QUICK GUIDE
HowTo configure your new Multi Factor Authentication

Please note: This instruction has **two columns** – some steps have to be done on your **Smartphone** (left column) and some steps on your **PC/Notebook** (right column).

Smartphone

1 Please install the App „NetIQ Advanced Authentication“

Instructions for Wacker iPhone, Samsung or Samsung in China

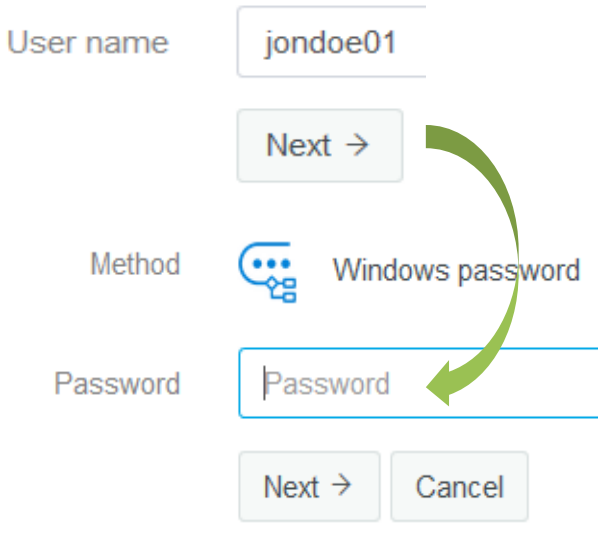
non Wacker Smartphones
Please use the App or Playstore on your device.

2 Open the app, agree to the licence agreement and configure a at least 4 digit PIN. Later, you can secure the app by fingerprint as well.

Please allow the app to use camera and location ressources of your phone.

PC/Notebook

3 Open this URL in your Browser:
https://mfauth.idm.wacker.com
and login with your Wacker Useraccount and Password (without a repository prefix)

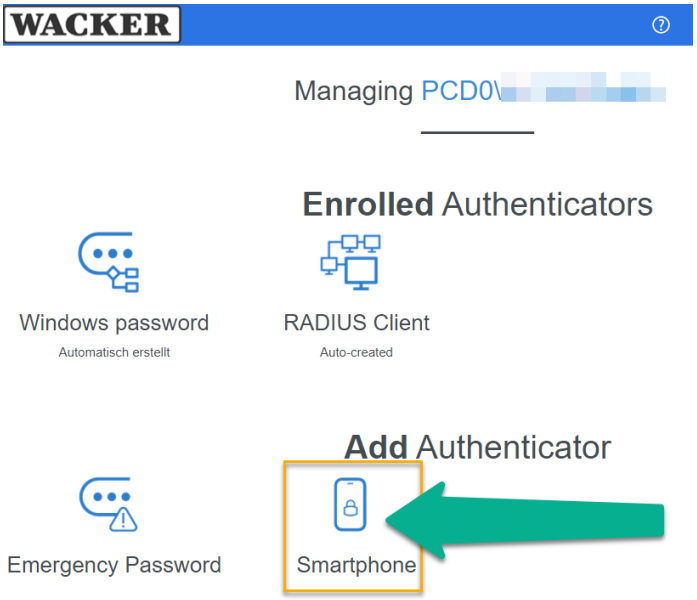


Smartphone

PC/Notebook

4

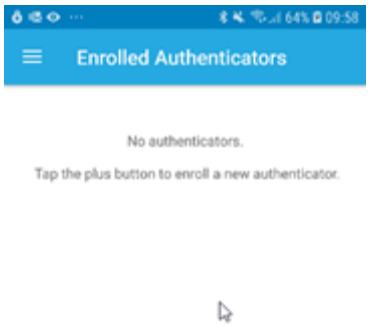
Klick on „Smartphone“



and on „Save“ on the next dialog to start the configuration.

5

Press the „+“ Button in the app



If prompted, please allow the app the usage of the camera

6

… to take a picture of the displayed QR-Code with your App

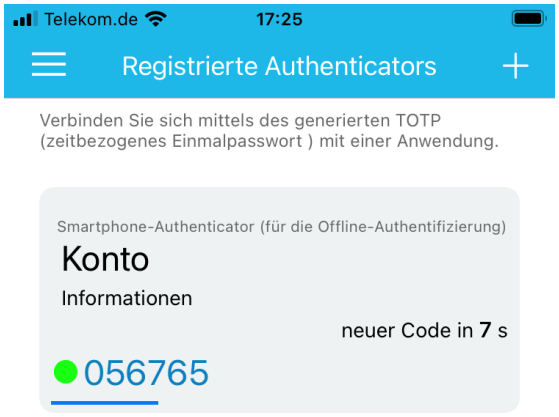
Am Smartphone

Tip: You can define additional information about the authenticator in your app. This is optional

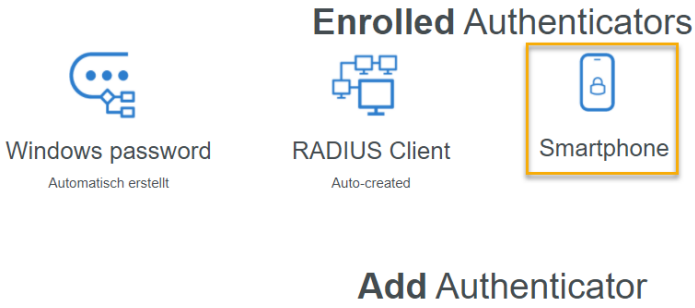
Am PC/Notebook

7

You have successfully finishied the configuration of your app. It should now look like this:



The webpage in your browser will change accordingly



→ you can now close the browser window

The App creates a new 6-digit One Time Password (OTP) every 30 Seconds which is used for authentication with Citrix Access Gateway or VPN.

Important for Entrust Migration Users:
Your old PIN is no longer needed. If asked for the passcode, just use the 6-digit OTP

Depending on the dial in platform, the authentication process might slightly change:

- **Citrix Access Gateway**: Usage as usual, just use the One Time Password from your new app when prompted
- **Global Protect**: Usage as usual, just use the One Time Password from your new app when prompted
- **Palo Alto Authentication Portal**: You need your real password to log in. The usage of a "dummy" password is obsolete.
- **Citrix Receiver**: You will have to enter your password twice. First in the field "Password", second in the field "Token". When prompted for "next Token" please enter the One Time Password from your new app

Your Entrust Token or Entrust App is no longer needed. Remove the old App from your phone. For Token Disposal, please follow the Disposal Instructions from Entrust:
https://web.entrust.com/tokendisposal/