

Using MFA4Daimler with an Authenticator App

Before you begin

To use an authenticator app with MFA4Daimler, the authenticator app first has to be paired with the user account. Pairing a device creates a trust between device and user account.

Setting up an authenticator app to authenticate with MFA4Daimler involves the following steps:

1. Download and installation of the authenticator app of choice on the user device (e.g. smartphone/desktop client).
2. Pairing of the device.

After successful setup, the authenticator app can be used for strong authentication.

Any external authenticator app that can generate a standard one-time password (see [RFC 6238 – TOTP](#)) can be used.

Examples:

- [Google Authenticator](#)
- [Microsoft Authenticator](#)
- [FreeOTP](#)
- [Authy](#)
- [Aegis](#)
- [WinAuth](#)
- [Keepass Plugin](#)

Hint: Download and installation of the preferred authenticator app has to be performed individually.

Please keep in mind that in case of issues we cannot fully support every external authenticator available, we encourage you to use the corresponding help pages of your authenticator.

The PingID Smartphone app and the use of hardware security keys is still fully supported.

General advice:


- We recommend to separate first and second factor (e.g. entering UserID/PW on your laptop and using a mobile authenticator on your smartphone for MFA) wherever possible to ensure the highest level of security.
- We recommend to pair more than one device with MFA4Daimler to ensure that a fallback device is always available for authentication.

Using MFA4Daimler with an Authenticator App


1) Initial Pairing

1 Start a MFA4Daimler protected application & Login with UID/Password


Start application or website.
Login at the Corporate Weblogin.



Afterwards select "Next" to finish the pairing process.

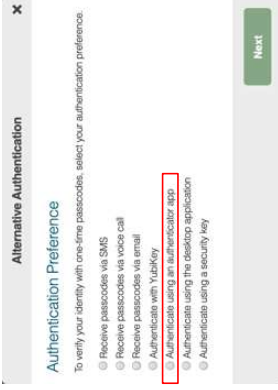


Afterwards select "Next" to finish the pairing process.



2 Select Authenticator App as Authentication Method


On the following page, select "Authenticate using an Authenticator App".




Available options may vary

3 Scan the QR Code

Scan the displayed QR code with your authenticator app of choice or enter it manually. You can use any external authenticator app that can generate a standard (TOTP) one-time password.


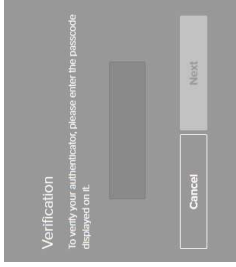


Afterwards select "Next" to finish the pairing process.



4 Authenticate with your Authenticator App

Enter the the displayed one time passcode (OTP) generated by your authenticator app into the input field to authenticate with MFA4Daimler (in this example Google Authenticator) and click "Next".





Using MFA4Daimler with an Authenticator App

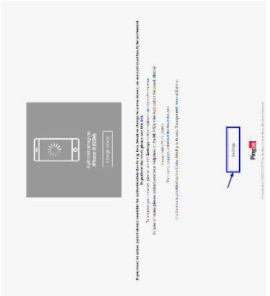
2) As additional device

1 Open your Device Management Page

Start application or website.
Login at the Corporate Weblogin.

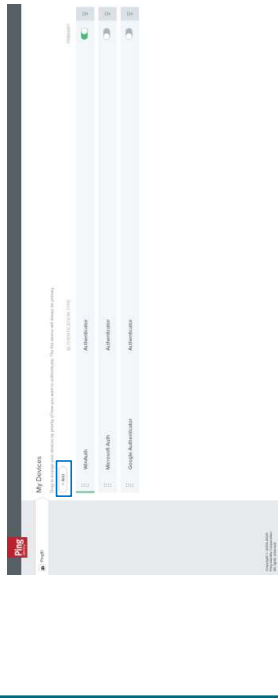


Select the "Settings" button displayed during authentication.



2 Add Authenticator App as New Device


On the following page, select "Add Device" and afterwards the option "Authenticate using an Authenticator App" to start the pairing process.



3 Scan the QR Code

Scan the displayed QR code with your authenticator app of choice or enter it manually. You can use any external authenticator app that can generate a standard (TOTP) one-time password.

Afterwards select "Next" to finish the pairing process.



4 Authenticate with your Authenticator App

Enter the the displayed one time passcode (OTP) generated by your authentication app into the input field to authenticate with MFA4Daimler (in this example Google Authenticator) and click "Next".

