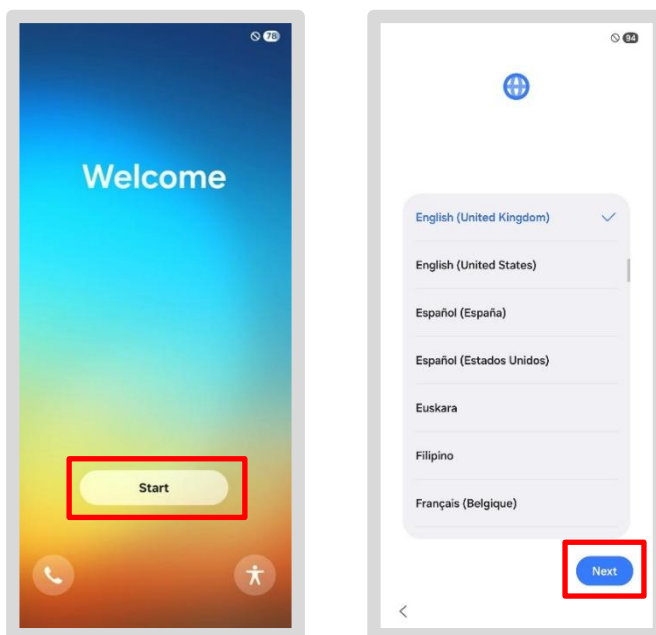
> Then go to Chapter 3 Re-Setup in Microsoft Intune

3 Set up again in Microsoft Intune

3.1 Select language

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

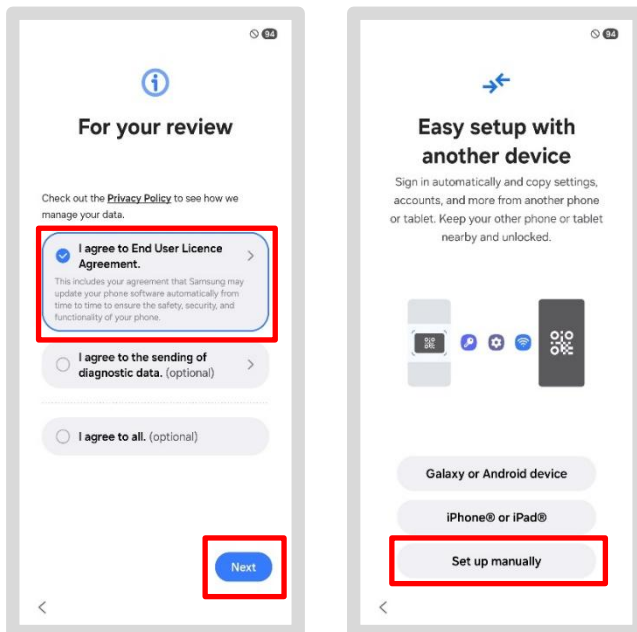
- Hold your tablet in **portrait mode** to get the screens in the same way as they are shown in the instructions
- Turn on your smartphone/tablet
- Make sure that your phone/tablet is either plugged into power or has a high battery level during the restoration process
- Tap Start
- On the next screen, select the language you want from the selection and tap Next



> Go to [Chapter 3.2 Agreeing to End User License Agreement](#)

3.2 Agree to End User License Agreement

- Just tap "I agree to the End User License Agreement" and then tap "Next"
- Tap in the "Setup with another device" on "Set up manually"



> Go to [Chapter 3.3 Setting up Wi-Fi](#)

3.3 Set up Wi-Fi

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

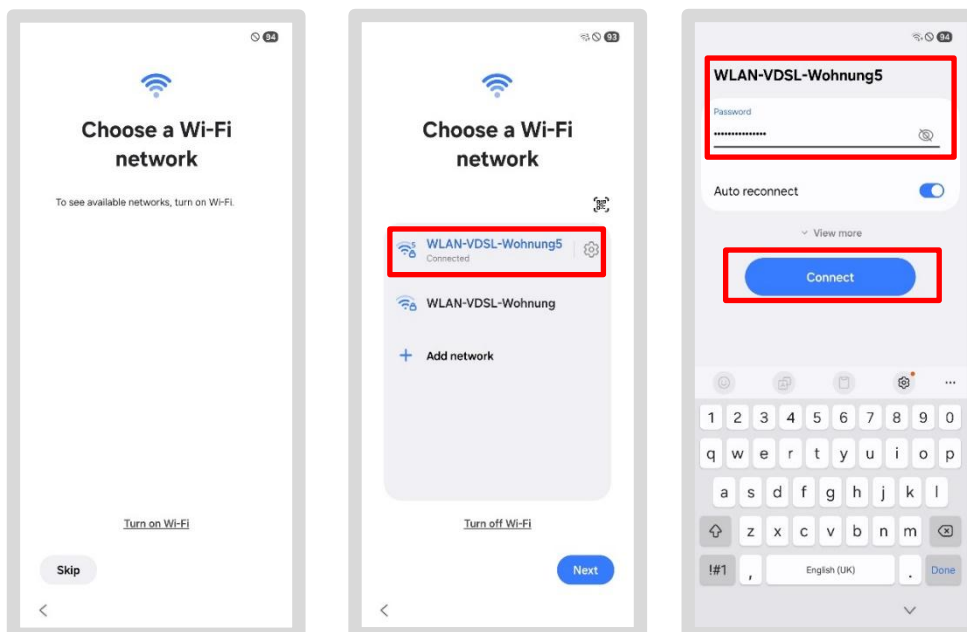
- Use your **mobile data** if you have a SIM card in your smartphone/tablet (this could be subject to a fee!)
- Set up a hotspot with your private smartphone/tablet

or

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

When choosing a different Wi-Fi network, proceed as follows:

- Tap the Wi-Fi network you want to select
- Enter your personal credentials and tap Connect
- For a second request, tap Continue



As soon as your smartphone/tablet is connected to the Wi-Fi, the link to the DB network starts.

> Go to [Chapter 4 Logging Samsung into the DB](#)

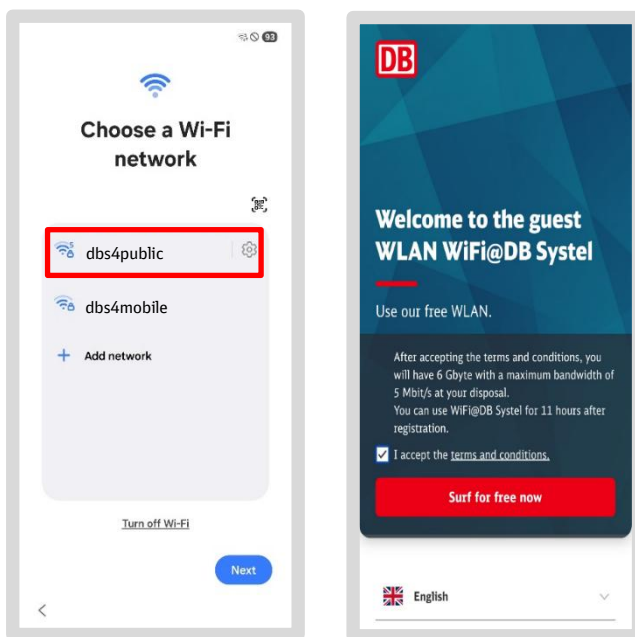
3.4 Setting up Wi-Fi in the DB building

Since the WLAN "*dbs4public*" does not always work satisfactorily in the DB buildings, we recommend that you select one of the following steps:

> Chapter 3.3 Setting up Wi-Fi

If you are in a **DB building** and want to use the "dbs4public" Wi-Fi, follow these steps:

- Tap on the "dbs4public" Wi-Fi network
- A dialog will open, accept the terms and conditions
- Tap Free Browsing Now
- Tap Close



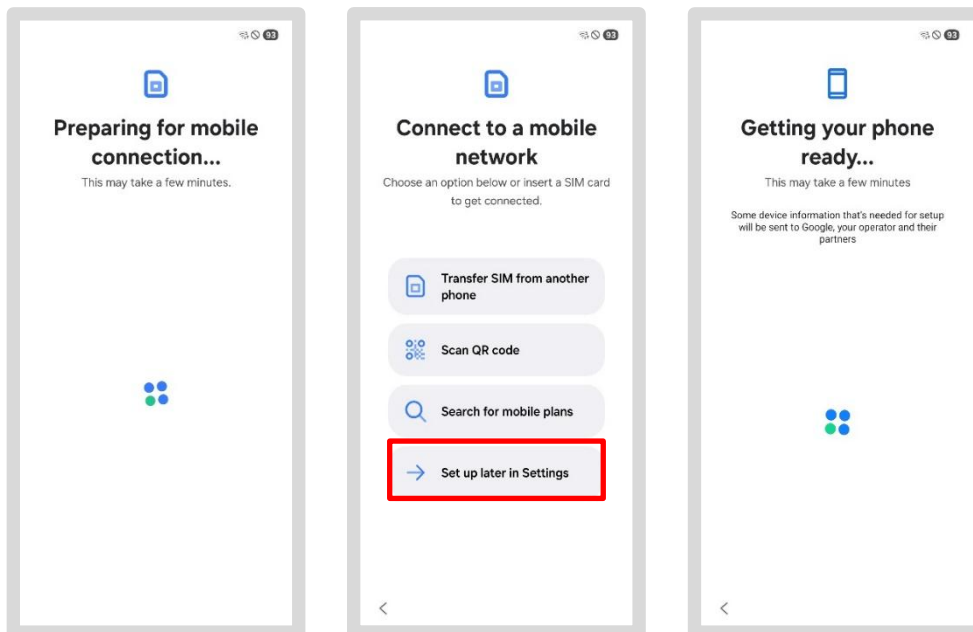
As soon as your smartphone/tablet is connected to the Wi-Fi, the link to the DB network starts.

> Go to Chapter 4 Logging Samsung into the DB

4 Log Samsung into the DB

In the next step, your DB smartphone/tablet must be linked to *DB Management* (more precisely in Enterprise Mobility Management, EMM for short). Wait for the changing information until an instruction appears. Depending on the network connection, the screens will hiss or change.

- Hold your tablet in **portrait mode** if you've held it in landscape mode up to this point
- Individual screens now change through
- Tap "Set Up Later", some screens are now displayed again without you having to do anything

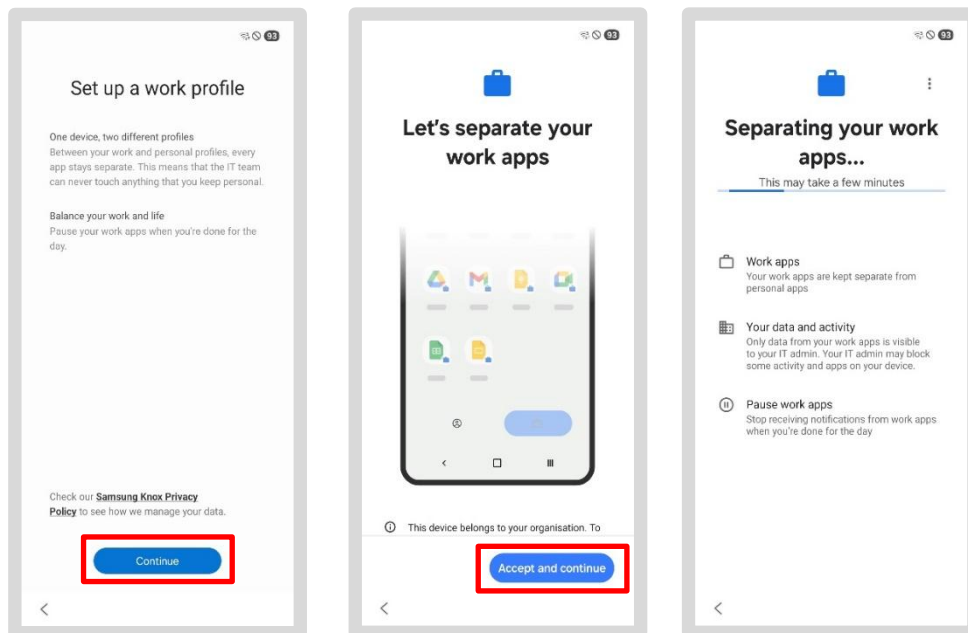


> Go to [Chapter 4.1 Setting Up a Work Profile](#)

4.1 Set up your work profile

In order for the work apps to be assigned on your smartphone/tablet, you need a work profile. This must be set up here:

- The smartphone/tablet is set up
- Confirm the following query with "Next"
- When "Set up a work profile" appears, tap Next or Agree
- If you see "The IT administrator can control this device & block apps" (the text may be cut off), tap "Next"

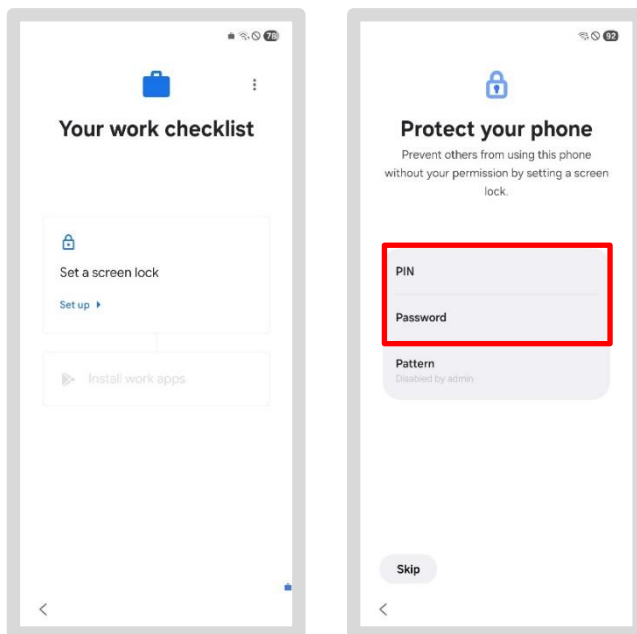


- The update of the smartphone/tablet can take a bit or sometimes a very long time, be patient here!
 - The necessary apps will be installed
- > Go to [Chapter 4.2 Set Screen Lock](#)

4.2 Set screen lock

The next step is to set up the screen lock for your device. This is mandatory at DB for data protection reasons and reliably protects your data.

- Tap Set Up
- Choose for yourself what is the best option for you
- Tap one of the two options (PIN or password), then set your own personal screen lock
- Make sure that the new password is a new combination of numbers has at least 8 digits
- When "Set up biometrics" appears, tap "Skip"

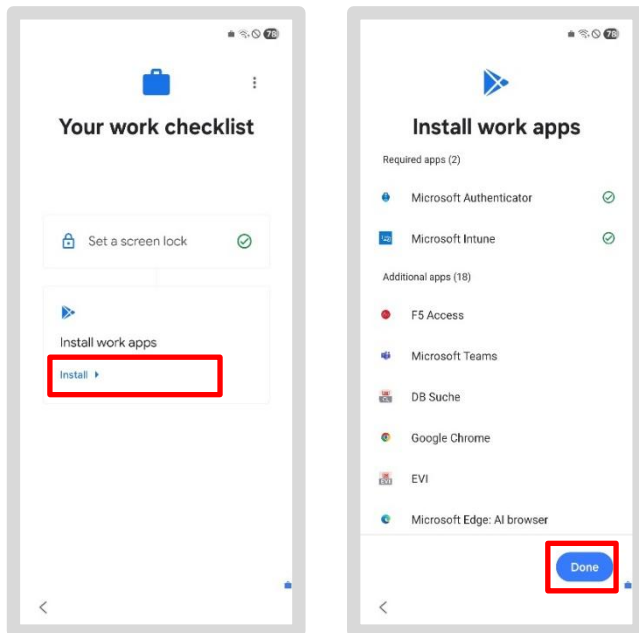


- Pay attention to the privacy and usage information in the initial setup guide
 - Confirm with "Next" and then with "OK" if you enter it twice
 - If the "Private Accounts" screen appears: Tap "Later" when prompting
- > Go to Chapter 4.3 Installing DB Apps

4.3 Installing DB Apps

In the next step , all DB apps will be installed again for your DB smartphone/tablet.

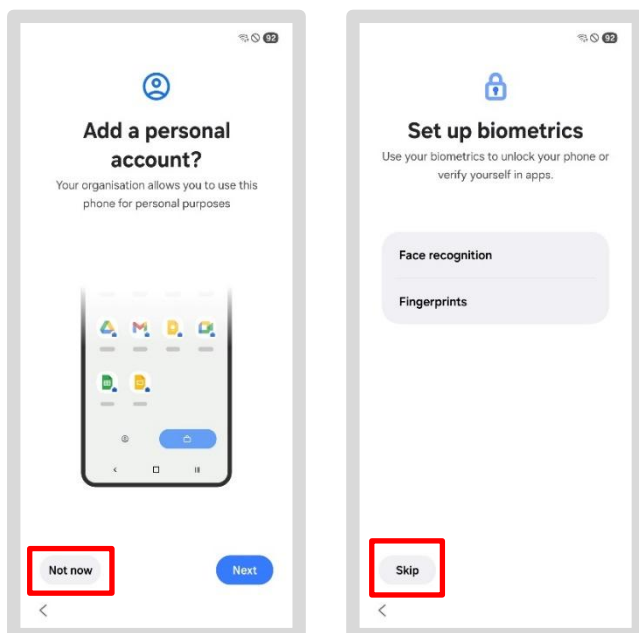
- Tap Install, then tap Done



> Go to Chapter 4.4 Google Account – Not Necessary

4.4 Google Account – Not Necessary

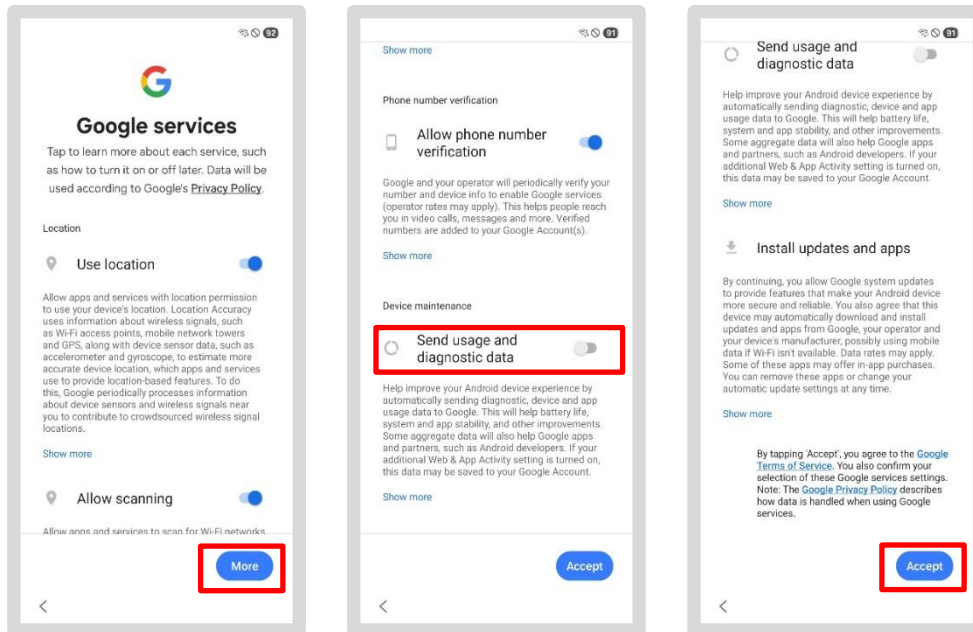
- No **personal** Google account required! Tap Later
- Therefore, tap on "Skip" in the next step



> Go to Chapter 4.5 Activate Google Service

4.5 Activate Google service

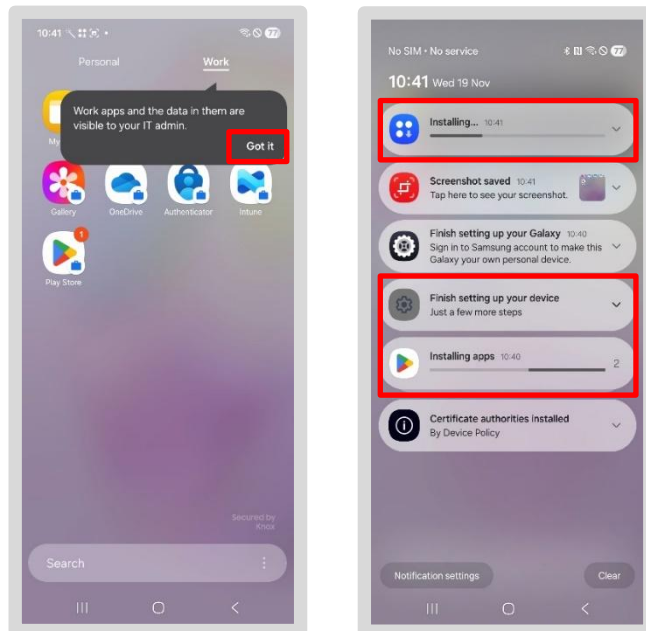
- Tap More in Google Services
- Send **usage and diagnostic data**: To turn it off, tap the slider
- Keep scrolling, then tap Accept



> go to Chapter 4.6 Completing the Setup - Optional

4.6 Complete setup - optional

- Swipe up your screen to see the Personal/Work section
- Tap All Right
- Swipe down your screen to see if there are any apps still loading or installing
- Tap the notification and you'll see how many apps are left to install



- **Note:** "Complete setup of your device" is not necessary to set up your DB smartphone/tablet. Ignore it!
- Wait here for a while until all the apps are installed

Note: if your device doesn't behave like this or shows the screens shown here in the instructions, re-set it again.

> To do this, go to Chapter 2 Start Recovery: Reset Smartphone/Tablet

Important!

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

Get the **Temporary Access Pass (TAP)**
and enter it in the *Intune App* a.

Follow the step-by-step instructions in

> Chapter 5 Activating Device - Creating a Temporary Access Pass (TAP)

5 Activate Device - Create Temporary Access Pass (TAP)

5.1 What is necessary for the creation of the Temporary Access Pass (TAP)

To set up your smartphone/tablet on the DB network, you need these things:

- A valid Temporary Access Pass (TAP)
- Your DB User Name and DB User Password
- the *Intune app*

If you've already created an Access Pass:

- > Go to Chapter 6 Activate Device with the Temporary Access Pass
- > Otherwise, continue to Chapter 5.2 Creating a Temporary Access Pass (TAP)

Just for information:

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

- > If you **have forgotten your DB User password**, you can reset it under db.de/password

Alternatively: Open the *DB Mobile Info* app on your old smartphone/tablet, select the "Service" tab and tap on the line "Reset DB User Password"

- > To **change your password**, see DB User Change Password
- > How to **get your DB User** can be found in Precondition: DB User
- > Your "**DB User Name**" can be found in DeBI under: db.de/debi

5.2 Create a Temporary Access Pass (TAP)

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

Variant 1:

You have a second smartphone/tablet or a DB Workplace Windows or Mac that is logged into the DB network. In this case, stay in the current chapter.

Variant 2:

A colleague from the same company (z.B. DB sales) will support you if he/she owns a DB smartphone/tablet (or iPhone/iPad) or a DB Workplace Windows or Mac.

- > Go to Chapter 5.3 Create a temporary access pass for a colleague here

Variant 3 - Expert Mode:

You only own one smartphone/tablet and were able to use it to the extent that you created a temporary access pass (TAP) before the reset. Make a note of your access pass.

- > Then go to Chapter 6 Activate Device with Temporary Access Pass (TAP)

Note: Your tap is only valid for 60 minutes and for multiple smartphones/tablets!

Continue with variant 1:

- Open your default browser and go to db.de/tap
- Enter your DB User Name and DB User Password
- Select For Myself and tap the blue button
- Now select "DB Workplace Mobile"
- You'll then see the Temporary Access Pass (TAP)
- Write down the Temporary Access Pass (TAP) on a piece of paper or notebook

Note: The TAP is now valid for 60 minutes and for multiple smartphones/tablets.

Important!

The **TAP** may only be used in the **Intune App** even if you're asked for it in another DB app or device.

- You can now activate your phone/tablet in the *Intune app*
- > Go to Chapter 6 Activate Device with Temporary Access Pass (TAP)

Important!

Your smartphone/tablet is not yet connected to the DB Management (Intune)!

Enter the **Temporary Access Pass (TAP)** in the *Intune App* a.

Follow the step-by-step instructions in:

- > Chapter 6 Activate Device with Temporary Access Pass (TAP)

5.3 Create a temporary access pass for a colleague

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

- Open your default browser and go to db.de/tap
- Enter your DB User Name and DB User Password
- Select "For another DB employee"
- Enter the DB user name of your colleague(s): in and tap on the magnifying glass
- Select the correct colleague(s): in and confirm the entry below
- Tap the blue button

The left screenshot shows the 'Create a Temporary Access Pass (TAP)' screen. It includes a header with the DB logo and a menu icon. Below the title, there is a description of the TAP service. A section titled 'Register' asks for 'DB user login details'. A red box highlights the input fields for 'DB User Anmeldename' (Max Mustermann) and 'DB User Password'. At the bottom, there is a blue button with a right arrow.

The right screenshot shows the 'Create a Temporary Access Pass (TAP) - Person selection' screen. It asks to 'Choose for whom the TAP should be created:'. The option 'For another DB employee' is selected. A red box highlights the search results for 'Max Mustermann', showing details like 'DB User: Name', 'E-mail', 'Department', and 'Company: DB Systel GmbH'. A confirmation checkbox 'I confirm that I have established the employee's identity.' is checked. At the bottom, there is a blue button with a right arrow.

The colleague must now enter his/her DB user password:

- To do this, let the colleague: in to the computer

or

- Give control in *Teams* to the colleague: in
- The DB colleague: enter the DB user password in
- Now select "DB Workplace Mobile"
- You'll then see the Temporary Access Pass (TAP)
- Write down the Temporary Access Pass (TAP) on a piece of paper or notebook

Note: The TAP is now valid for 60 minutes and for multiple phones/tablets. You'll need it later when you set it up in the **Intune app**!

Issue a Temporary Access Pass (TAP) for Lisa Mustermann

The TAP recipient must now sign in.

Sign in

DB user login name
Lisa Mustermann

DB user password

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

← →

Create a Temporary Access Pass (TAP)

y&r3%9=cg2u#

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

Start a new session To the homepage

- The colleague can now activate their smartphone/tablet in the Intune app

> Go to Chapter 6 Activate Device with Temporary Access Pass (TAP)

Important!

Your smartphone/tablet is not yet connected to the
DB Management (Intune)!

Enter the **Temporary Access Pass (TAP)**
in the *Intune App* a.

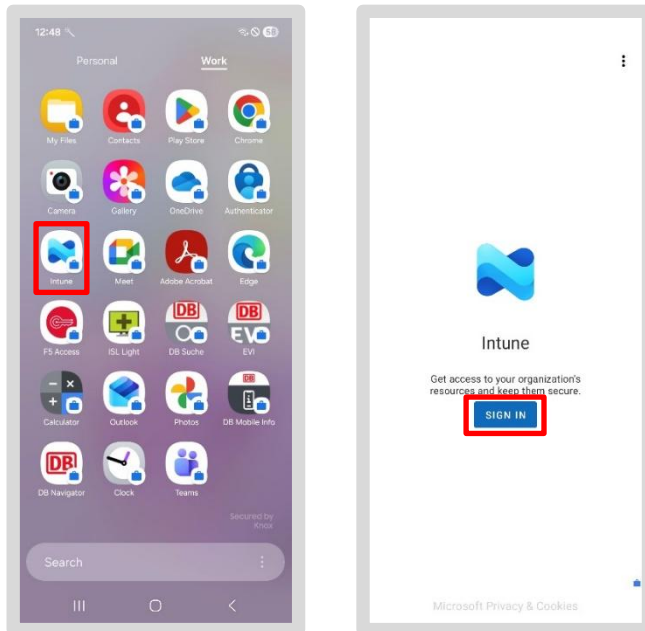
Follow the step-by-step instructions in:

> Chapter 6 Activate Device with Temporary Access Pass (TAP)

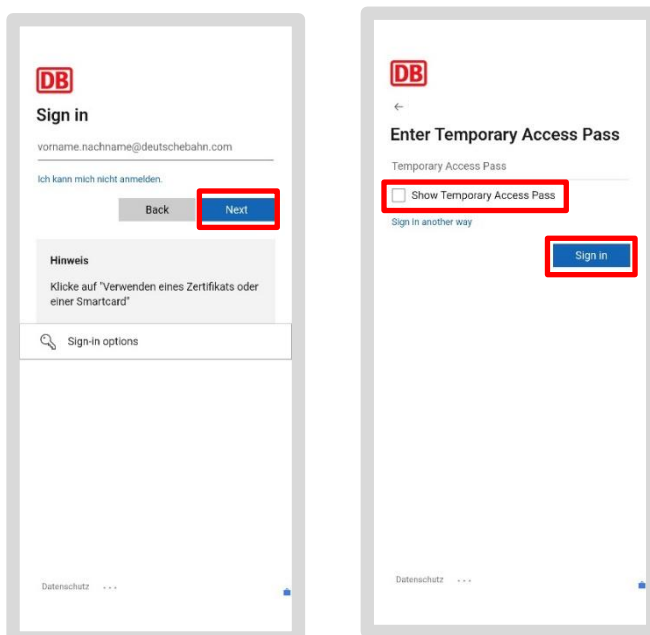
6 Activate your device with the Temporary Access Pass (TAP)

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

- First, check if you've received a Temporary Access Pass (TAP)
- Open the Intune app
- Then tap on the "Sign in" button



- Enter your **DB User email address** (Non: DB User) and tap "Continue"
- **Tip:** Check the box next to "Show temporary access pass"
- Enter your temporary access pass, then tap Sign In



If you get an error message:

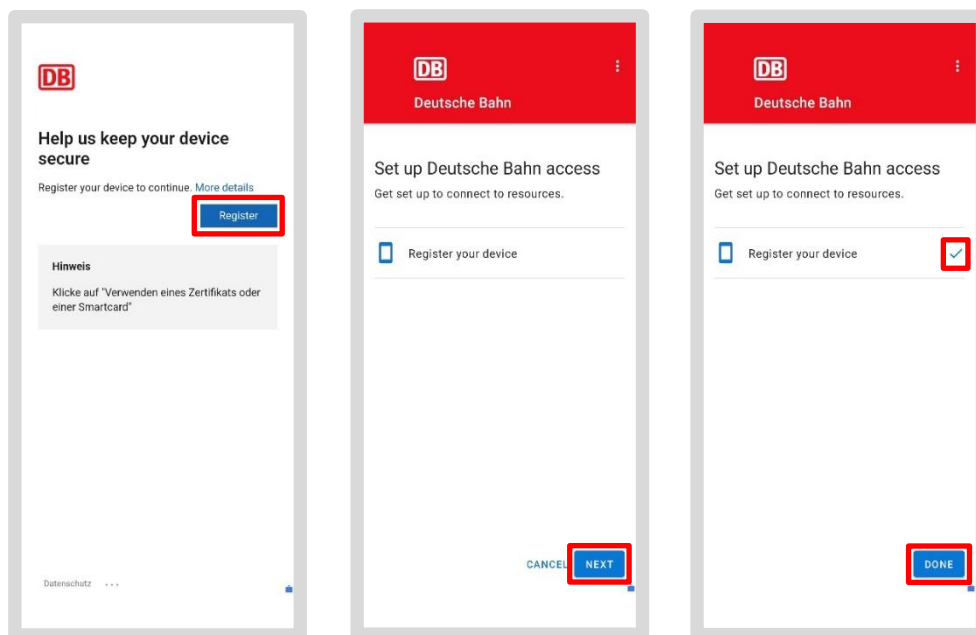
- Create a new TAP and repeat the registration!
- > Go to [Chapter 5 Activate Device - Create Temporary Access Pass \(TAP\)](#) described
- > Otherwise, continue to [Chapter 6.1 Setting up access to all DB apps and websites](#)

Note: As long as the Temporary Access Pass (TAP) is valid (within the 60 minutes) and you, for example, *Outlook*, *Teams* or the *IT ServiceDesk* app, you'll be asked for the Temporary Access Pass, type in your noted Temporary Access Pass here as well.

6.1 Set up access to all DB apps and websites

Now access to DB Management is set up:

- Tap Sign Up, then tap Continue
- When the check mark for "Register device" appears, tap the "Done" button



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

- Open the Intune app again and go through the steps again:
- > [Chapter 6 Activate Device with Temporary Access Pass \(TAP\)](#)

Note: Wait from 5 minutes to 24 hours after registration!

Then all information and certificates have been transferred to the smartphone/tablet and you can use your apps such as *Outlook*, *Teams*, etc.

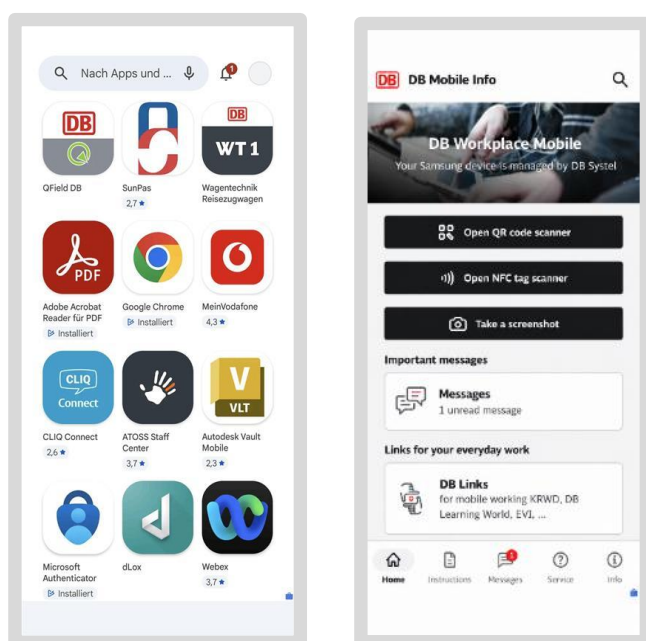
6.2 DB Apps

Note: The provision of the certificates can **take 5 minutes to 24 hours**. Only then can you use your apps, such as *Outlook*, *Teams*, etc.

After the setup is complete, DB apps such as *Outlook* or *Teams* are automatically downloaded. Your company- or business-specific apps are then loaded.

- You can download other DB apps from the official Google Play Store (the app with the suitcase symbol) in the "Business" section
- If you use *ASES* or *ATOSS Staff Center* as a time tracker, here is the guide to the most important functions:
 - > [ATOSS Staff Center - most important functions](#)
- If you use your Deutschlandticket in *DB Navigator*, you can reactivate it in this way:
 - > [Can I transfer the digital Deutschland-Ticket job ticket to another mobile phone?](#)

The **Welcome App** is **no longer** on the DB smartphone/tablet, for which there is the **App DB Mobile Info** with all information, useful links and data about your DB smartphone/tablet.

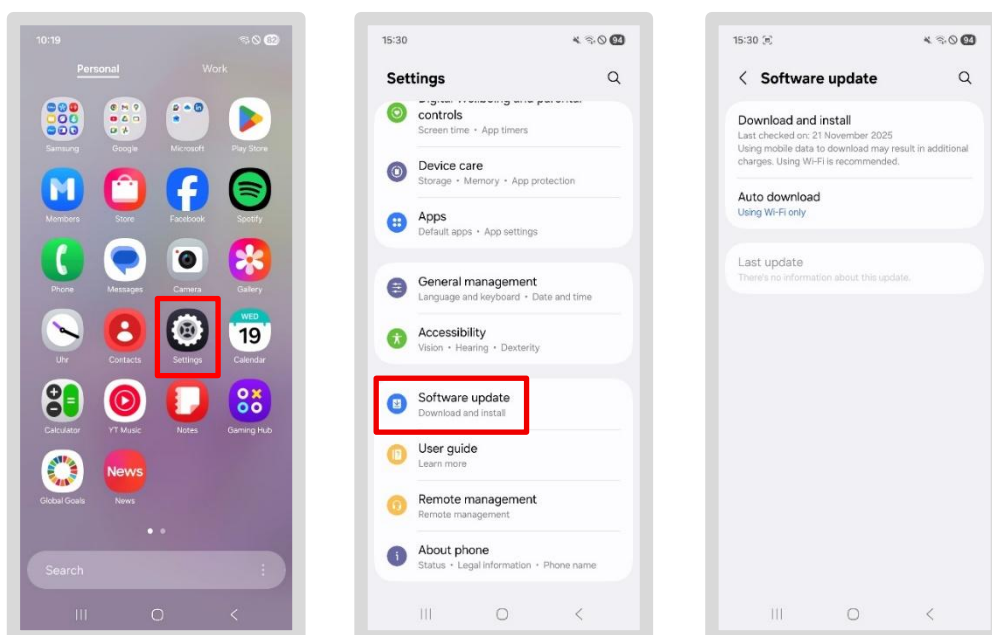


7 Necessary settings

Note: The provision of the certificates can be **5 minutes to 24 hours** . Only then can you use your apps like *Outlook*, *Teams*, etc.

7.1 Install Android OS Updates

- On your phone/tablet, go to the Personal section
- Tap the *Settings app*
- Tap on "System Update" (it says whether an update is offered)
- Perform upcoming updates by tapping "Install Update"



7.2 MS Defender App – Activation required

After activating *Outlook* and *Teams*, activate the app "*Microsoft Defender for Endpoint Mobile*" (MS *Defender App for short*) on your smartphone/tablet. The app protects against cyberattacks and scans existing apps for malicious software. For the protection to be active, open the app 1x.

Due to the large number of different DB smartphones/tablets, there may be slight deviations in the description for individual steps.

Important:

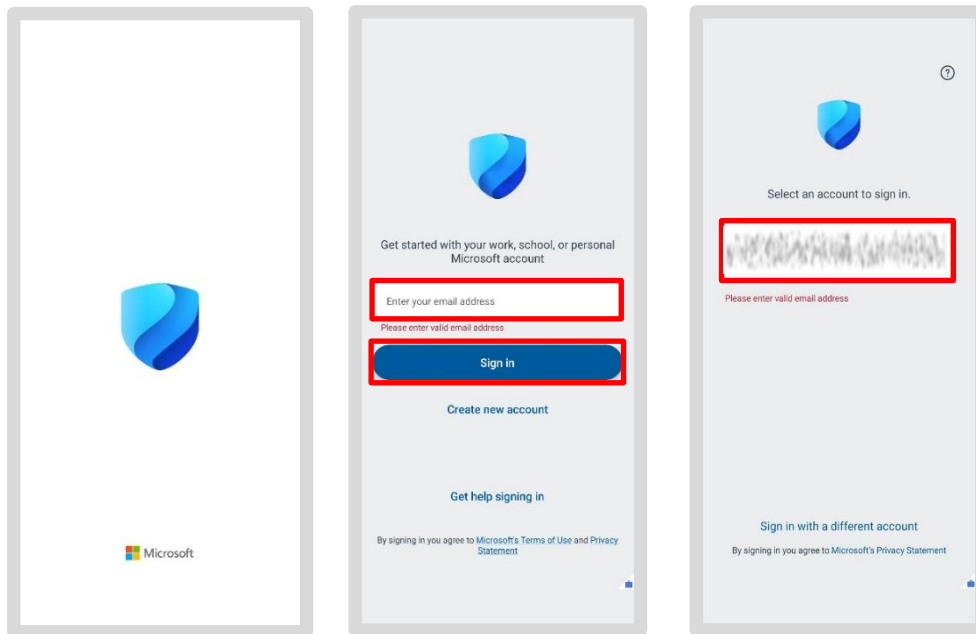
if your iPhone/iPad has the **Defender not enabled** your iPhone/iPad is not compliant with the applicable DB *CSIRT Secure Configuration Policies* and will **to 21 days Be of limited use**.

This means: Apps like *Teams*, *Outlook*, *OneDrive* are **no longer usable**.

Setting up the MS Defender app:

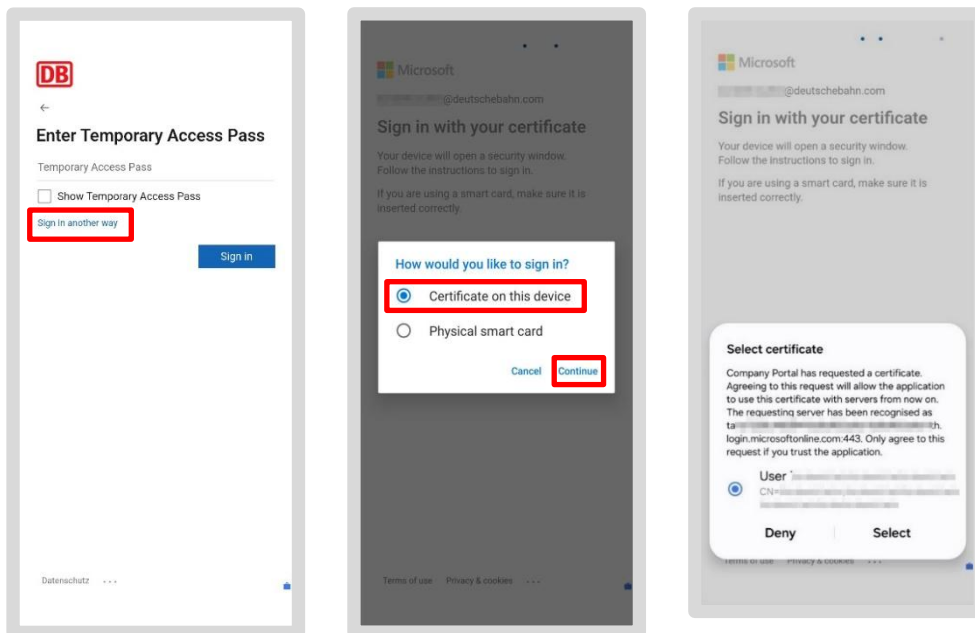
- Go to the Work/Business section and open the "DB Google Play Store"

- Search for the Microsoft Defender: Antivirus app and tap Install
- Tap on the app icon of the *MS Defender app* to open the app
- You will be asked for your work email address
- Tap on the "Sign in" button or the app will automatically redirect 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 an hour, you may be asked to enter your temporary access pass again.

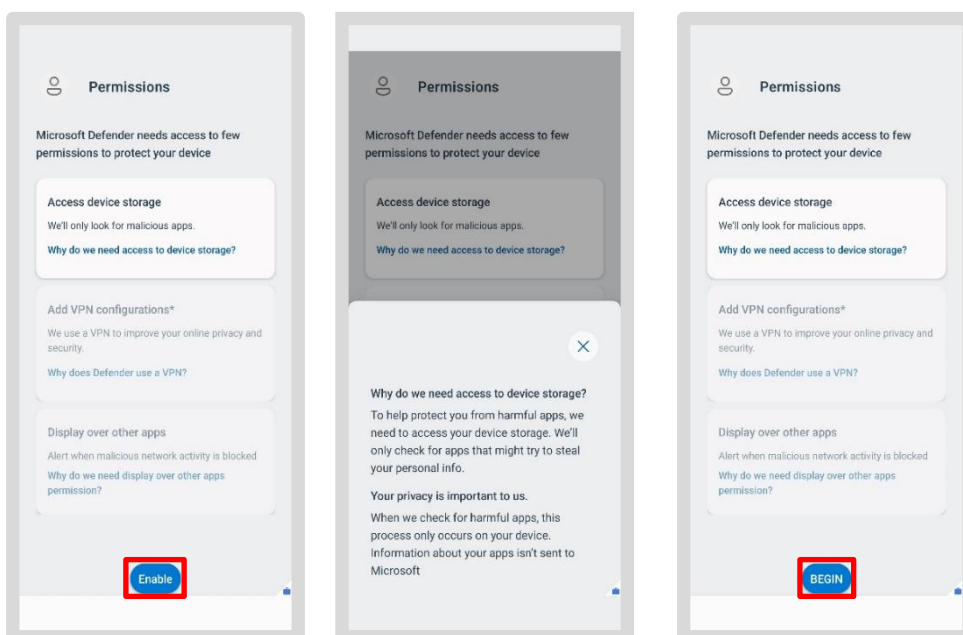
- Tap Sign in in another way
- When prompted, tap Certificate on This Device, then tap Next
- Select the certificate



Assign permissions:

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

- Tap Activate
- Then tap Start
- The Settings app of your smartphone/tablet will open

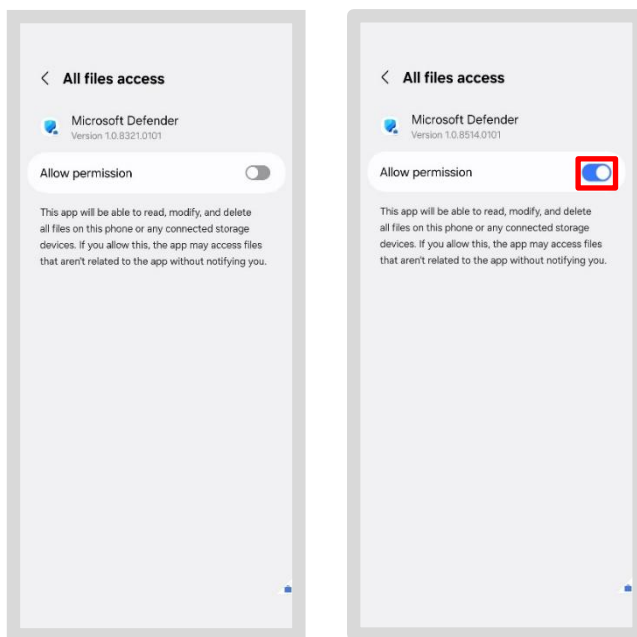


Background Info Permissions:

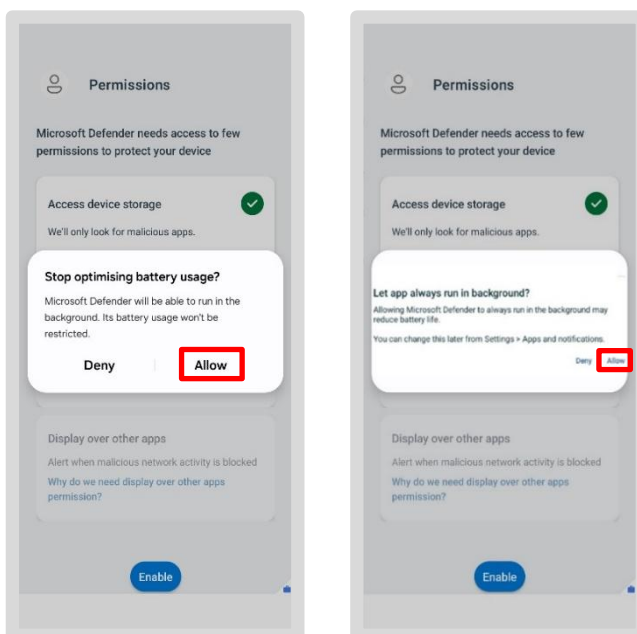
These permissions are required for the application to work properly and ensure security on your device.

You can display an info window for each of the individual permissions (e.g. by clicking on "Why do we need access to the device storage?"). However, some elements are not selectable (they are grayed out, such as "Add VPN configuration") or already activated (green tick, such as "Run in the background"), because they are predefined by the system.

- Now, slide the slider to the right to grant permission
- Tap "Allow" in the subsequent prompt



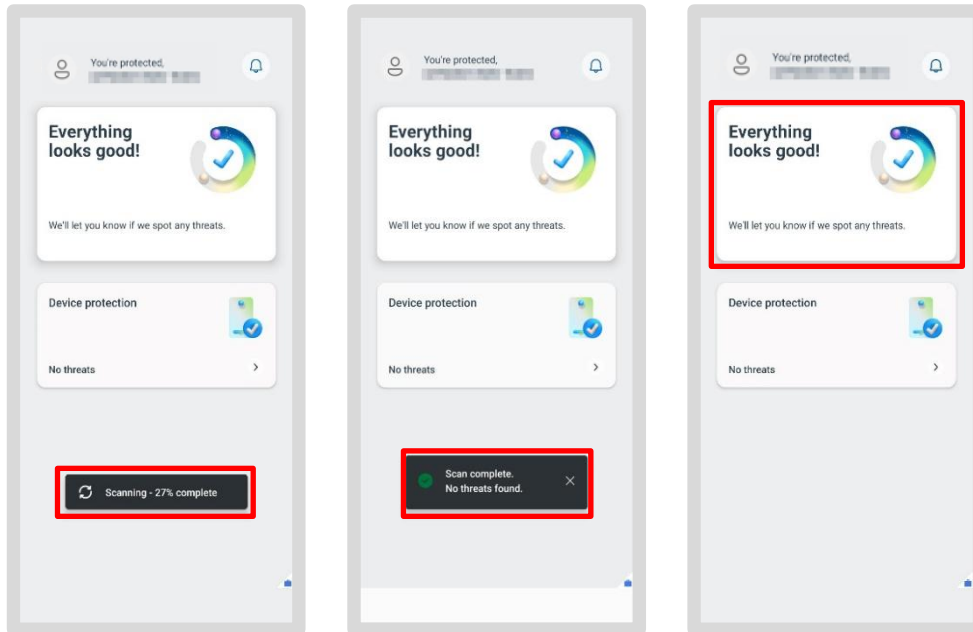
- Tap Allow for each of the following queries



Note: Depending on the device type, different authorizations will be asked! This may only result in one of the requested requests shown.

You will then land on the home page of the *MS Defender app*. A check for malware for your smartphone/tablet will be carried out automatically. Intermediate steps will be displayed during the check.

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



The smartphone/tablet is now protected against malware.

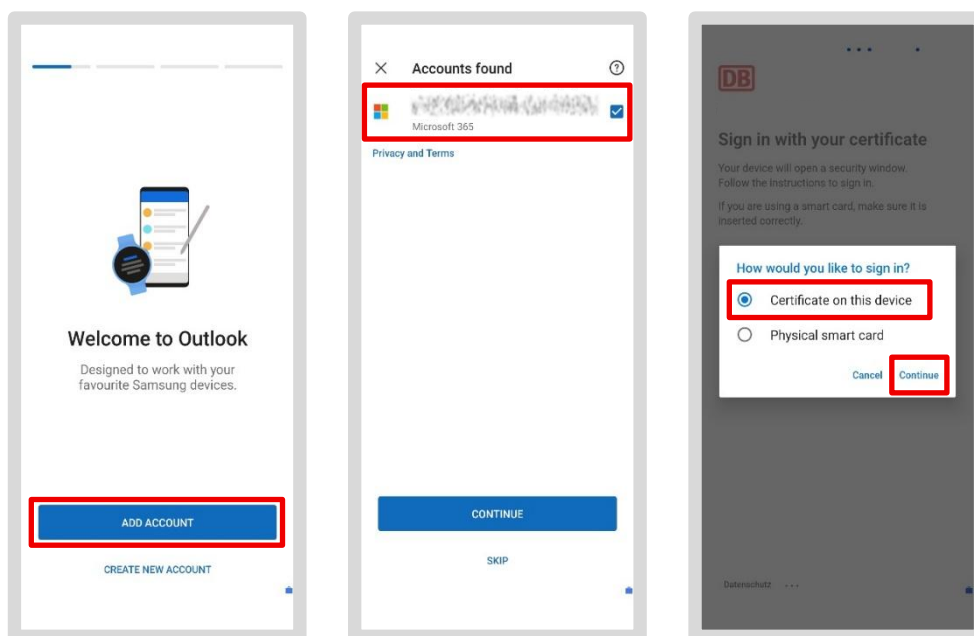
7.3 Setting up Outlook /creating an email account/setting up email encryption

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

- > Do you have questions about writing and sending emails? On ITfit you will find useful tips and instructions on how to use *Outlook*.
- > You are an employee of DB E&C: You have questions and/or there was an error or problems with the certificates, then take a look at DB Questions

To set up Outlook:

- Go to your "Work/Business" section and tap on the Outlook app
- Your email account is automatically saved – tap "Add Account"
- In the next step, select your email address and tap "Next"



When registering, you may be asked for a TAP:

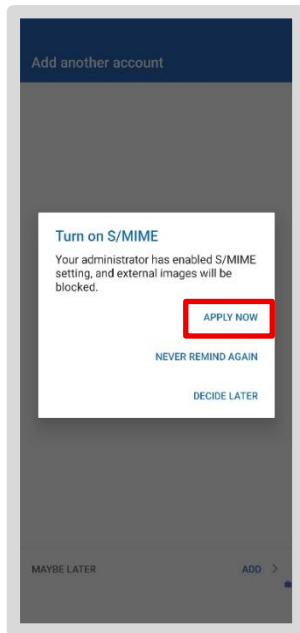
- If your temporary access pass is still valid, enter it here
- > described in Chapter 5.2 Creating a Temporary Access Pass (TAP)

Alternatively:

- Under "*Choose another sign-in option,*" select "*Certificate on this device*"
- Tap "*Select*" when requesting certificates

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 so-called S/MIME encryption for this purpose.

- Tap *Apply Now* on the next query

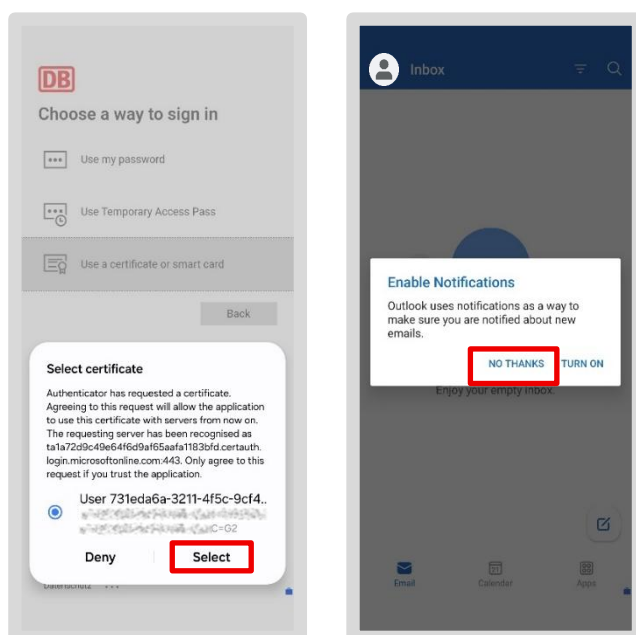


Then comes the certificate request. You can recognize the certificate valid for you as follows:

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

Your email account will now be set up:

- Tap "Maybe Later" when prompting for another account
- And "No Thank you" Activate on notification



- Your emails will now load (this process may take a few minutes)
- Then you can read and write e-mails again

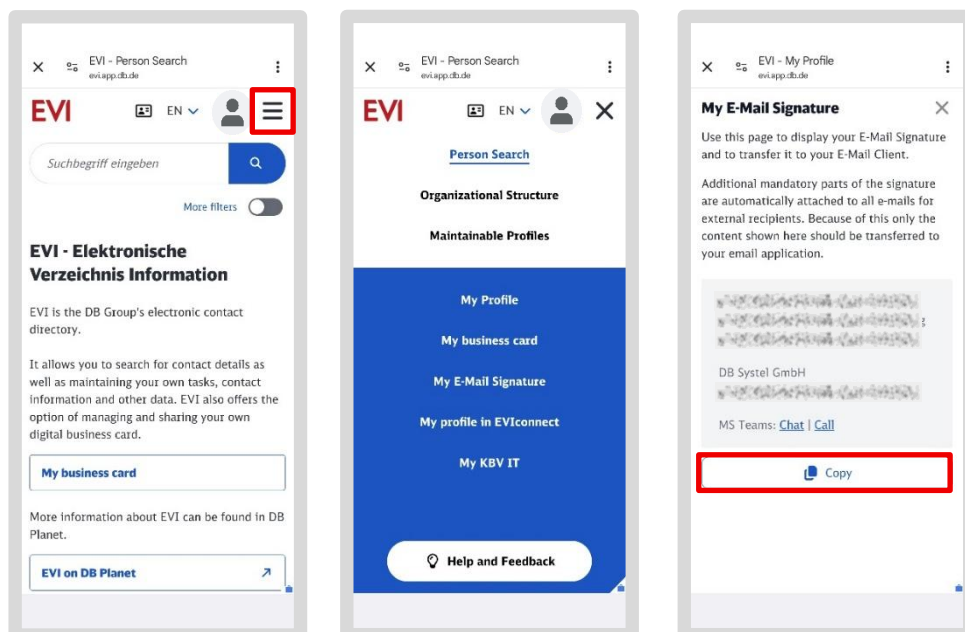
Android 16: For smartphones/tablets running Android 16, it may happen that the step to enable S/MIME is skipped. In this case, the setup of *Outlook* and restart the app! The activation prompt will then appear.

7.3.1 Outlook: Setting up your e-mail signature

An e-mail signature is a mandatory part of official communication. It is at the end of an e-mail and, according to the law, must 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 DB's central telephone book, the so-called "EVI".

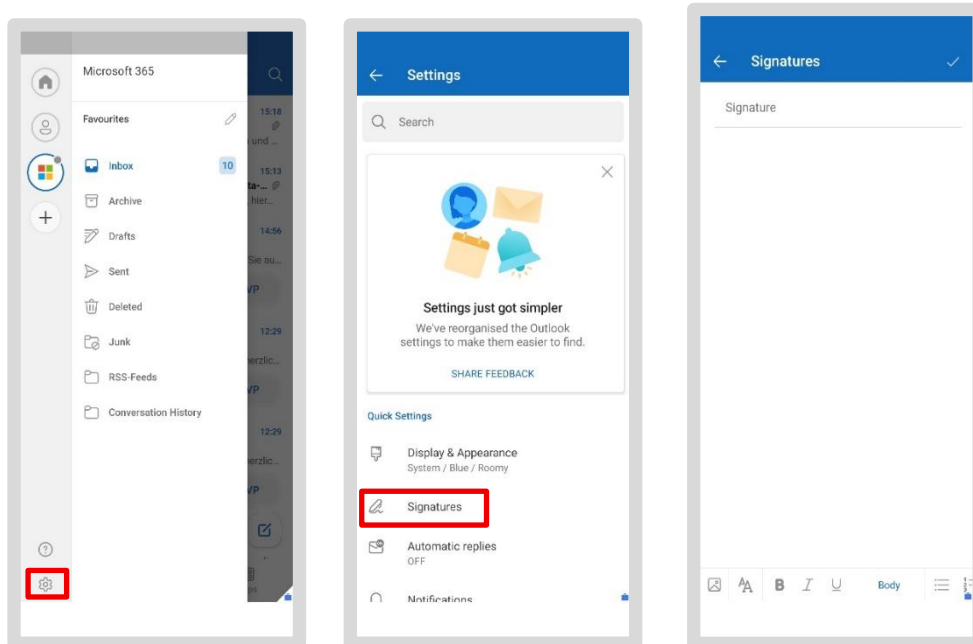
This is how you get your email signature from EVI:

- Open the *EVI* app
- Tap the three lines next to your profile picture in the top right corner
- Then tap *My Email Signature*



Paste the signature in **Outlook** :

- Open the *Outlook app*
- Tap your profile picture in the top left, then tap the gear at the bottom
- Now tap on "Signature"



- A field for the signature will open. If there is already an entry there, delete it with
- Now long tap on the 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 on all new emails

Note: If you've set up multiple email accounts, you can use the slider "*Signature per account*" set up a separate signature for each account. Otherwise, the signature on file will be used for all your email accounts.

7.3.2 Outlook: Synchronize e-mail

All your emails are automatically backed up in the *Outlook app* and synchronized with your connected Office account. This means that no matter which device, whether smartphone/tablet or BKU/Basic Workplace computer, you log in, you are always **up to date**.

7.3.3 Outlook: Create new contacts in

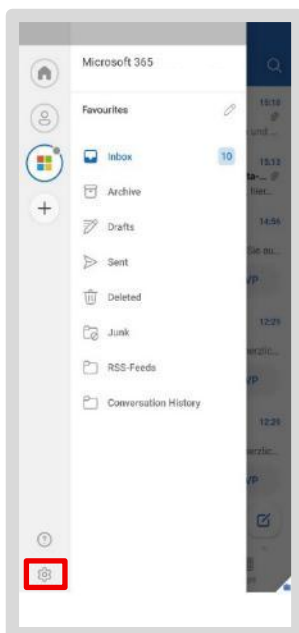
- Go to the Work section and open the Contacts app
- Tap on the "+" to create a new contact
- In the upper-left corner above the arrow, select Outlook
- The new contact will be *Outlook* secured



7.3.4 Outlook: Sync Contacts

If you create a new contact in the "Work/Business" section of your smartphone/tablet via the Contacts app, it is advisable to enable them to be synchronized to *Outlook*. Here's how to do it:

- Open the *Outlook app* in the Work/Work pane
- In the app, there is a circle with an icon in the top left corner - tap it
- An overview of your email folders will open on the left side
- Select the gear in the bottom left corner (the settings will open)
- Under Email Accounts, select your *Outlook* account. Then tap the little slider next to Sync Contacts
- Then confirm the request for access with "Allow"
- After you turn on sync, exit the *Outlook App*



7.4 DB M 365

You can also open and read Word, Excel, PowerPoint or PDF files on your smartphone/tablet. Download the corresponding apps once:

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

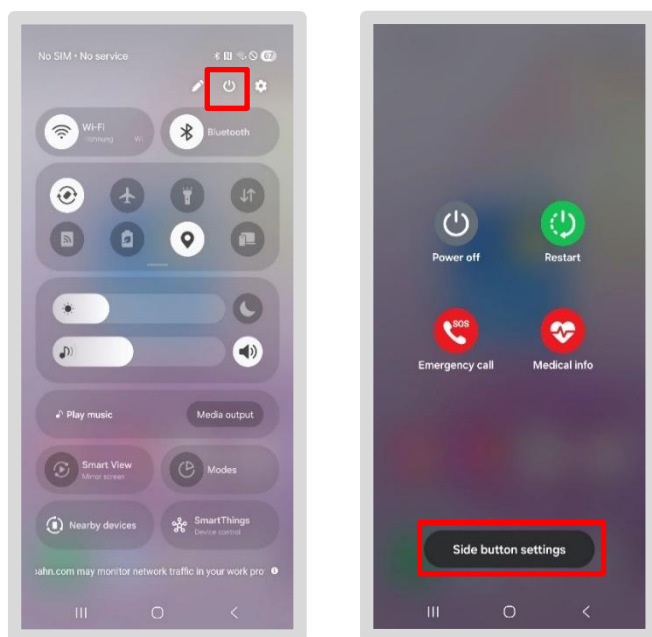


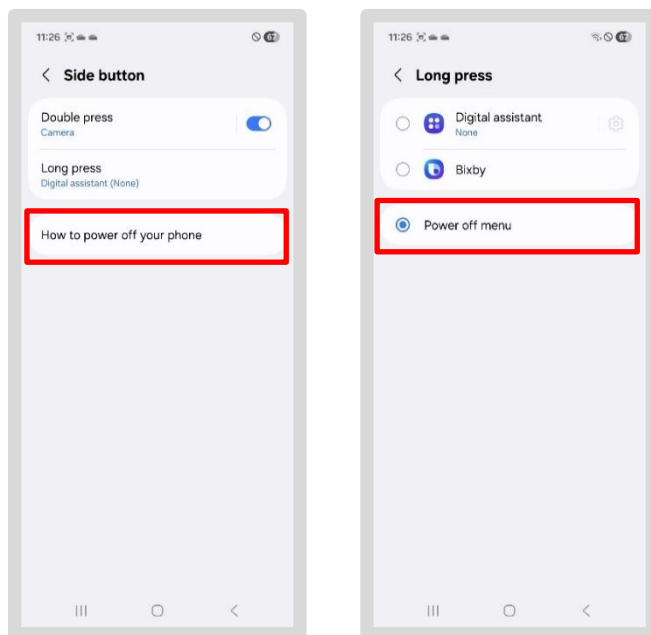
- Then tap on "Install"
- Now, when you open a file, the app opens automatically

Note: You can only open one file at a time. It is e.g. not possible to open several Word files at the same time.

7.5 Turn off the Bixby button

- The power button starts the Bixby voice assistant by default. For security reasons, this must be deactivated:
- Swipe down from the top of the screen. The Control Center will open
- Tap the power icon in the top right of the settings icon
- Select Function Key Settings
- Change the function at "Long press" to "Power off menu"

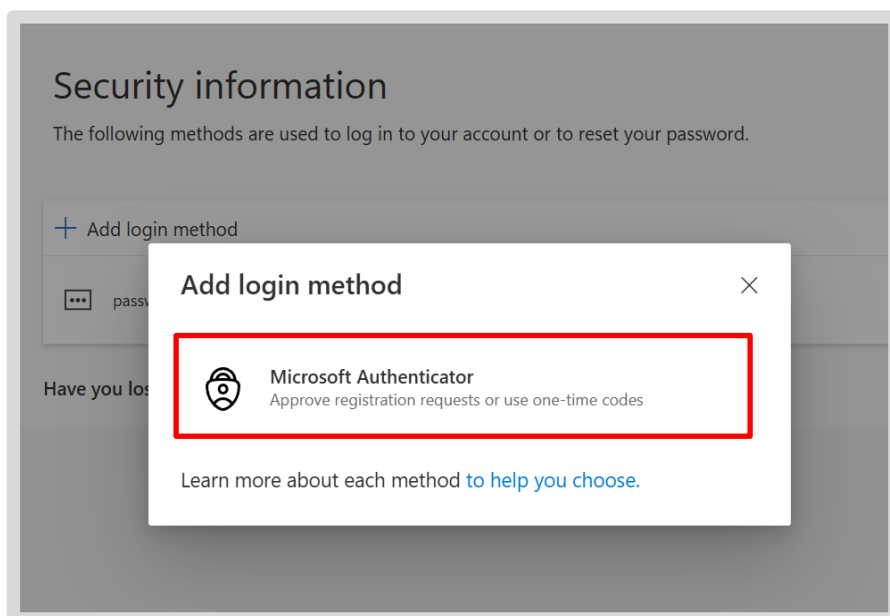




7.6 Re-enable the Microsoft Authenticator app

If you've been using the Authenticator app, follow these steps:

- Tap db.de/authenticator on your BKU or Basic Workplace calculator
- Tap the "Plus icon" and the "Add login method" button
- A dialog will open, select "Microsoft Authenticator"



- Switch to your phone/tablet and open the *Microsoft Authenticator app*
- Open this page for [step-by-step instructions](#) and tap on the "MFA setup guide" button and go through the steps provided

- You can then use the Microsoft *Authenticator app* to authenticate on your smartphone/tablet
- If you have used the **Authenticator app for websites or tools** , activate the app again in the websites

Tip: If you're having trouble reactivating connections in the Authenticator app after recovery, use Self Service: Reset Microsoft *Authenticator App* (MFA): db.de/resetmfa, then follow the steps.

Congratulations!

You have successfully restored your work smartphone/tablet!

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

> To save and reimport your contacts to OneDrive, see the setup guide under [Backup contacts to OneDrive](#)

> You can find a long guide on how to set it up under db.de/mobile-setup