New authentication in XENTRY Diagnosis

09/2022

Before **commissioning, programming or coding control units of any type (XENTRY Flash)**, you must authenticate yourself in XENTRY Diagnosis with a second factor.

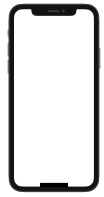
Multi-Factor-Authentication

What you will need in the future

- **As usual**
  Your user name and password.
- **Plus:**
  - An authentication app on your smartphone or
  - A USB security key

Smartphone app

- Please install an authentication app on your smartphone.
- Please note: The app must comply with the **RFC6238 TOTP Standard**.



Or:

USB security key

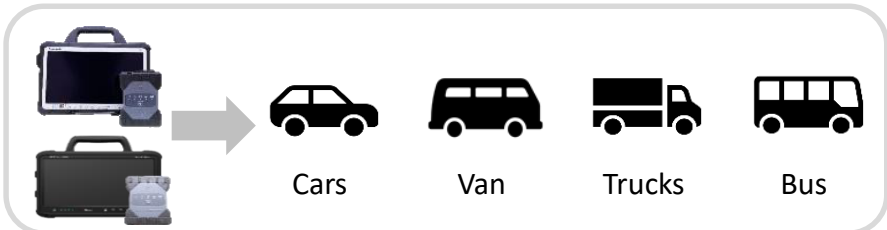
- Please obtain enough USB security keys.
- You can obtain these from electrical retailers or directly from the manufacturer.
- Note that the USB security key must comply with the **FIDO2 Standard**.

Authentication in XENTRY Diagnosis

- Each time you perform an XENTRY Flash operation, you will be automatically guided through the authentication process.
- The corresponding window opens automatically in XENTRY Diagnosis.

CARS TRUCK

Multi-factor authentication is mandatory for all XENTRY Diagnosis users worldwide.



Issue date: April 2022 – Subject to change

How authentication works in XENTRY Diagnosis

Multi-factor authentication is required during commissioning, programming and coding of all control units.

Preparation

We recommend that you set up your second factor in advance using the following URL: https://login.mercedes-benz.com/password/mfa-settings

Initial login

1. Use XENTRY Diagnosis as usual. As soon as it is necessary, XENTRY Diagnosis will inform you that you need to perform authentication.
2. If you have not yet stored your second factor, set it up now for authentication.

Click here if you want to use a **USB security key**

Click here if you want to use an **authentication app** on your smartphone

3. Once you have completed the process, the system confirms your authentication. You can now continue working in XENTRY Diagnosis as usual.

As of your second login

1. Use XENTRY Diagnosis as usual. As soon as it is necessary, XENTRY Diagnosis will inform you that you need to perform authentication.
2. Now use your second factor for authentication.

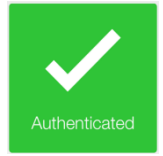
2.1 App on smartphone

If you have stored an authentication app as your second factor, then a corresponding push notification automatically appears on your smartphone.

2.2 USB security key

If you have stored a USB security key as your second factor, now insert it into a free USB port in your XENTRY Diagnosis Pad | Pad 2.

3. You are now authenticated and can continue working in XENTRY Diagnosis as usual.



Issue date: April 2022 – Subject to change

MFA4Daimler – Quick Guide for Hardware Security Keys

Before you begin

- Make sure your browser supports this method of authentication.
- Make sure you are using a security key which is suitable for your device (e.g. USB-A, USB-C, NFC, BLE).

When using security keys with MFA4Daimler, the following requirements and limitations apply:

- MFA4Daimler supports FIDO2 and U2F security keys.
  - **Note:** U2F security keys can only generate a single credential per domain. A device can only be paired by one user per domain.
- Security keys can be used for web-based authentication through WebAuthn supporting browsers only

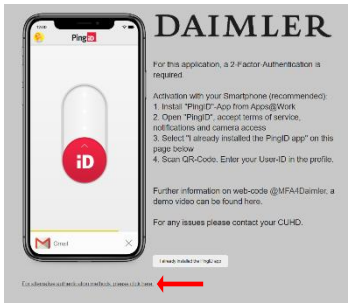
- Registration and authentication must be performed with a WebAuthn supported browser, such as the latest versions of Google Chrome or Microsoft Edge.

Register your security key with MFA4Daimler

1 Start an application protected with MFA4Daimler

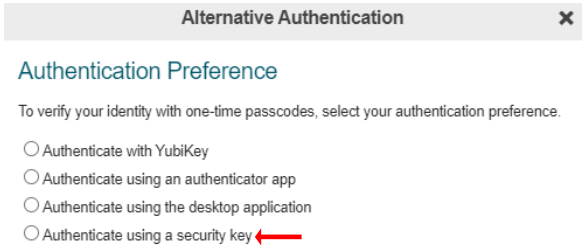
Log on using your corporate UserID and password.

On the registration page, select the link **„For alternative authentication methods, click here“**.



2 Select your authentication method

Select „security key“ and click **Next**.



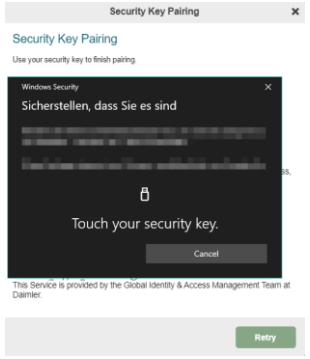
3 Perform authentication

You are prompted to authenticate with your security key.

Insert the security key into your computer USB port and then tap the contact.

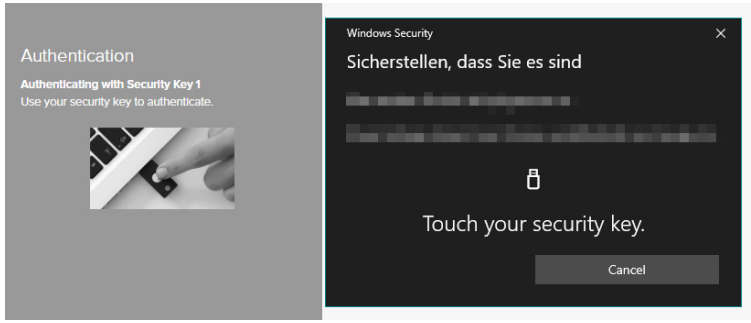
This triggers authentication with your security key. A green check mark appears, indicating the pairing request is successful.

You might be asked to setup a user verification for your security key during this step (e.g. a PIN code). If so, this PIN will be requested with every authentication attempt to unlock your key.



4 Use your security key for authentication

Whenever you are required to authenticate with MFA4Daimler, insert your security key into your computer USB port and then tap the contact to authenticate.



MFA4Daimler – Quick Guide for Yubikey

Before you begin

- Make sure your browser supports this method of authentication.
- Make sure you are using a Yubikey which is suitable for your device (e.g. USB-A, USB-C, NFC, BLE).

YubiKeys can be paired for either:

- Yubico OTP authentication
- Security Key FIDO2 authentication

If you have a YubiKey that supports FIDO2 or U2F, pair the device as a “security key”.

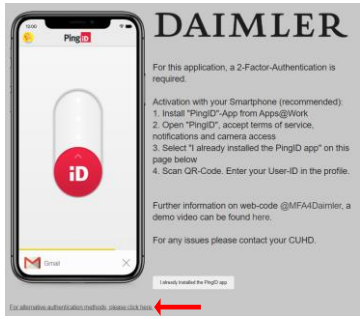
If you have a Yubikey that only supports Yubico OTP, pair the device as “Yubikey”.

Register your Yubikey with MFA4Daimler

1 Start an application protected with MFA4Daimler

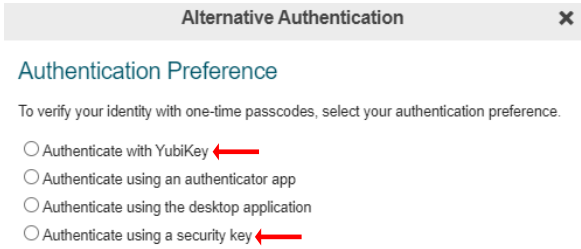
Log on using your corporate UserID and password.

On the registration page, select the link „**For alternative authentication methods, click here**“.



2 Select your authentication method

Select „security key“ if your Yubikey supports FIDO2 or U2F, otherwise select „Yubikey“ and click **Next**.



3 Perform authentication

You are prompted to authenticate with your Yubikey.

Insert the YubiKey into your computer USB port and then tap the contact.

After a verification code has been generated into the input field, “Verify” is selected automatically.
A confirmation appears, indicating the pairing request is successful.

You might be asked to setup a user verification for your Yubikey during this step (e.g. a PIN code). If so, this PIN will be requested with every authentication attempt to unlock your Yubikey.

4 Use your Yubikey for authentication

Whenever you are required to authenticate with MFA4Daimler, insert your YubiKey into your computer USB port and then tap the contact to authenticate.