MFA4Daimler - User Guide for use with external Authenticator Apps (dealer/supplier community)

Table of contents

1. About this document

This document describes the installation and use of the multi-factor authentication service "MFA4Daimler" in combination with external authenticator apps.

Multi-factor authentication (MFA) combines several access authorisation factors for enhanced security when users sign-in to applications.
The aim of this multi-stage authentication is to verify the access authorisation of the user with more certainty when logging-in, thereby minimising the risk of account hacking and unauthorised access to sensitive information.

With MFA, access authorisation is verified by at least two independent features (factors).

These factors can be divided into the following categories:

- possession of physical objects such as a hardware token

- secret knowledge such as a password or PIN
- unique physical characteristics or biometric data, e.g. a fingerprint

MFA4Daimler supports the following authentication methods:

Described in this guide:

- Use of an external authenticator app (e.g. Microsoft Authenticator, Google Authenticator, ...) with a mobile device
- Use of an external authenticator app (e.g. WinAuth) with a desktop device

Other methods:

- Use of the "PingID" app with a mobile device (iOS/Android)
    - For more information see the manual "MFA4Daimler_Dealer_Supplier_UserGuide_Mobile"
- Use of a compatible FIDO2 hardware security code with a mobile or desktop device
    - For more information see the manual "MFA4Daimler_UsersQuickGuide_HardwareSecKey"

The following example describes the use of the "external authenticator app" method when logging-in with MFA4Daimler.

2. General notes

To use an authenticator app with MFA4Daimler, it is first necessary to pair the authenticator app with the MFA4Daimler account. Pairing a device creates a relationship of trust between the device and the account.

The following steps are necessary to enable an authenticator app for authentication with MFA4Daimler:

- Download and installation of the desired authenticator app on the device (e.g. smartphone or desktop device).
- Pairing the device.

When this is successfully completed, the authenticator app can be used for authentication when using applications protected by MFA4Daimler.

Couple more than one device

We recommend that more than one device is paired with MFA4Daimler if possible. This ensures that an alternative authentication method is possible if your primary device is not available.
For more information see Managing devices.

Separate the first and second factor

We recommend that you separate the first factor (e.g. user ID/p&assword) from the second factor (e.g. MFA4Daimler - authenticator app) to ensure maximum security.

Example:
When authenticating access to an application with a laptop, we recommend the use of a mobile authenticator app (e.g. Microsoft Authenticator) on a mobile device as the second factor.

3. Applications

In general, all authenticator apps which are able to generate a standard time-based one-time password (TOTP) according to RFC6238) can be used with MFA4Daimler.
This means that most generally known authenticator apps are supported.

The following is a list of generally known authenticator apps:

- iOS devices
  - Microsoft Authenticator
  - Google Authenticator
  - Authy
- Android devices
  - Microsoft Authenticator
  - Google Authenticator
  - Authy
- Desktop devices
  - WinAuth

Examples of different applications are described in the following sections:

- Use with an iOS mobile device, using "Microsoft Authenticator" as an example
- Use with an Android mobile device, using "Microsoft Authenticator" as an example
- Use with a Windows desktop device, using "WinAuth" as an example

3.1. Use with a mobile device

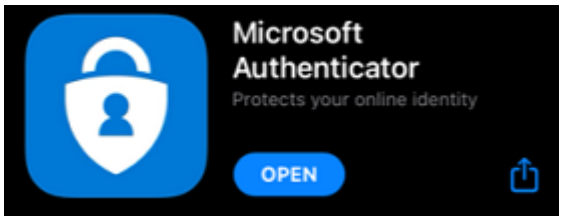
This section describes the use of MFA4Daimler with a mobile device, using the "Microsoft Authenticator" app as an example.

3.1.1. iOS devices

Installation

Install the "Microsoft Authenticator" app on your iOS device:

1. Open the App Store on your device.
2. Search for the "Microsoft Authenticator" app.



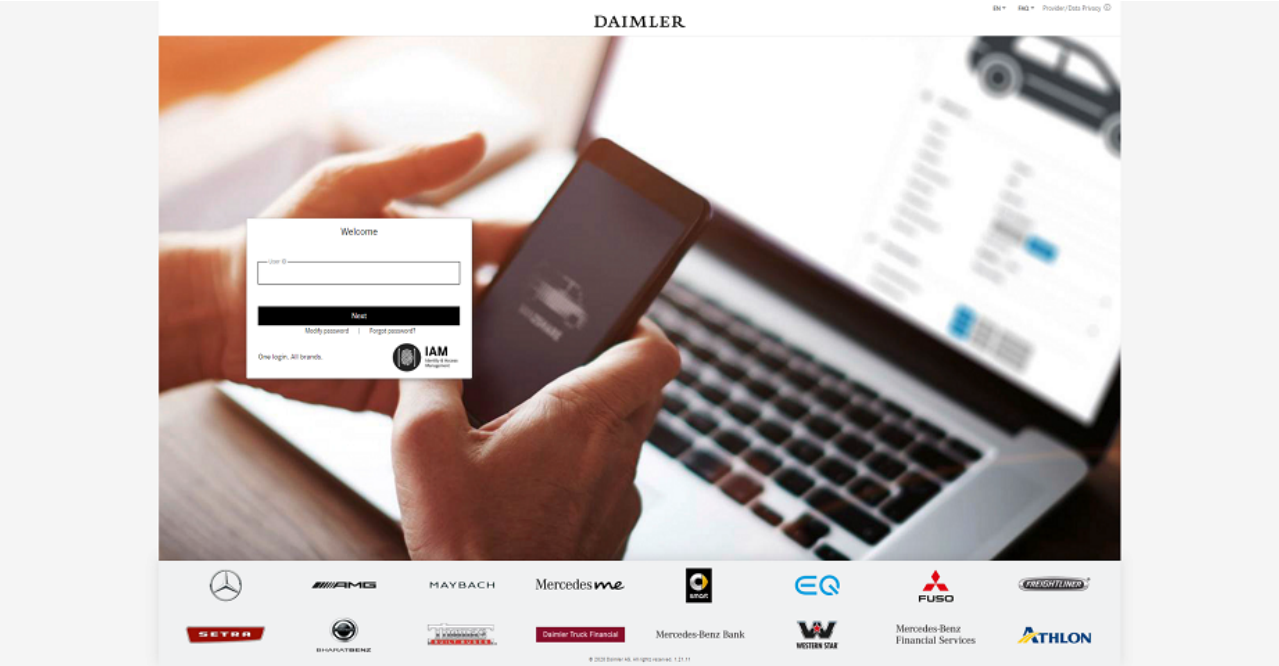
3. Install the app on your device. More information on this can be found here.

Initial pairing

When the "Microsoft Authenticator" app has been installed on the device, initial pairing is carried out by calling up an application protected by MFA4Daimler.

1. Call up an application protected by MFA4Daimler.

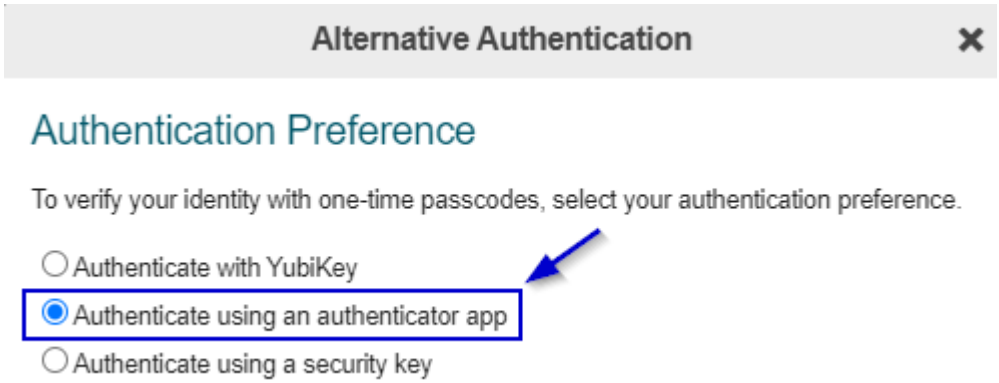
2. Log-in to the corporate web with your user ID and password.



3. After logging-in successfully, you are guided through the initial pairing process with MFA4Daimler.

   To pair an authenticator app, select the link "I want to use a different authentication method".

4. Select the option "Authenticate using an authenticator app".



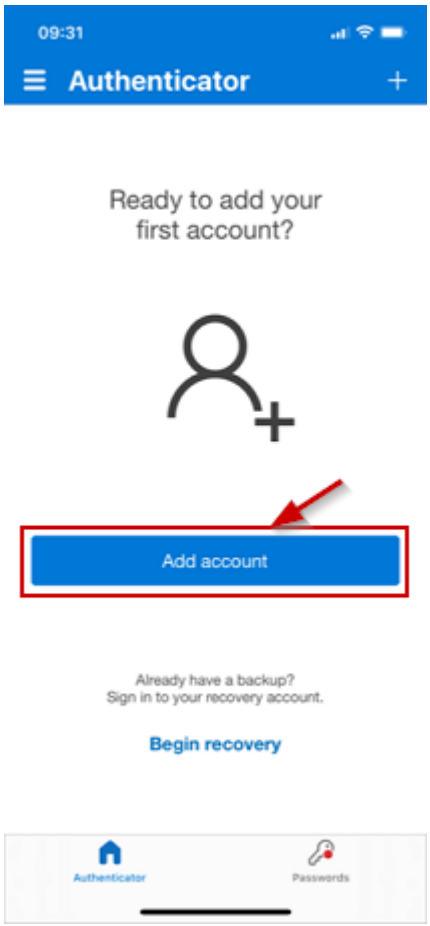
5. Pairing procedure.

   A QR code is displayed to pair your account with an authenticator app.
   You can pair the "Microsoft Authenticator" app either by scanning the displayed QR code with your smartphone, or by manually entering the code.

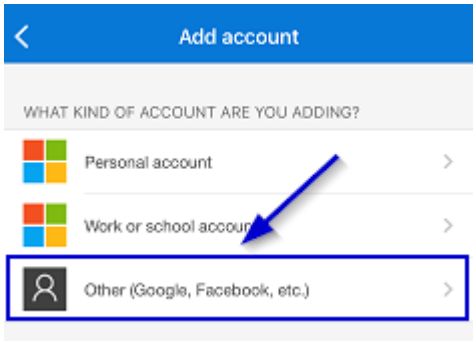
   Start the "Microsoft Authenticator" app to begin the pairing process.
   For information on manual pairing see "5.2".

   5.1 Scan the QR code (the "Microsoft Authenticator" app needs camera access to do this)

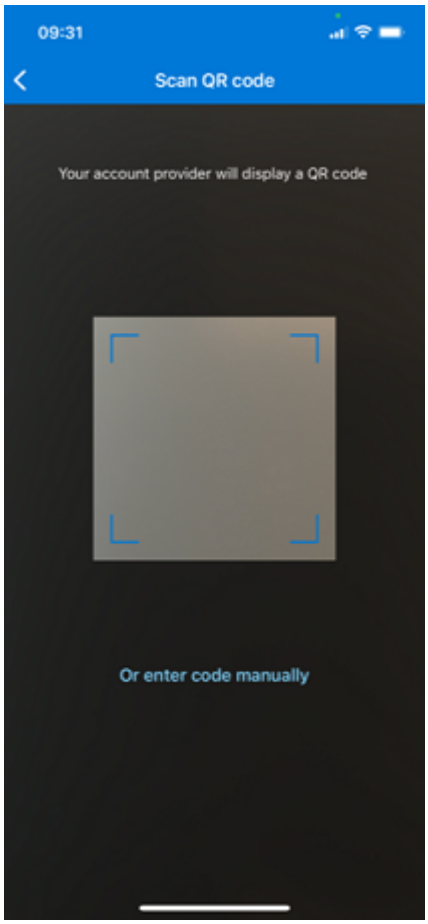
   a) Select "Add account" in the "Microsoft Authenticator" app.



b) For the kind of account, select "Other (Google, Facebook, etc.)".

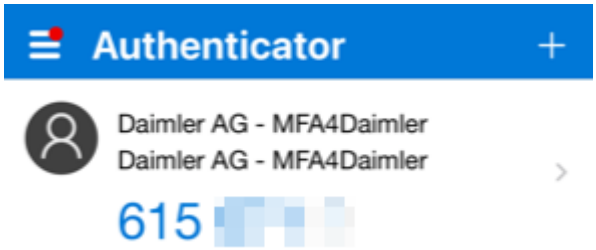


c) The "Microsoft Authenticator" app now expects you to scan a QR code.



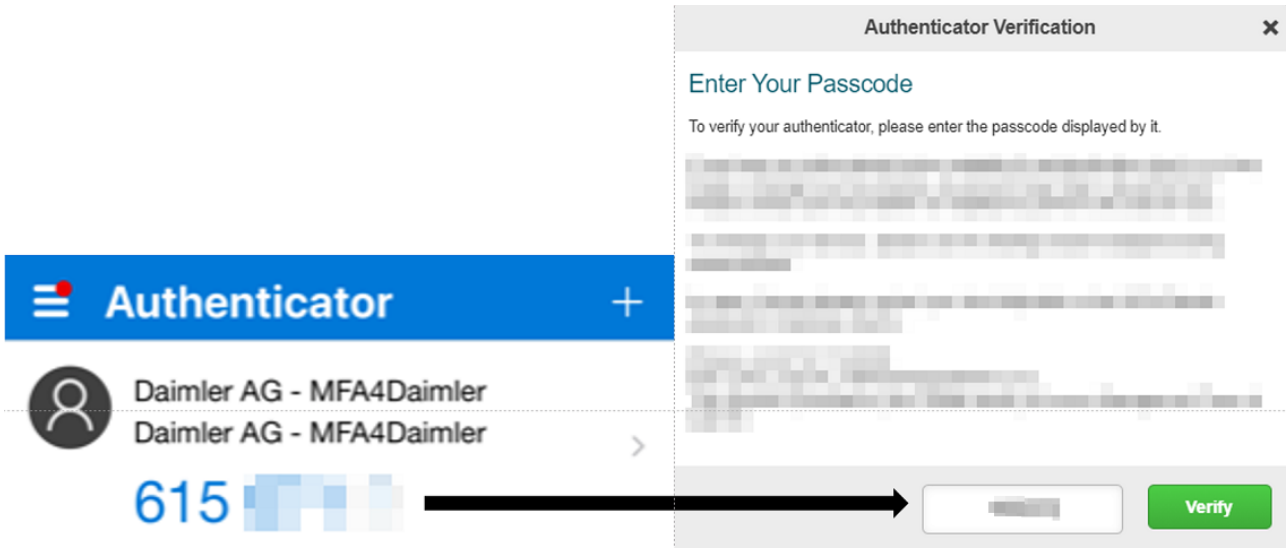
d) Scan the QR code shown in your browser using your mobile device.

e) A new entry (in this example "Daimler AG - MFA4Daimler") appears in the "Microsoft Authenticator" app.

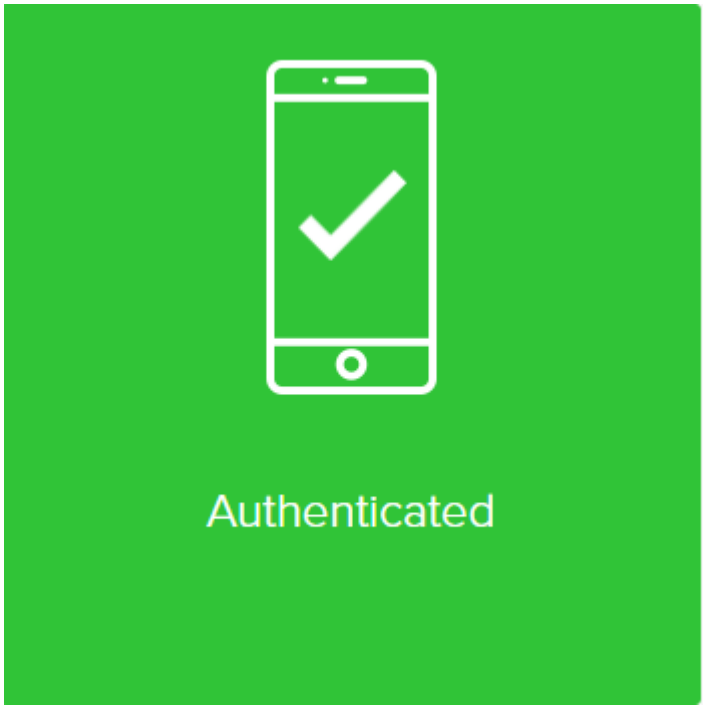


f) Select "Next" in the browser.

g) Enter the passcode shown in the "Microsoft Authenticator" app into the entry field of the browser and select "Verify".

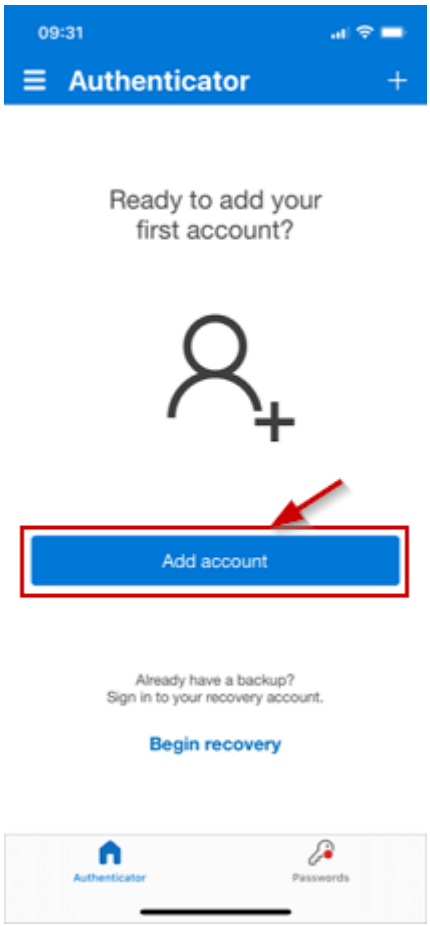


h) Pairing has been successfully completed if the following display appears. In future you can sign-in with MFA4Daimler using the "Microsoft Authenticator" app.

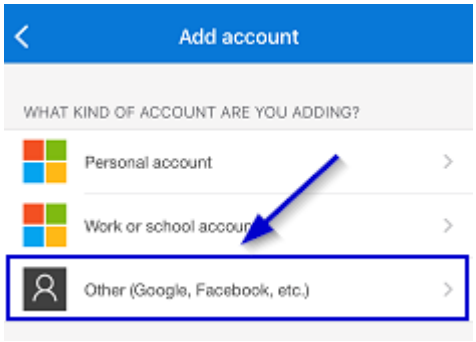


5.2 Manual pairing

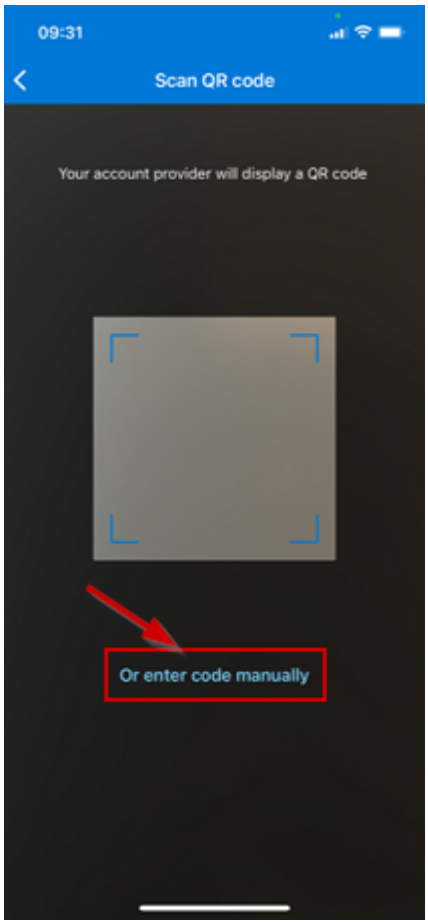
a) Select "Add account" in the "Microsoft Authenticator" app.



b) For the kind of account, select "Other (Google, Facebook, etc.)".

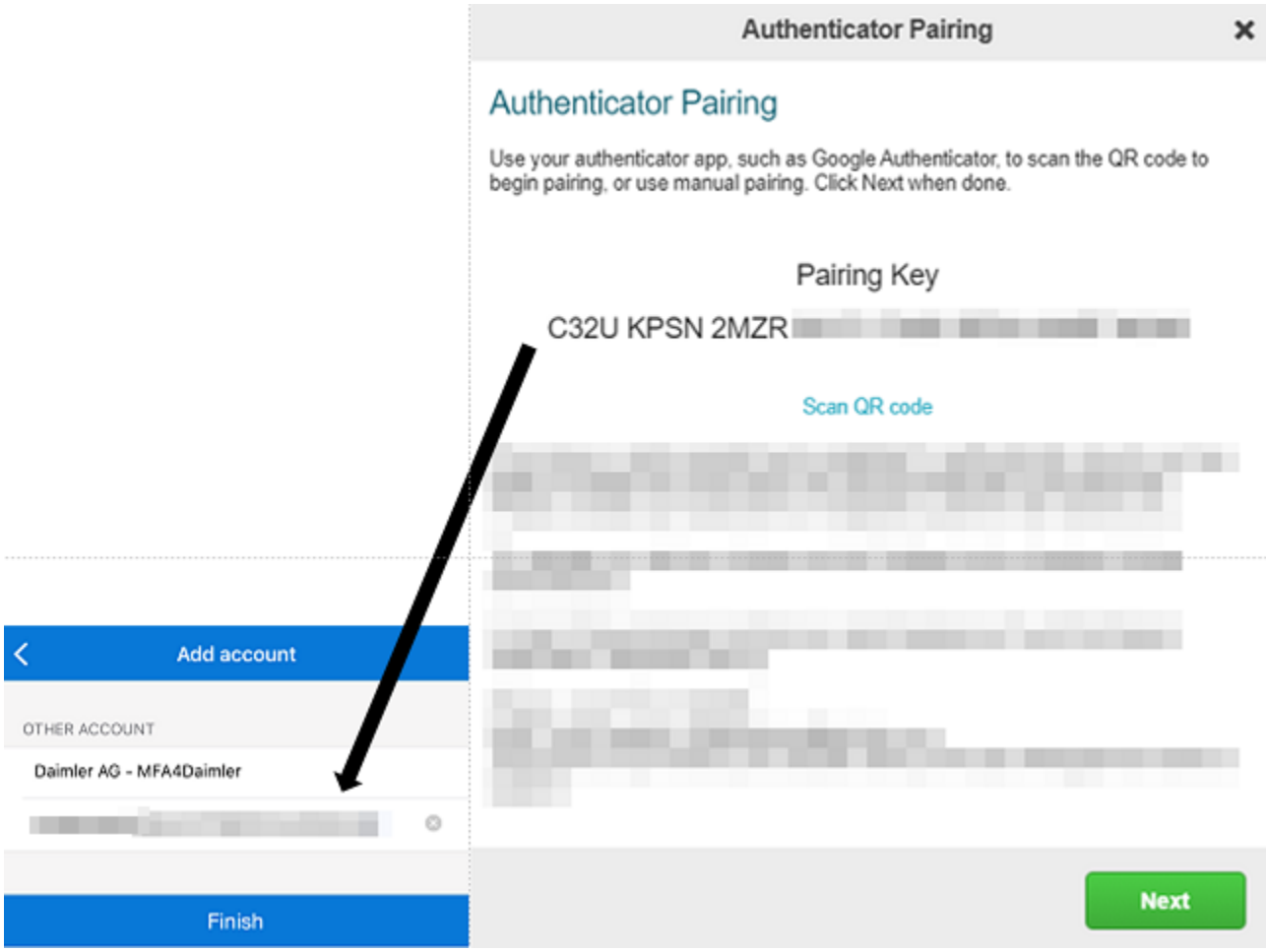


c) The "Microsoft Authenticator" app now expects you to scan a QR code. Select "Or enter code manually" to enter the pairing key manually.

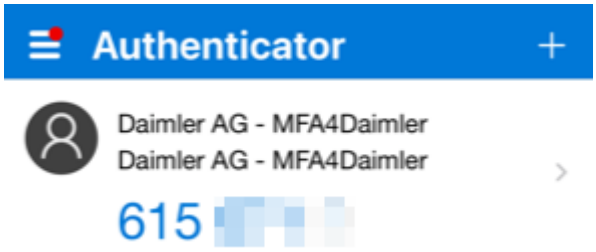


d) Select "Manual pairing" in MFA4Daimler to display the manual pairing key.

e) Enter an account name in the "Microsoft Authenticator" app (e.g. "MFA4Daimler") and enter the pairing key shown in the browser. Then select "Finish".

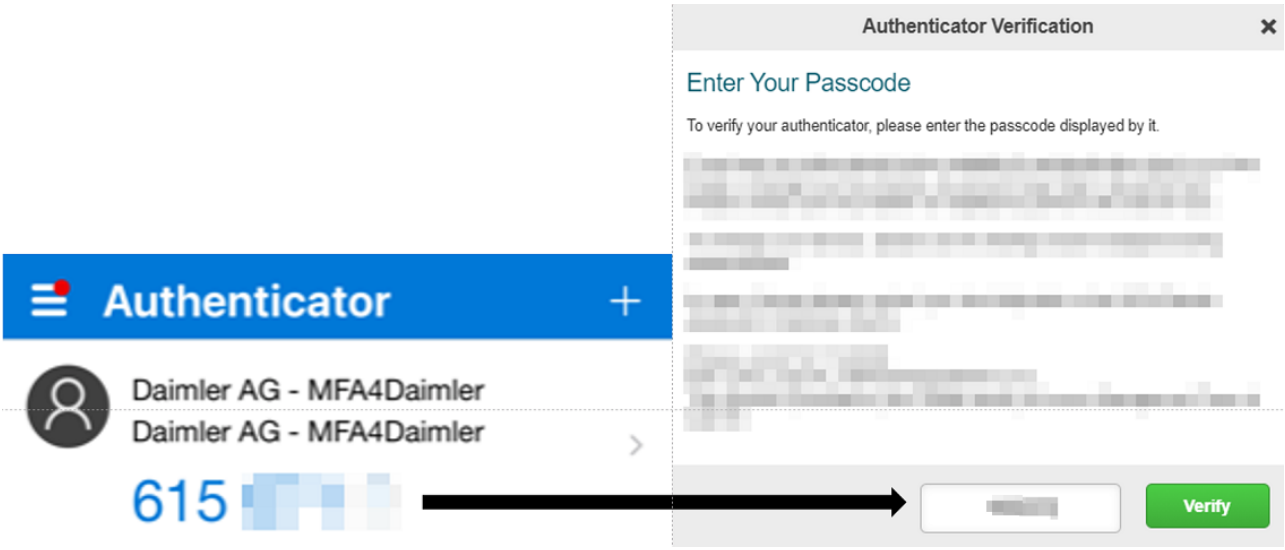


f) A new entry (in this example "Daimler AG - MFA4Daimler") appears in the "Microsoft Authenticator" app.

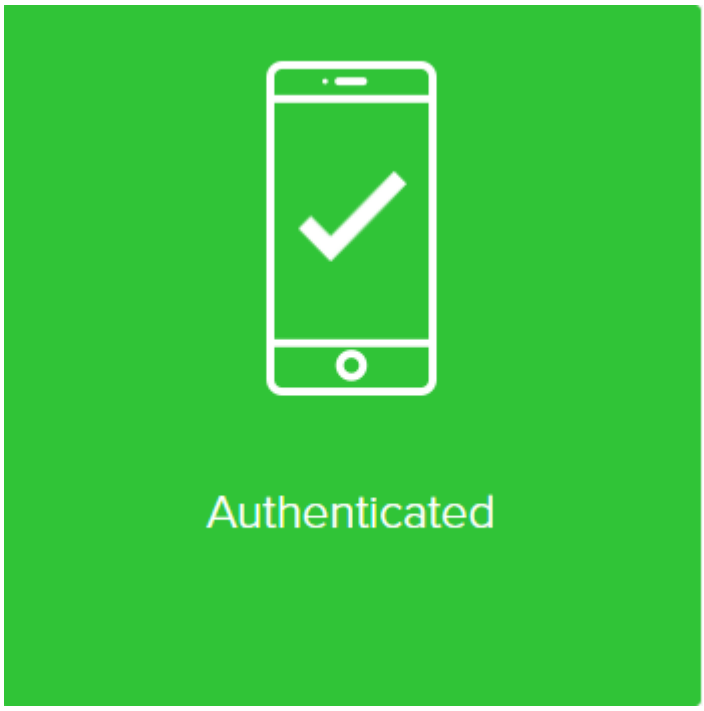


g) Select "Next" in the browser.

h) Enter the passcode shown in the "Microsoft Authenticator" app into the entry field of the browser and select "Verify".



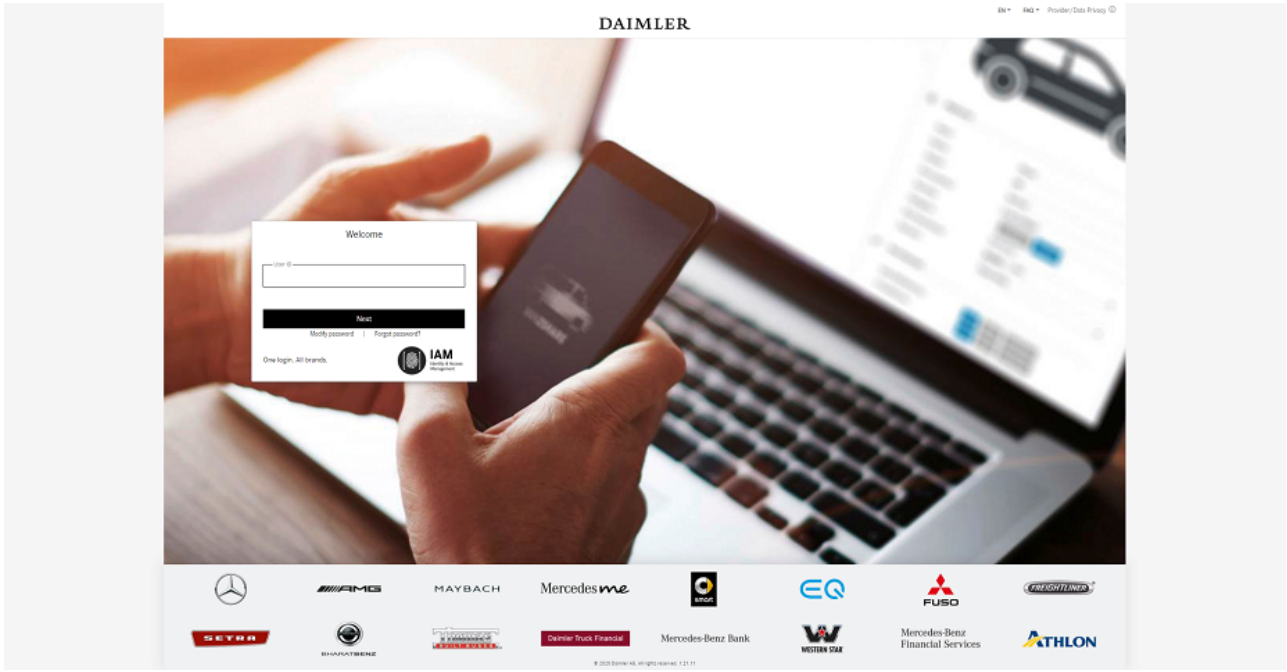
i) Pairing has been successfully completed if the following display appears. In future you can sign-in with MFA4DDaimler using the "Microsoft Authenticator" app.



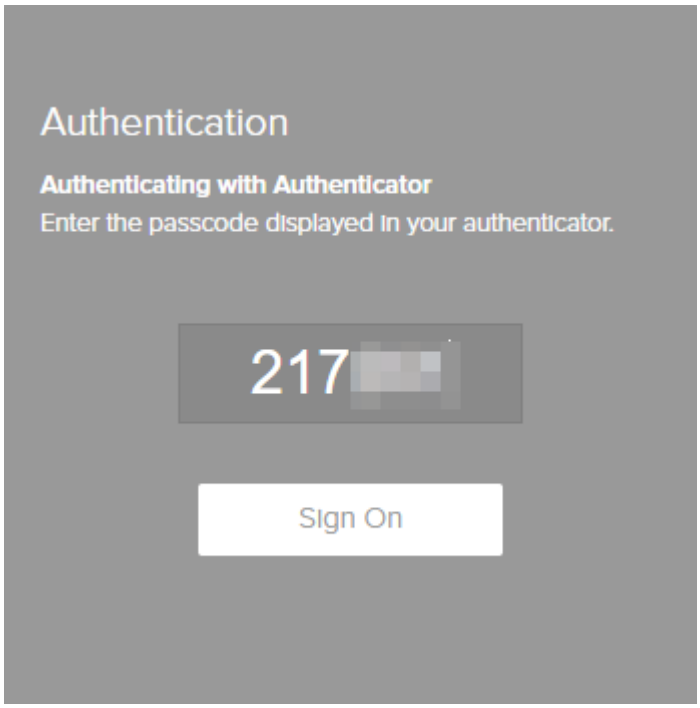
Authentication

Once you have successfully paired the "Microsoft Authenticator" app with your account, you can use it for future authentications with MFA4Daimler.

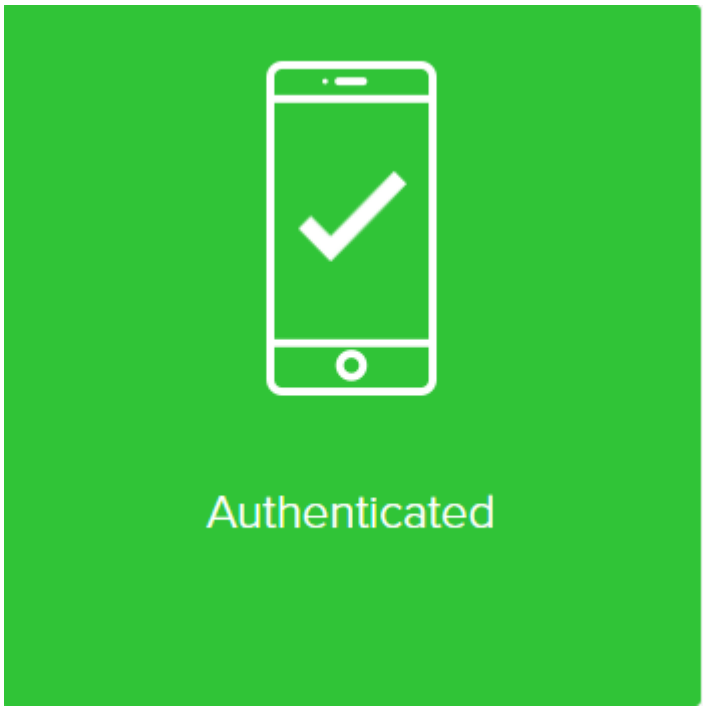
1. Call up an application protected by MFA4Daimler.
2. Log-in to the corporate web with your user ID and password.



3. After logging-in, you are prompted to authenticate yourself using a method paired with MFA4Daimler. Open the "Microsoft Authenticator" app.
4. Enter the passcode shown in the "Microsoft Authenticator" app into the entry field of MFA4Daimler and select "Sign on".



5. You have successfully signed-on if the following display appears. You are then automatically taken to the application.

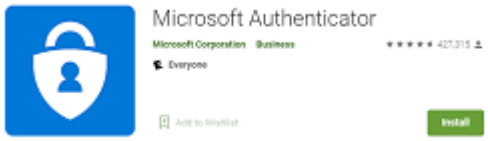


3.1.2. Android devices

Installation

Install the "Microsoft Authenticator" app on your Android device:

1. Open the App Store on your device.
2. Search for the "Microsoft Authenticator" app.



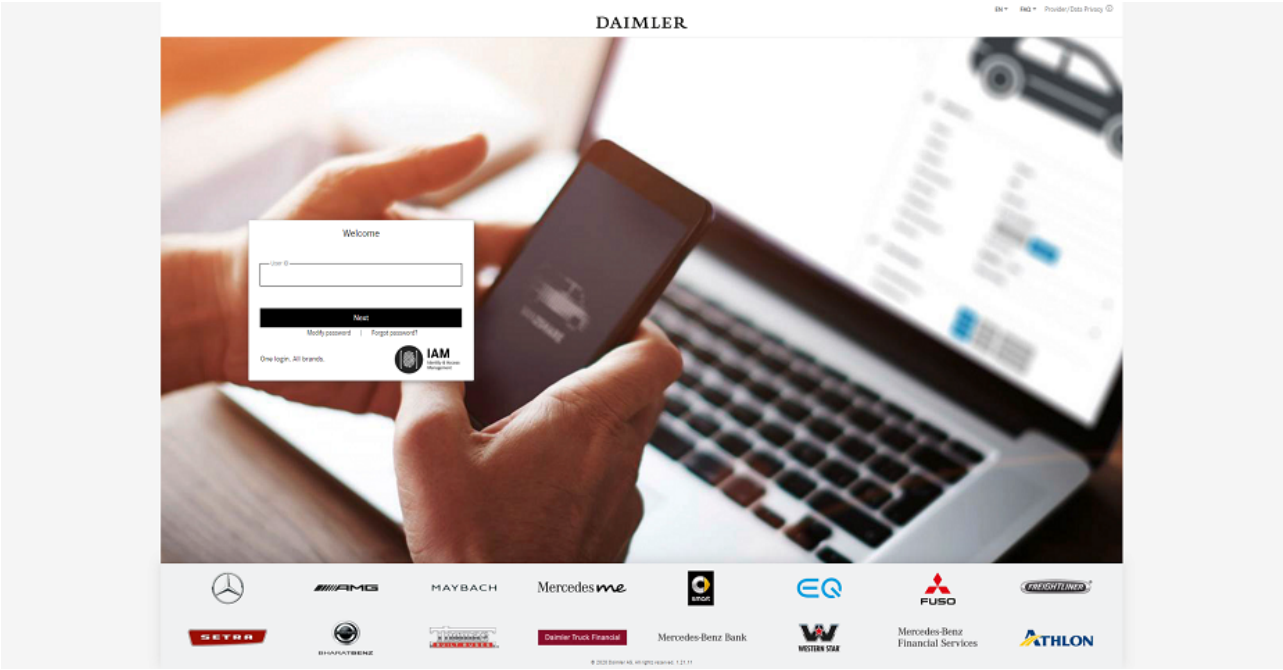
3. Install the app on your device. More information can be found here.

Initial pairing

When the "Microsoft Authenticator" app has been installed on the device, initial pairing is carried out by calling up an application protected by MFA4Daimler.

1. Call up an application protected by MFA4Daimler.

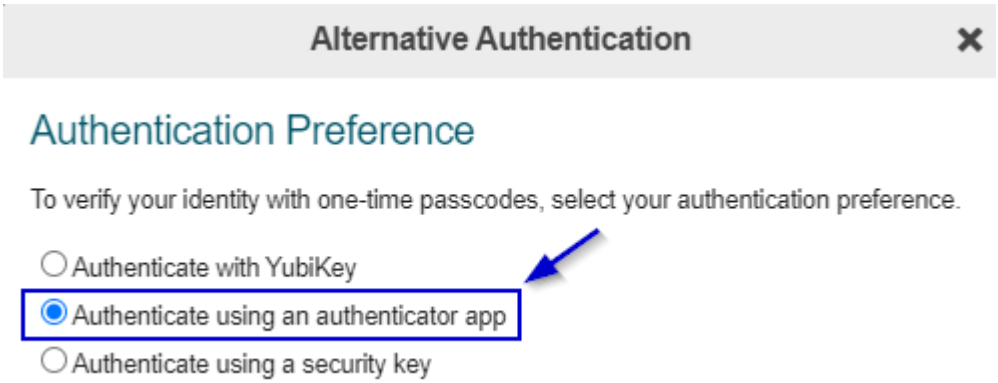
2. Log-in to the corporate web with your user ID and password.



3. After logging-in successfully, you are guided through the initial pairing process with MFA4Daimler.

To pair an authenticator app, select the link "I want to use a different authentication method".

4. Select the option "Authenticate using an authenticator app".



5. Pairing procedure.

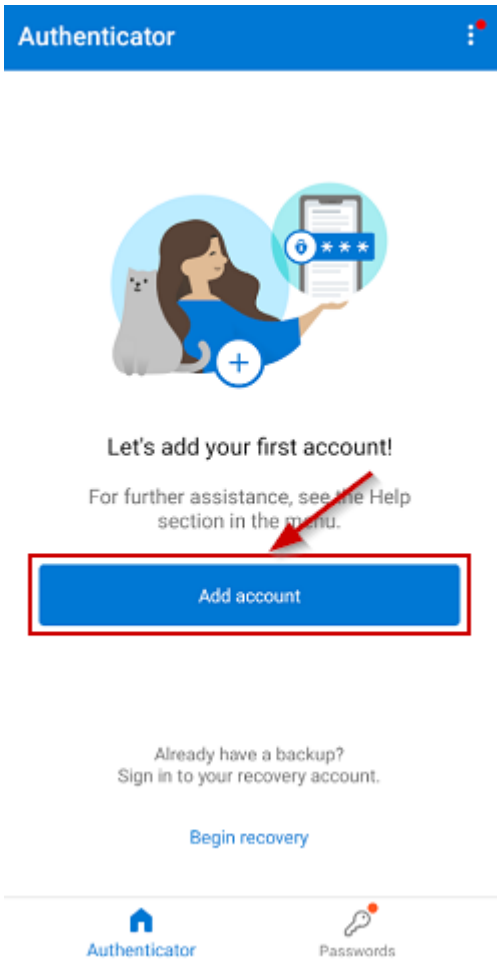
   A QR code is displayed to pair your account with an authenticator app.

   You can pair the "Microsoft Authenticator" app either by scanning the displayed QR code with your smartphone, or by manually entering the code.

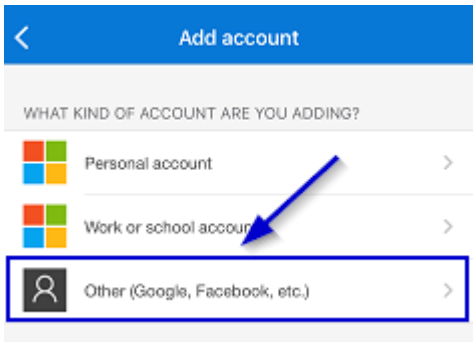
   Start the "Microsoft Authenticator" app to begin the pairing process.

   5.1 Scan the QR code (the "Microsoft Authenticator" app needs camera access to do this)

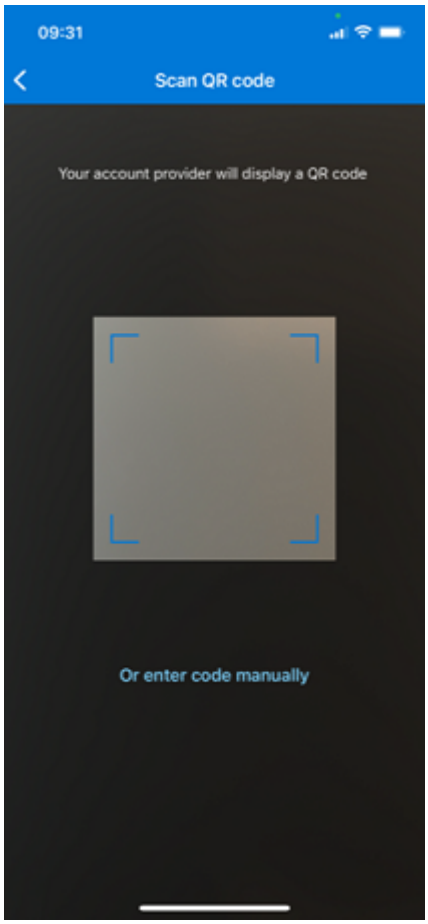
   a) Select "Add account" in the "Microsoft Authenticator" app.



b) For the kind of account, select "Other (Google, Facebook, etc.)".

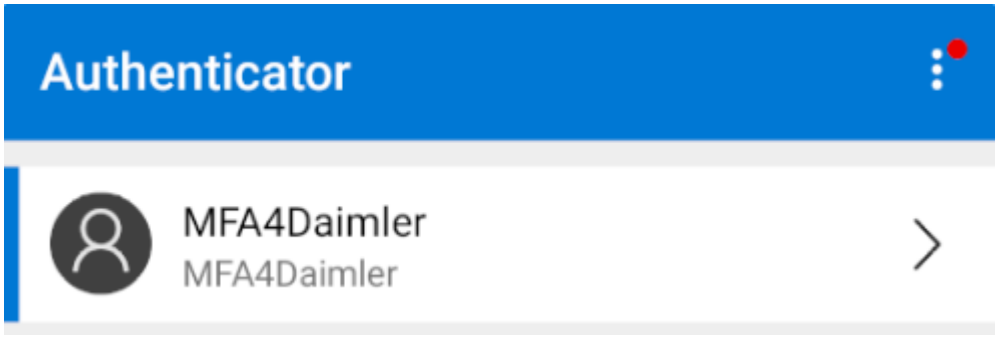


c) The "Microsoft Authenticator" app now expects you to scan a QR code.



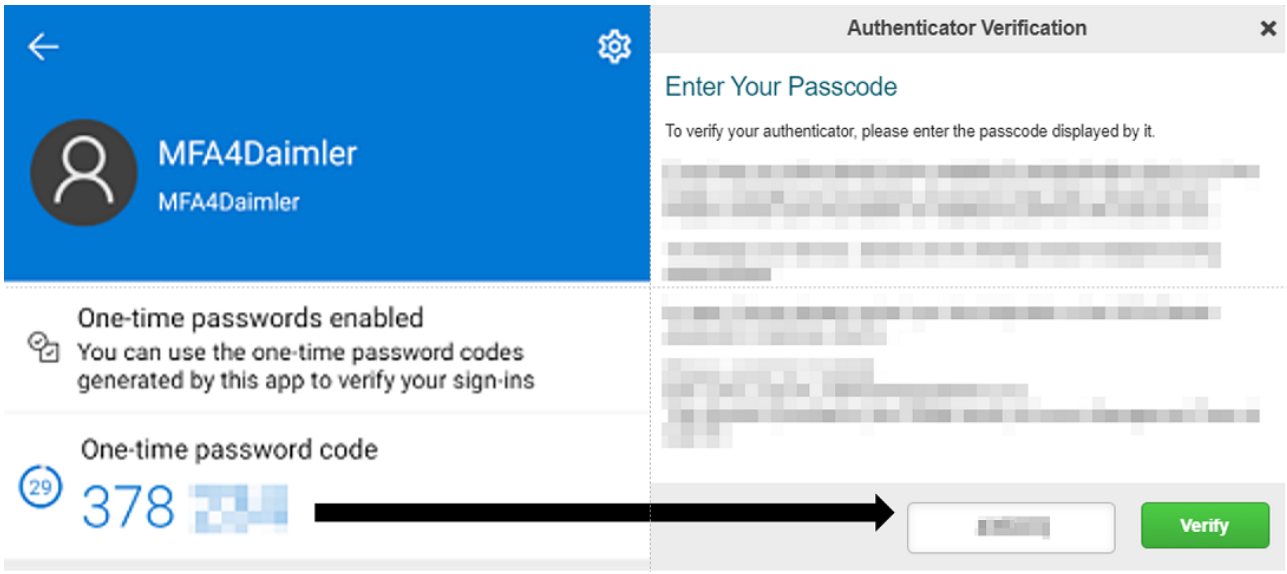
d) Scan the QR code shown in your browser using your mobile device.

e) A new entry (in this example "Daimler AG - MFA4Daimler") appears in the "Microsoft Authenticator" app.

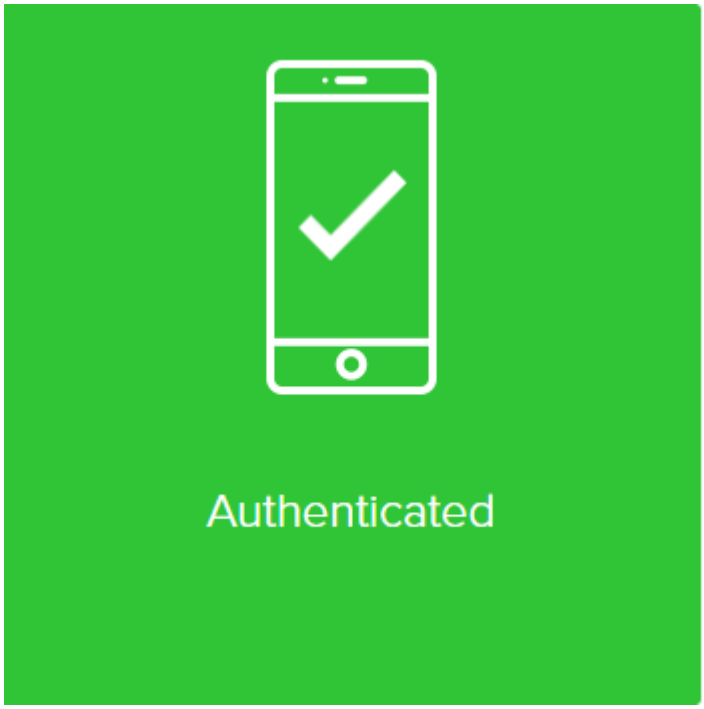


f) Select "Next" in MFA4Daimler.

g) Enter the passcode shown in the "Microsoft Authenticator" app into the entry field of the browser and select "Verify".

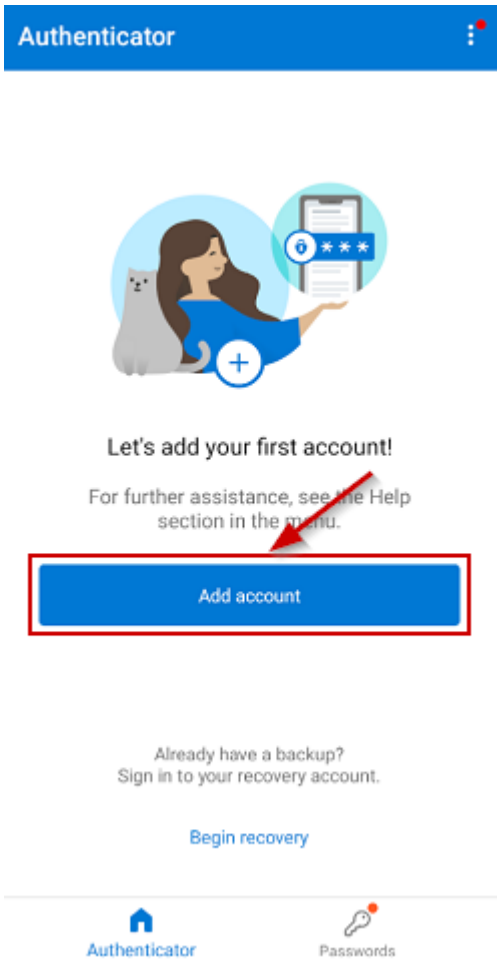


h) Pairing has been successfully completed if the following display appears. In future you can sign-in with MFA4DDaimler using the "Microsoft Authenticator" app.

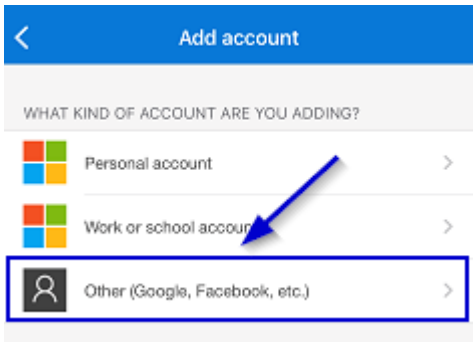


5.2 Manual pairing

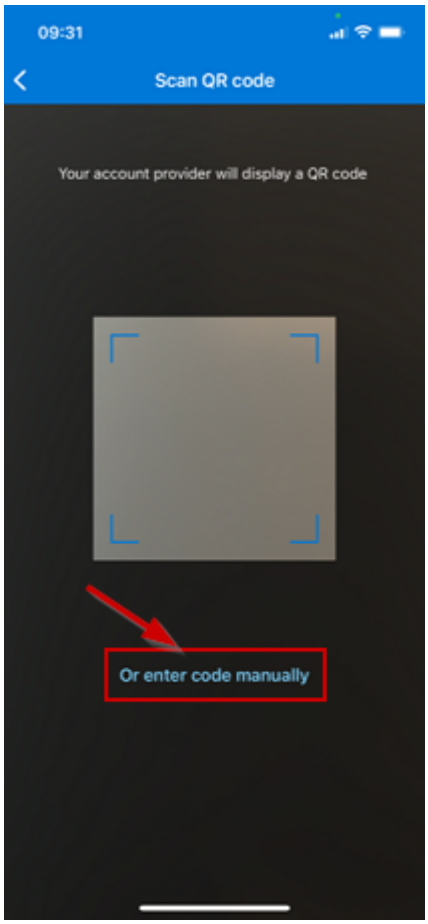
a) Select "Add account" in the "Microsoft Authenticator" app.



b) For the kind of account, select "Other (Google, Facebook, etc.)".

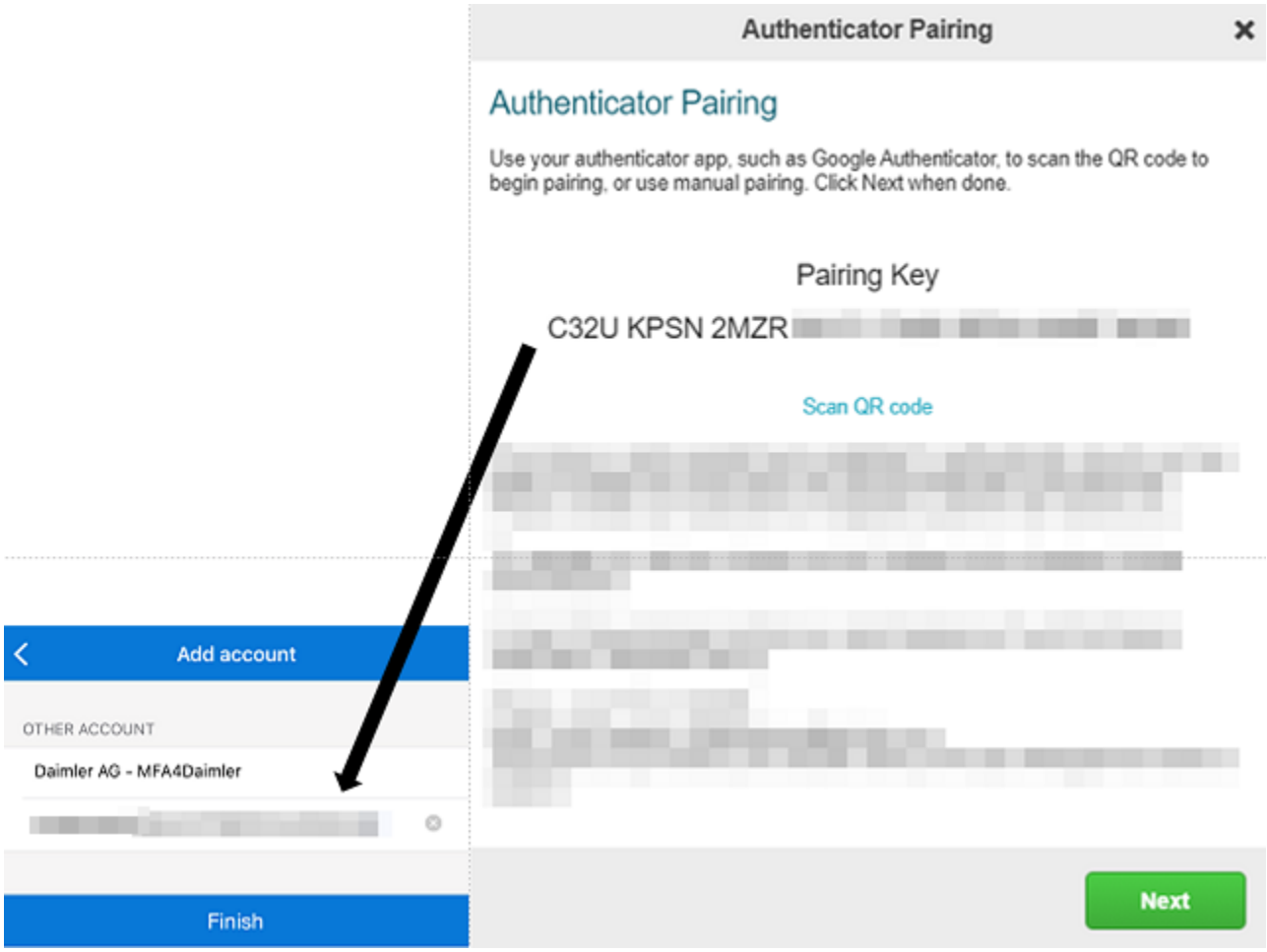


c) The "Microsoft Authenticator" app now expects you to scan a QR code. Select "Or enter code manually" to enter the pairing key manually.

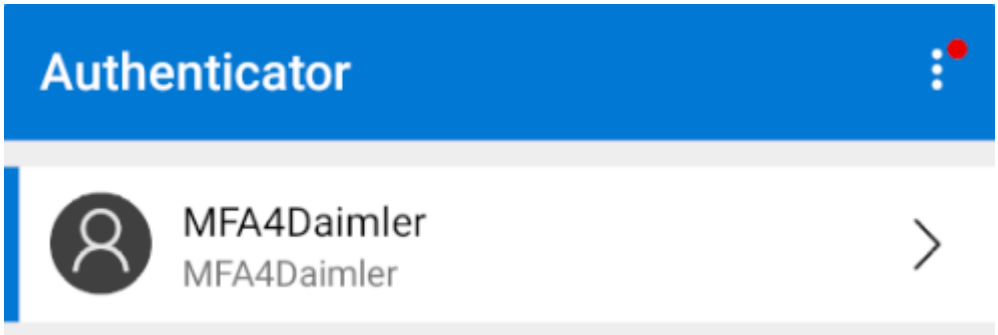


d) Select "Manual pairing" in MFA4Daimler to display the manual pairing key.

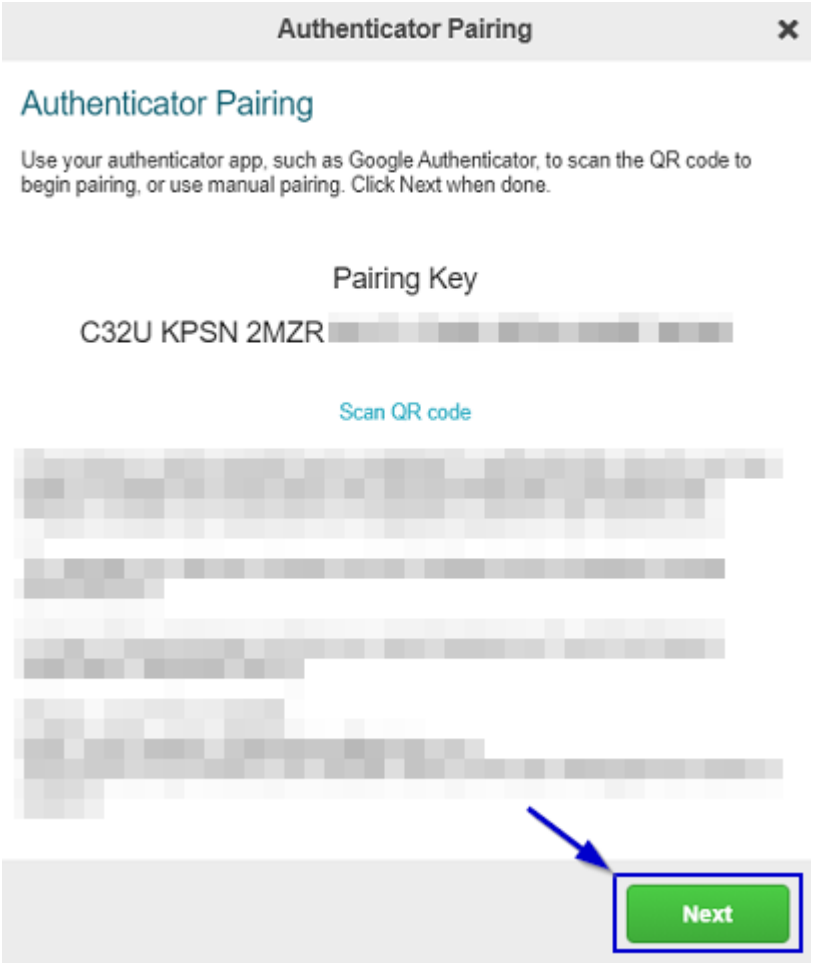
e) Enter an account name in the "Microsoft Authenticator" app (e.g. "MFA4Daimler") and enter the pairing key shown in the browser. Then select "Finish".



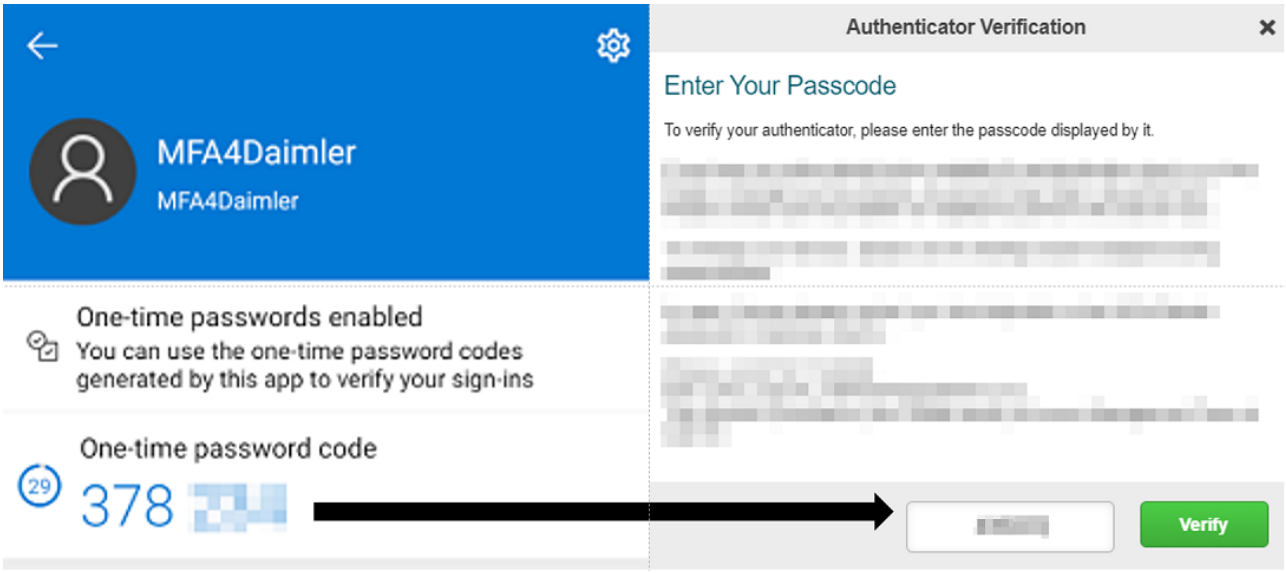
f) A new entry (in this example "Daimler AG - MFA4Daimler") appears in the "Microsoft Authenticator" app.



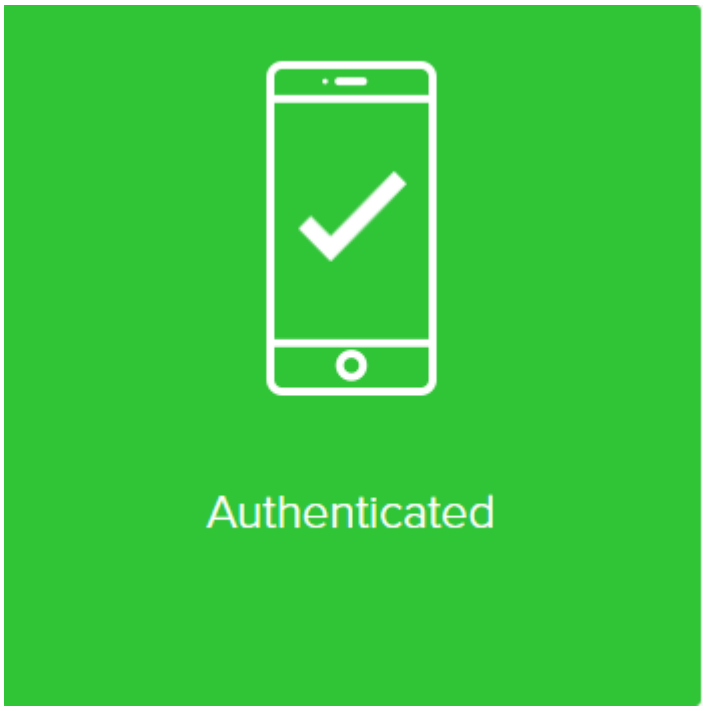
g) Select "Next" in MFA4Daimler.



h) Enter the passcode shown in the "Microsoft Authenticator" app into the entry field of the browser and select "Verify".



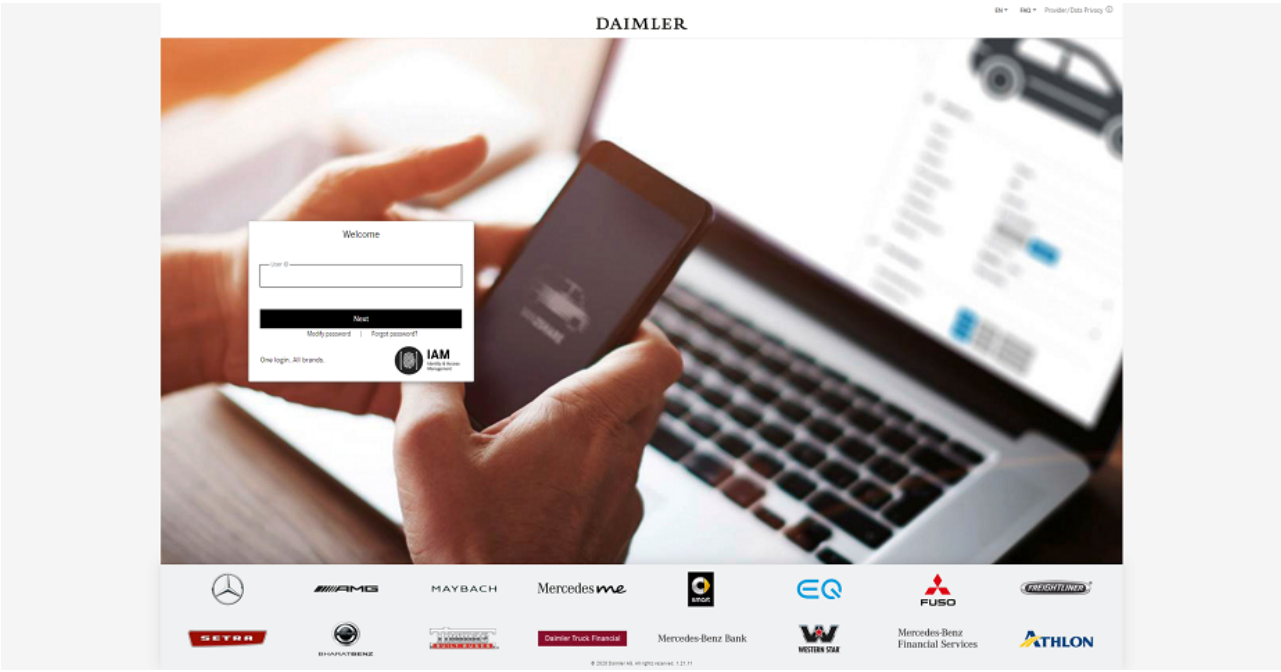
i) Pairing has been successfully completed if the following display appears. In future you can sign-in with MFA4DDaimler using the "Microsoft Authenticator" app.



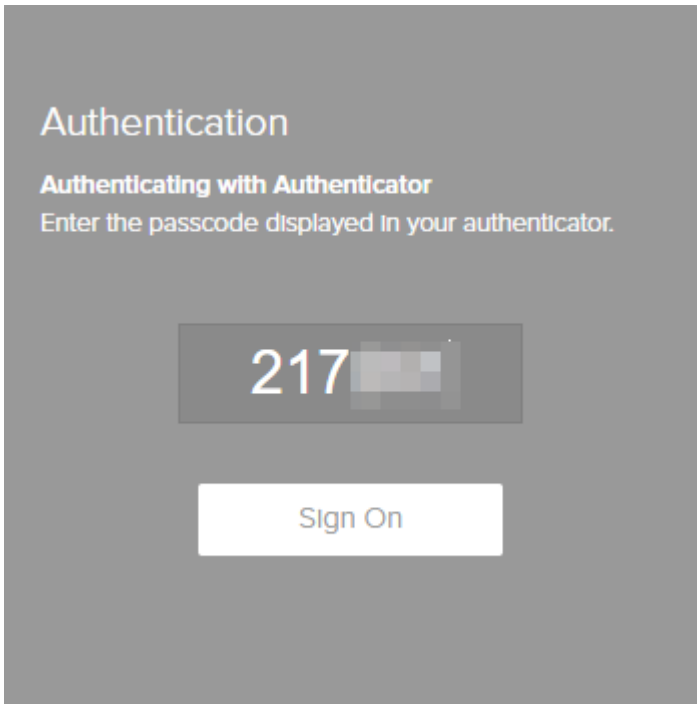
Authentication

Once you have successfully paired the "Microsoft Authenticator" app with your account, you can use it for future authentications with MFA4Daimler.

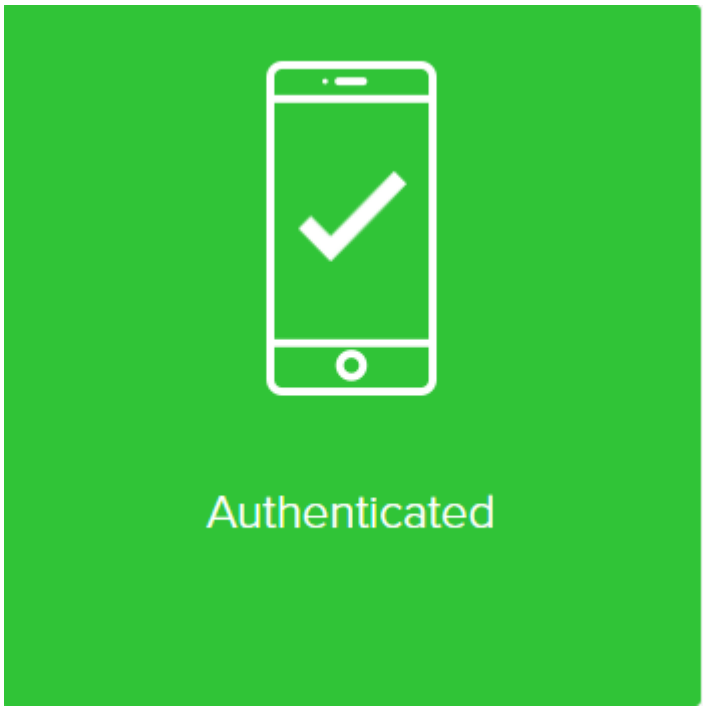
1. Call up an application protected by MFA4Daimler.
2. Log-in to the corporate web with your user ID and password.



3. After logging-in, you are prompted to authenticate yourself using a method paired with MFA4Daimler. Open the "Microsoft Authenticator" app.
4. Enter the passcode shown in the "Microsoft Authenticator" app into the entry field of MFA4Daimler and select "Sign on".



5. You have successfully signed-on if the following display appears. You are then automatically taken to the application.



3.2. Use with a desktop device

This section describes the use of MFA4Daimler with a desktop device, using the "WinAuth" app (version 3.5.1) as an example.

3.2.1. General notes on remote desktop/terminal server solutions

For authentication with MFA4Daimler using a remote desktop/terminal server solution, we recommend the use of an external authenticator app with a mobile device (see Use with a mobile device).

Alternatively an external authenticator app which accesses the remote desktop/terminal server solution can be used on the desktop device.

For security and function-related reasons, the use of an external authenticator app on the virtual remote desktop/terminal server solution itself is **not recommended**.

Note on the use of the authentication method "FIDO2 hardware security key":

- Owing to the many different implementations of remote desktop/terminal server solutions, restrictions can occur when using the "FIDO2 hardware security key" method with remote desktop/terminal server solutions and MFA4Daimler. **Before you use the FIDO2 hardware security key method in combination with a remote desktop/terminal server solution, we urgently recommend that you test and verify correct operation beforehand. If a fault occurs, only limited support is available in this scenario.**

3.2.2. Installation of the WinAuth authenticator app

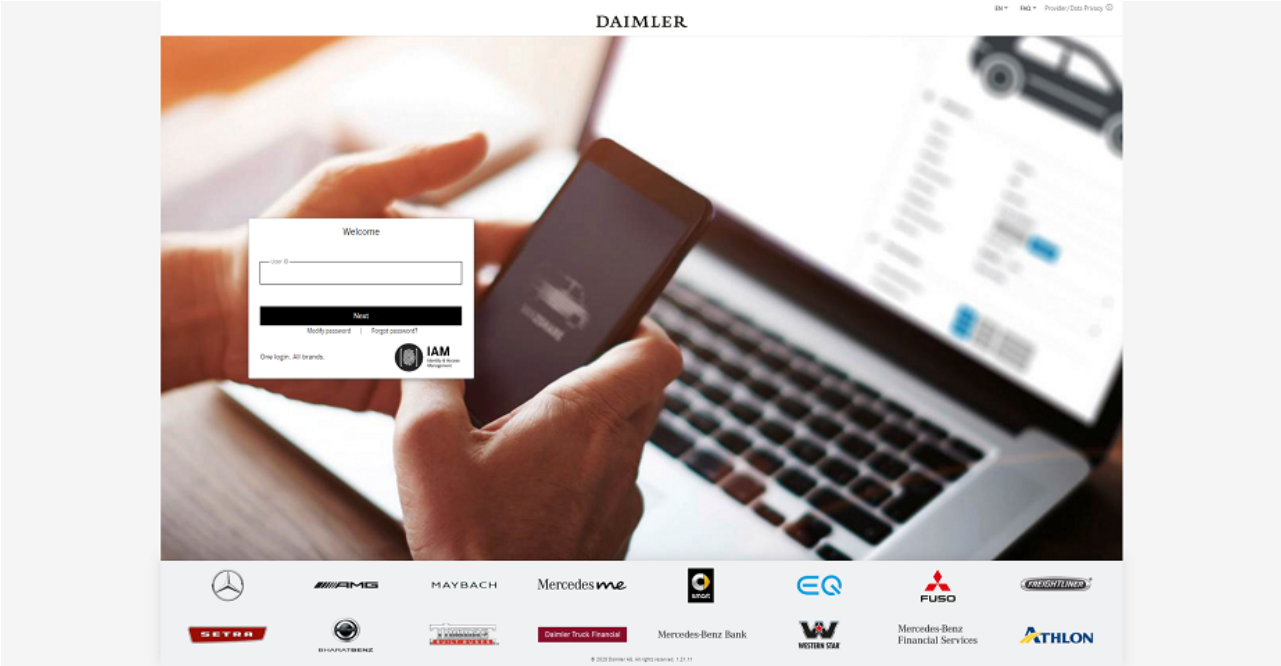
Load the "WinAuth" authenticator app on your desktop device.

No administrator rights are necessary for its use.

3.2.3. Initial pairing

When the "WinAuth" app has been loaded on the device, initial pairing is carried out by calling up an application protected by MFA4Daimler.

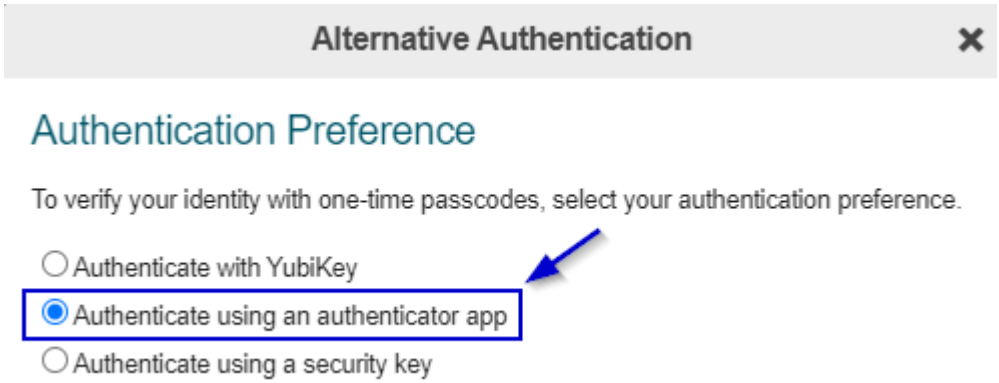
1. Call up an application protected by MFA4Daimler.
2. Log-in to the corporate web with your user ID and password.



3. After logging-in successfully, you are guided through the initial pairing process with MFA4Daimler.

   To pair an authenticator app, select the link "I want to use a different authentication method".

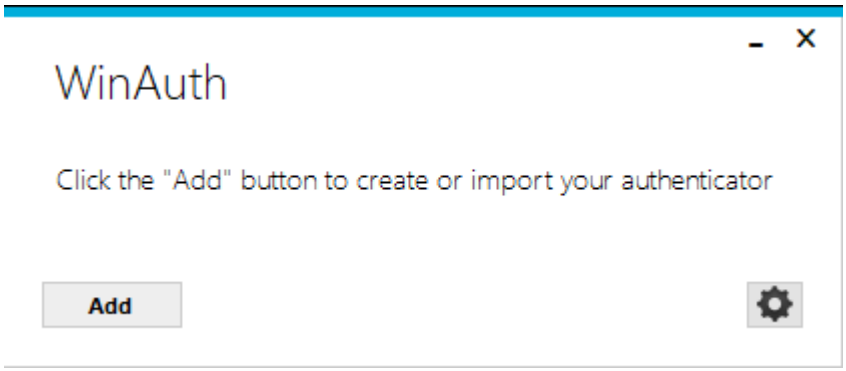
4. Select the option "Authenticate using an authenticator app".



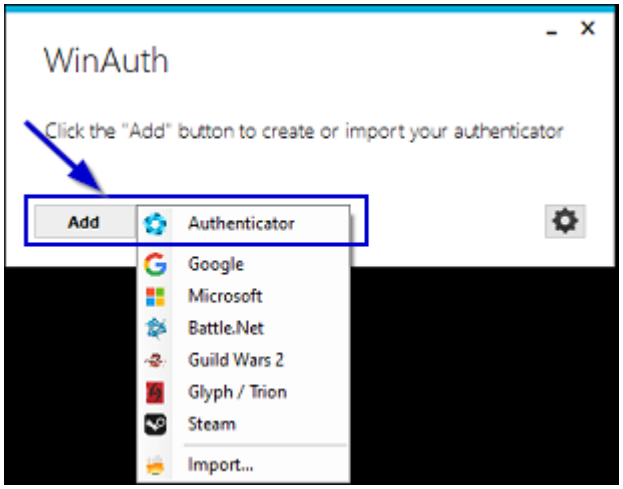
5. Pairing procedure.

   A QR code is displayed to pair your account with an authenticator app. Select "Manual pairing" in MFA4Daimler to display the manual pairing key.

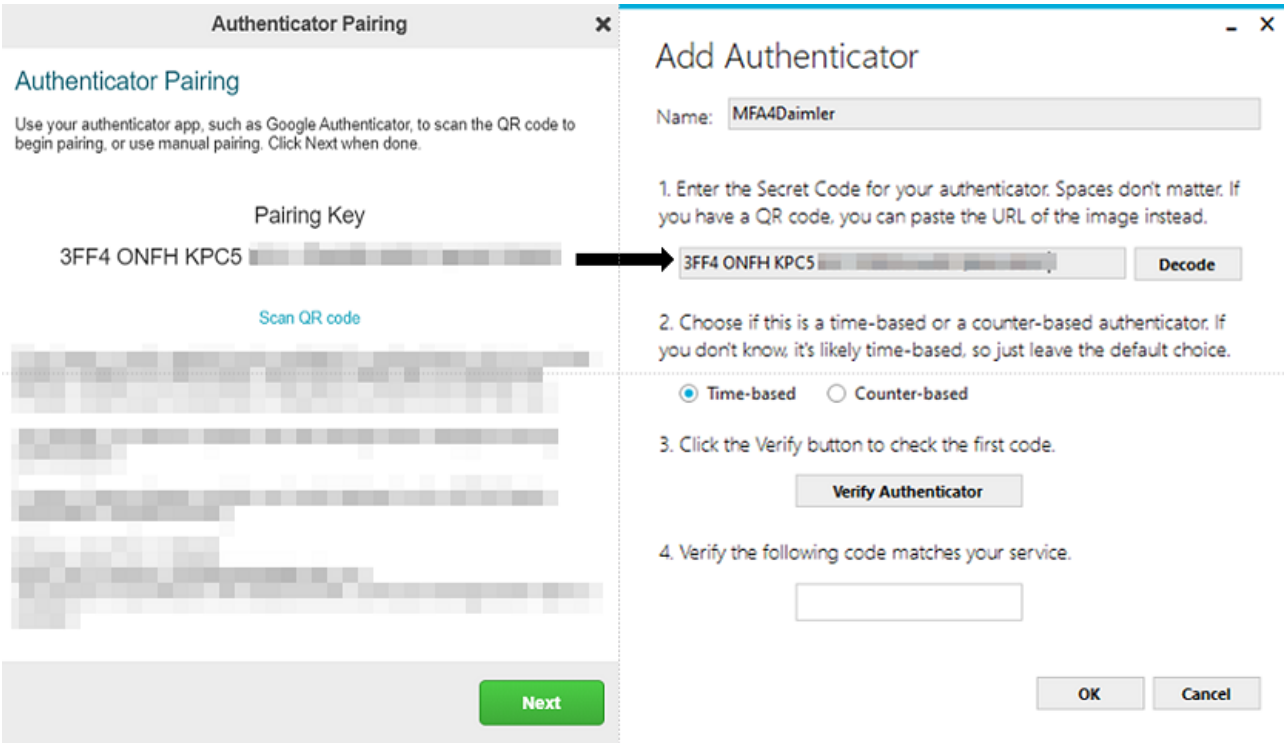
6. Open the "WinAuth" authenticator app. To do this start "WinAuth.exe".



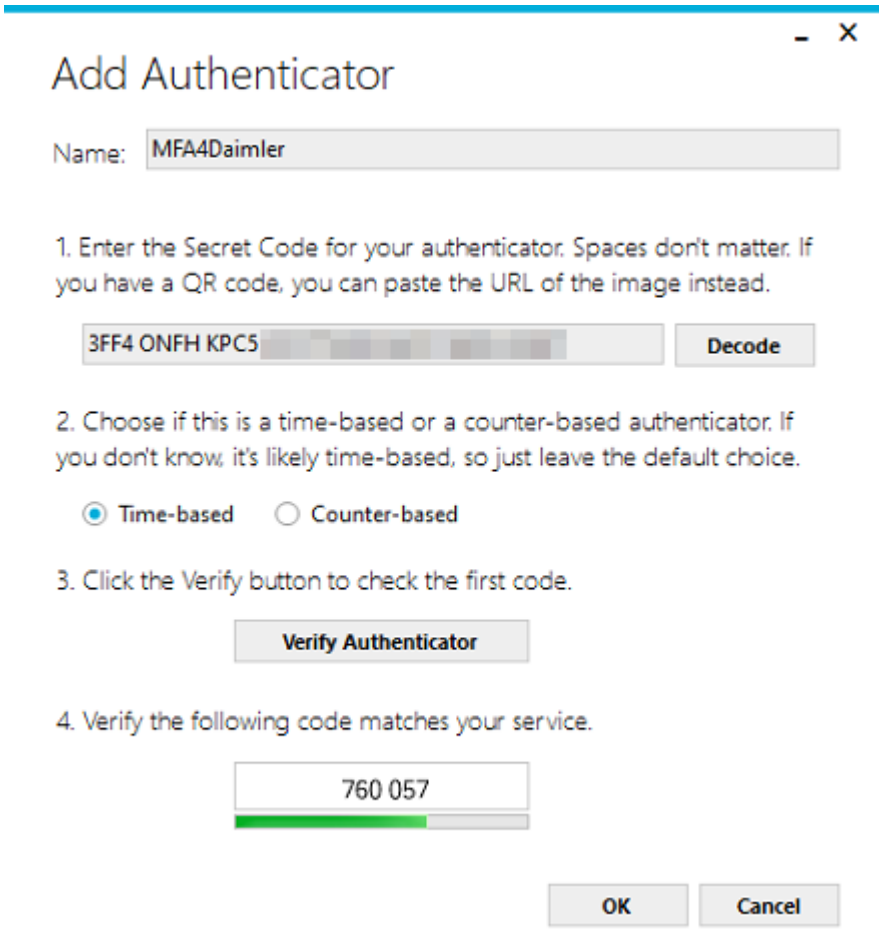
7. To add a new entry, select "Add" and then "Authenticator".



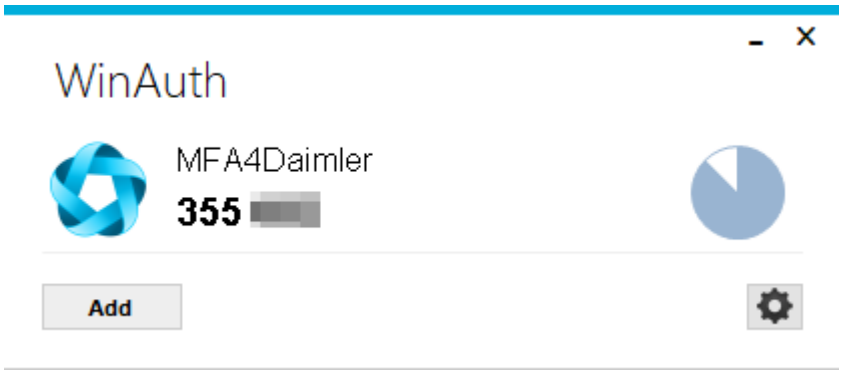
8. Enter an account name in the "WinAuth" authenticator app (e.g. "MFA4Daimler") and enter the pairing key shown in the browser (see step 5.).



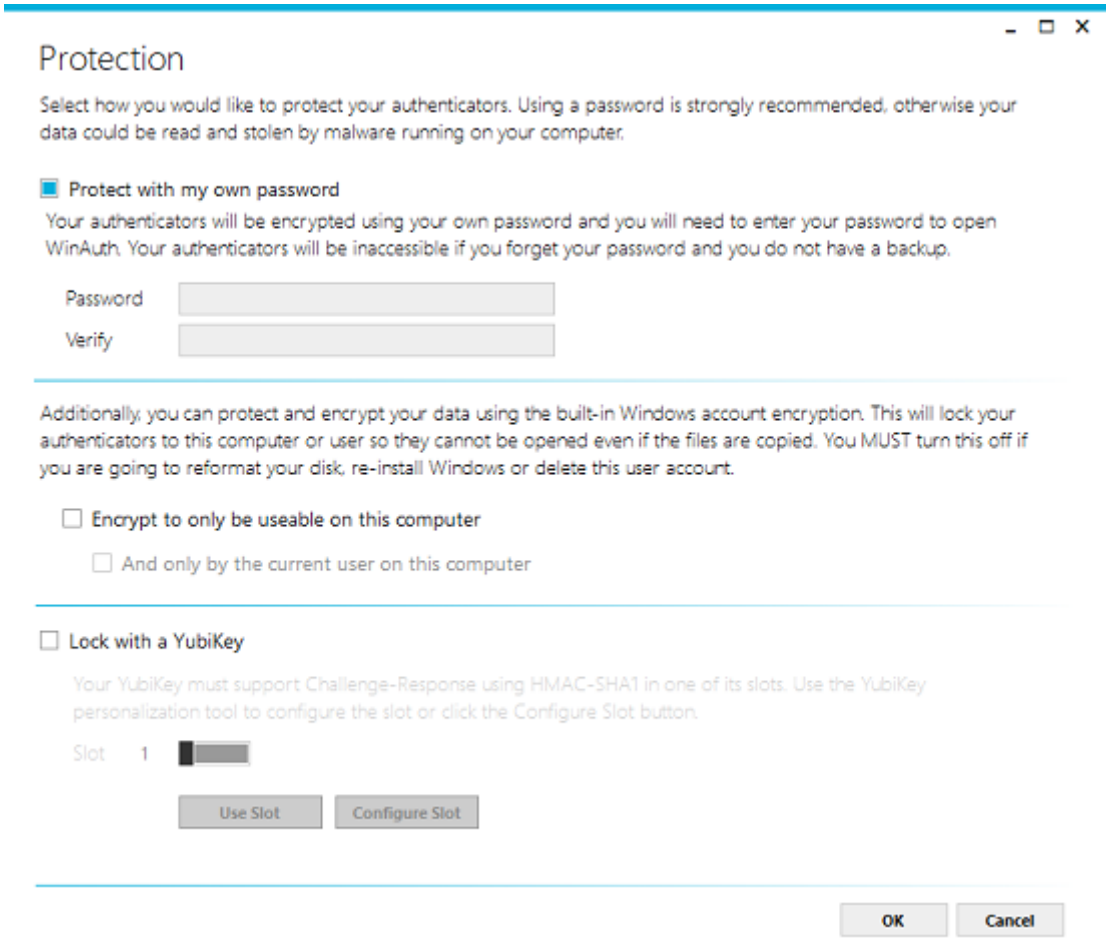
9. Select "OK" in the "WinAuth" authenticator app to generate passcodes.



10. Select "OK" again in the "WinAuth" authenticator app. A new entry is now displayed in the "WinAuth" authenticator app (in this example "MFA4Daimler").

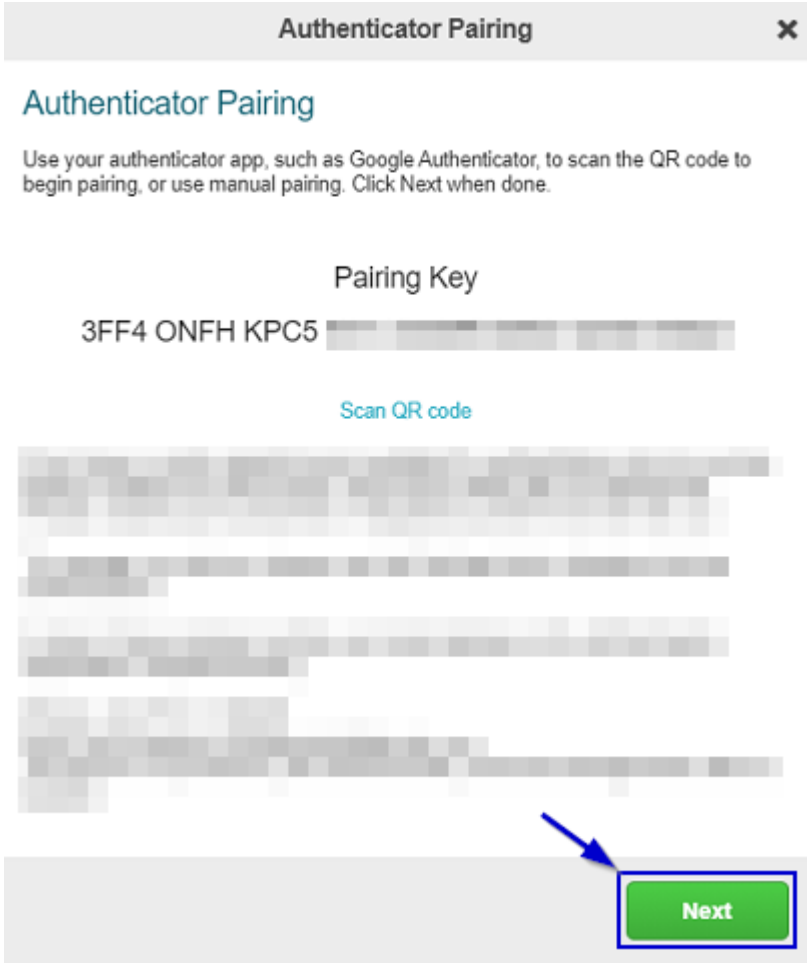


11. You may be prompted to protect access to your "WinAuth" authenticator app. We recommend that you choose one of the available methods to protect access to your "WinAuth" authenticator app. For example by assigning a password ("Protect with my own password"). This password will then be required for future sign-ins with "WinAuth".

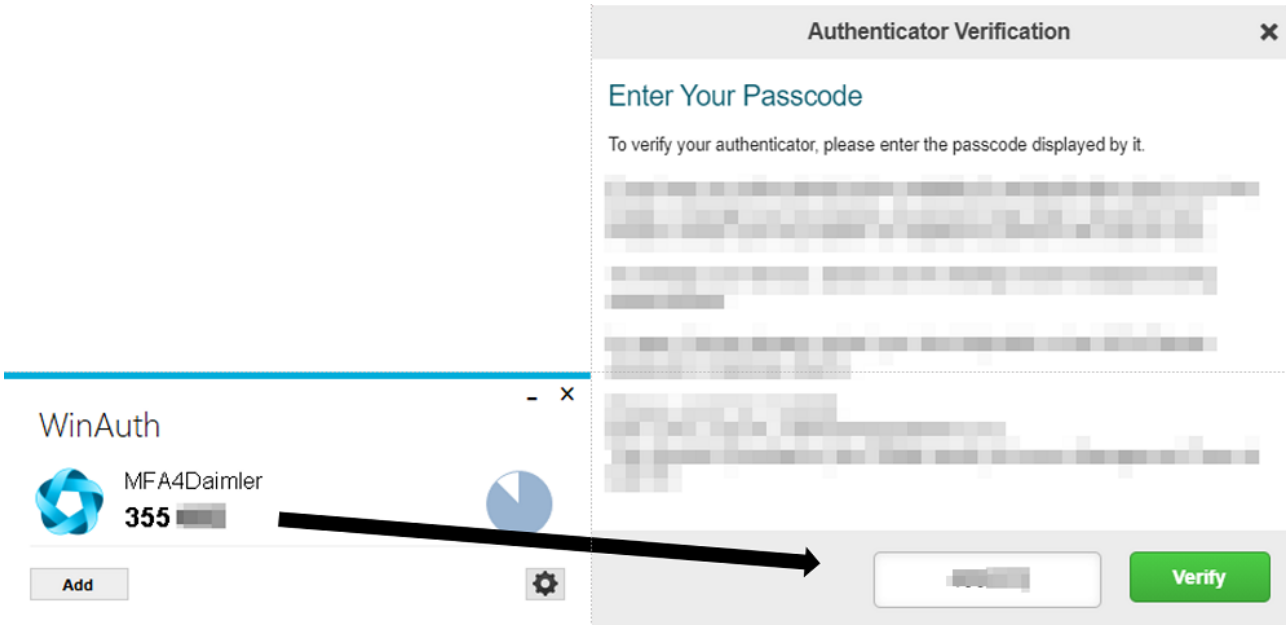


If you prefer not to add protection, select "Cancel".

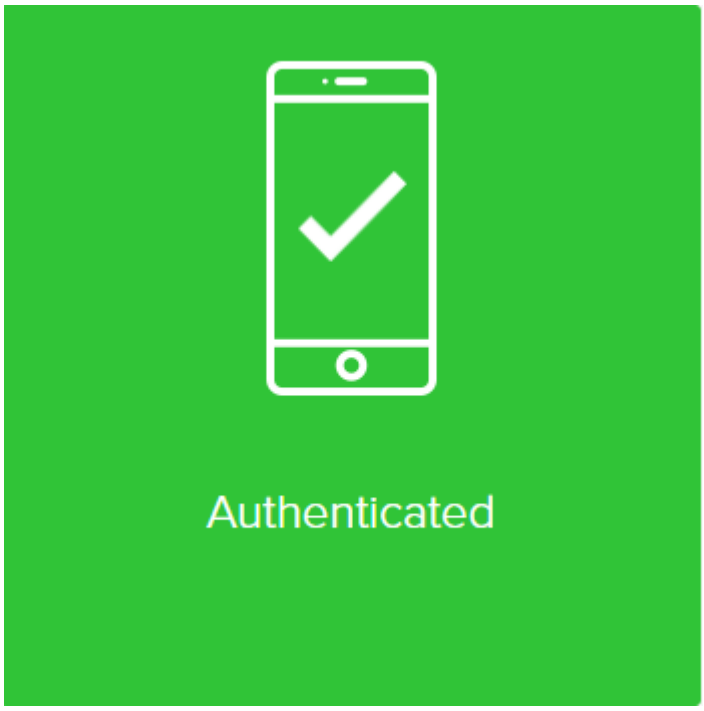
12. Select "Next" in the browser.



13. Enter the passcode shown in the "WinAuth" authenticator app into the entry field of the browser and select "Verify". If no passcode is shown, use the circular arrow button on the right side in "WinAuth" to show a passcode.



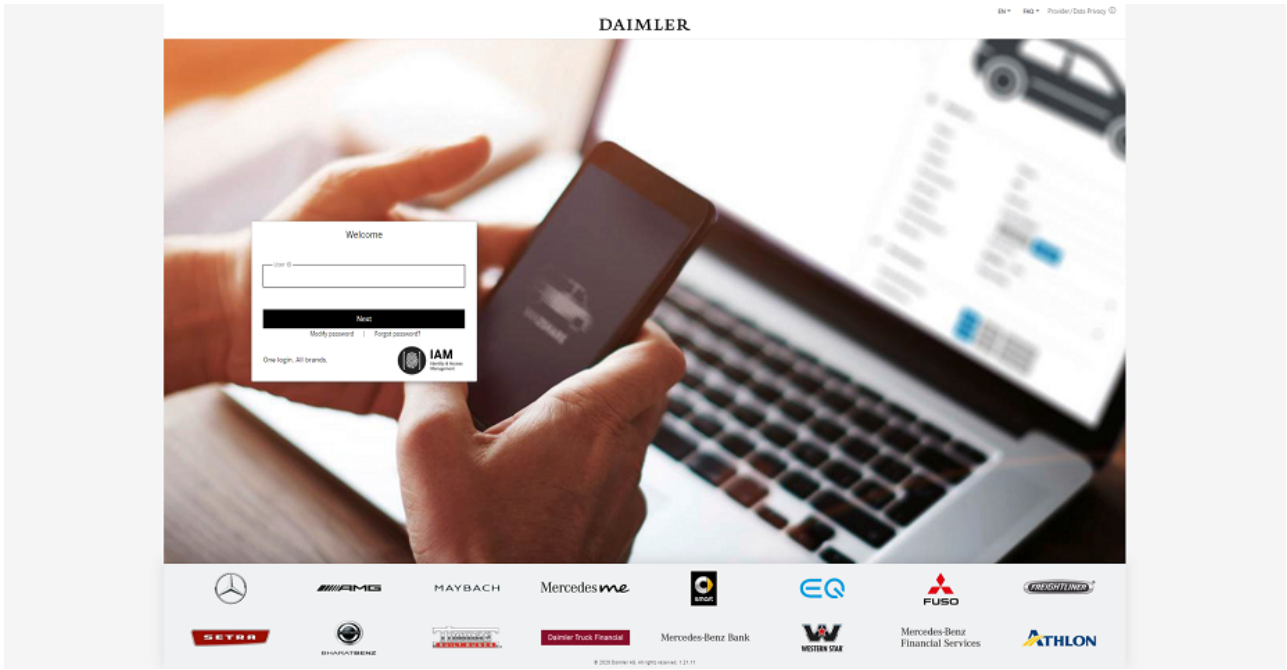
14. You have successfully completed the pairing if the following display appears. In future you can sign-in with MFA4DDaimler using the "Microsoft Authenticator" app.



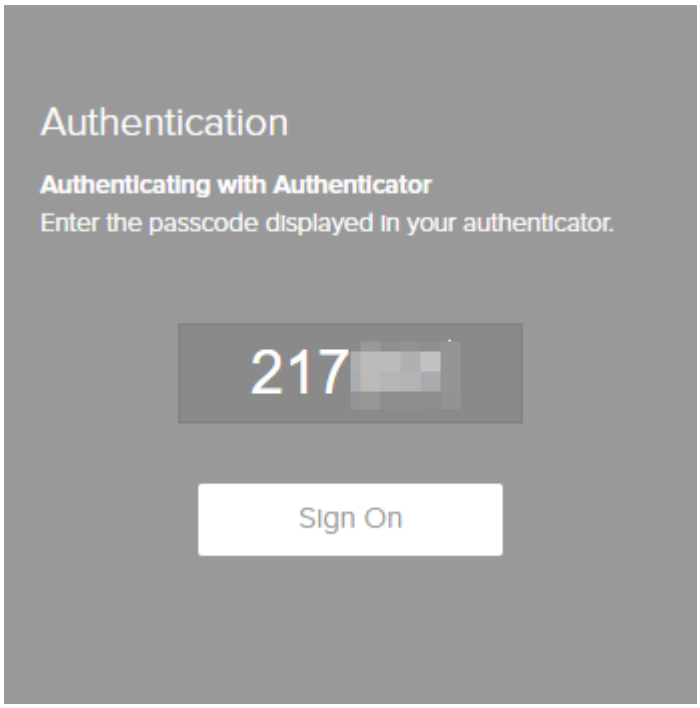
3.2.4. Authentication

Once you have successfully paired the "WinAuth" authenticator app with your account, you can use it for future authentications with MFA4Daimler.

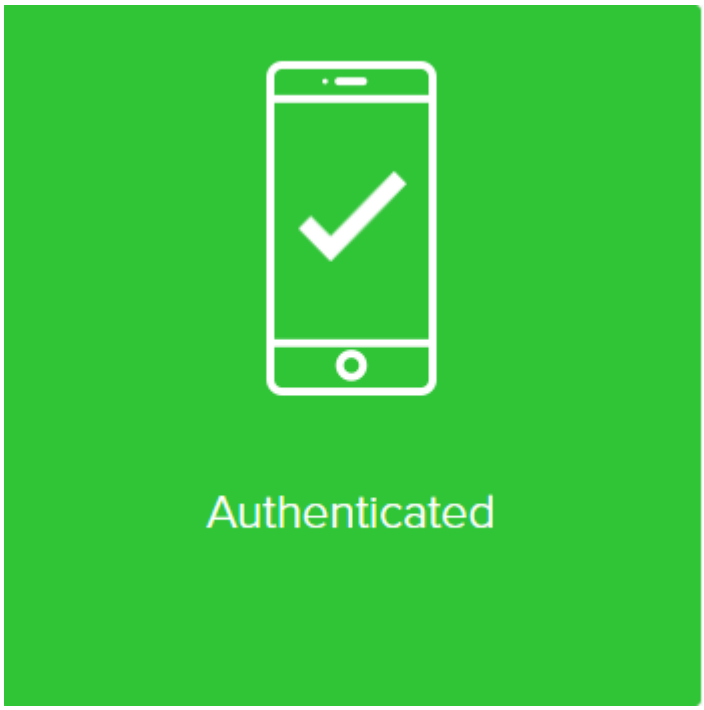
1. Call up an application protected by MFA4Daimler.
2. Log-in to the corporate web with your user ID and password.



3. After signing-in, you are prompted to authenticate yourself using a method paired with MFA4Daimler. Open the "WinAuth" authenticator app.
4. Copy the passcode shown in the "WinAuth" authenticator app into the entry field of MFA4Daimler and select "Sign on". If no passcode is shown, use the circular arrow button on the right side in "WinAuth" to show a passcode.



5. You have successfully signed-on if the following display appears. You are then automatically taken to the application.



4. Account reset and general self-service functions

4.1. Account reset

Your account must be reset if there is no longer any access to devices paired with your account.

To reset your MFA4Daimler account, please contact one of your administrators (OrgAdmin/MarketAdmin) who will reset your account for you in GEMS.

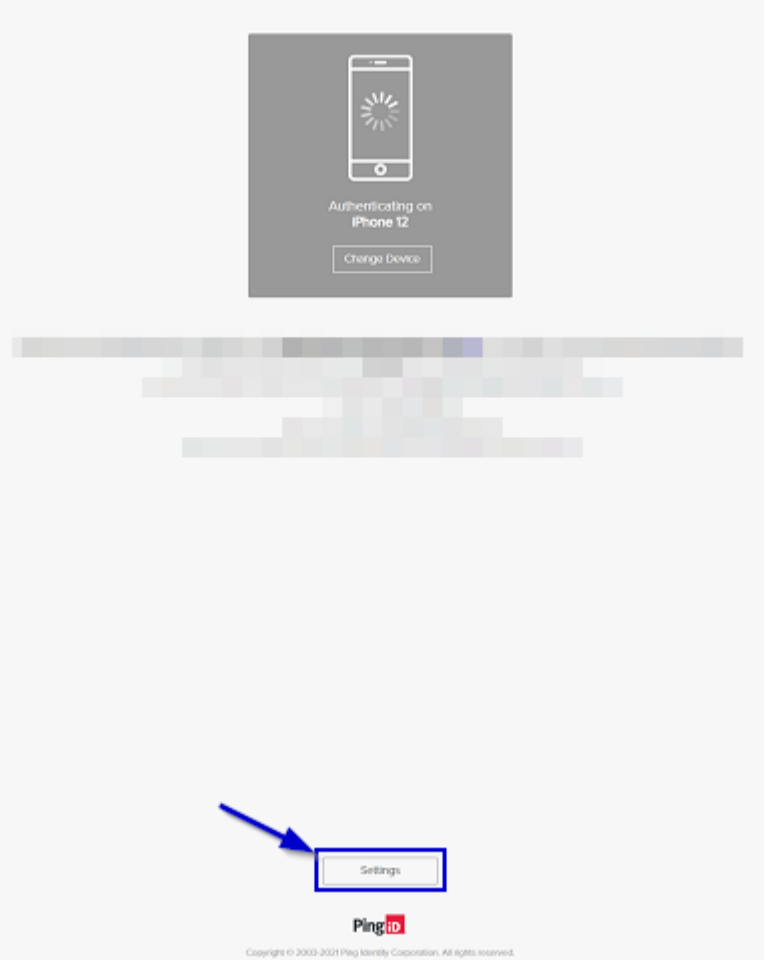
When you next access an application protected by MFA4Daimler, you will then be able to pair a new device.

> Note: Find out whether your account must be reset in the production or integration environment, as the two environments are separate. Be sure to add this information when requesting the reset.

4.2. Managing devices

If you wish to add, change or remove a device in your MFA4Daimler account, visit the Self Service Portal.

You can call up the Self Service Portal by clicking on the "Settings" button during an authentication request with MFA4Daimler.



To make changes in the Self Service Portal, it is necessary to sign-in with MFA4Daimler.

4.2.1. Adding devices

Open the MFA4Daimler Self Service Portal. For information on this see "4.2".

1. You can see your currently paired devices under "My devices". You can pair up to four different devices with your account at the same time. Select "Add" to start the registration process for a new device.
2. The "Add new device" dialogue appears. Follow the steps indicated to pair your new device.
3. Your added device is then shown under "My devices".

4.2.2. Changing your primary authentication device

If you have paired more than one device for authentication, you can choose a primary device as your standard sign-in device.

Use the slider in the MFA4Daimler Self Service Portal to select your primary authentication device.

4.2.3. Removing a device

If you wish to remove a device from your account, use the
MFA4Daimler Self Service Portal. For information on this see "4.2".

To make changes in the Self Service Portal, it is necessary to sign-in with MFA4Daimler.

> **Warning**
>
> If you have only one paired device and you remove it, you can carry out no more authentications until you pair a device again.

1. Select the device you wish to remove in the Self Service Portal.
   Extend the menu of the device to be removed using the button on the right side.
2. Select the waste bin button and confirm that you wish to remove the device from your MFA4Daimler account.
3. Once the device has been removed, your remaining devices are displayed under "My devices".

5. Support

If you have any questions about MFA4Daimler or problems with installation, please contact the Application Helpdesk of MFA4Daimler (currently available in English and German).

In the event of product-specific questions about individual external authenticator apps, please refer to the relevant product-specific manufacturer documentation.

Contact details of MFA4Daimler Application Helpdesk (AHD):

MFA4Daimler AHD	
Phone	+49 (711) 17-25005
Mail	cuhd_support_mfa4daimler@daimler.com

6. FAQs

6.1. How do I use MFA4Daimler on a computer that is also used by several other people?

We urgently recommend using the "Logout" function in the application before the device is used by another person.

For each user and browser, an MFA4Daimler session currently lasts for 8 hours before a new, strong authentication is necessary.

6.2. How often must I authenticate myself with MFA4Daimler?

For each user and browser, an MFA4Daimler session currently lasts for 8 hours before a new, strong authentication is necessary.
This also applies if you sign-in to another application protected by MFA4Daimler in the same browser session.

If you work in another browser session (e.g. Application A in Chrome, Application B in Firefox), or sign-in with another device, a new MFA authentication may be necessary.

6.3. For which applications is MFA4Daimler relevant?

The requirement for strong authentication, e.g. with MFA4Daimler, covers all applications classified as "confidential" or "critical to integrity".

6.4. Can MFA4Daimler be used with a private device?

MFA4Daimler can also be used with e.g. a private smartphone. Please agree the use of a private device with your employer beforehand.

6.5. What should be noted when using MFA4Daimler with Windows group accounts/pool accounts?

If you are signing-in with MFA4Daimler on a desktop client used by several people with a Windows group account, we recommend the use of a mobile authenticator app on a personalised device such as a smartphone when signing-in to applications protected by MFA4Daimler.

> Note: For security reasons, we do not recommend the use of an authenticator app on a client used by several users.