Zweifaktor-Authentifizierung mit TOTP (Time Based One-Time Password)

Zweifaktor-Authentifizierung mit TOTP

Eine Zweifaktor-Authentifzierung wird benutzt, um die Anmeldung in Projectile sicherer zu gestalten.

Normalerweise meldet man sich auf einer Website (mit Anmeldename und Passwort) an. Das passiert über eine Netzwerkverbindung und dies ist der 1. Faktor. Da diese Netzwerkbindung abgehört werden können, ist es mittlerweile üblich, einen 2. Faktor zur Sicherheit zu benutzen, der über ein anderes Gerät, eine andere Verbindung läuft. In Regel benutzt man dazu ein Mobiltelefon oder ein spezielles Gerät.

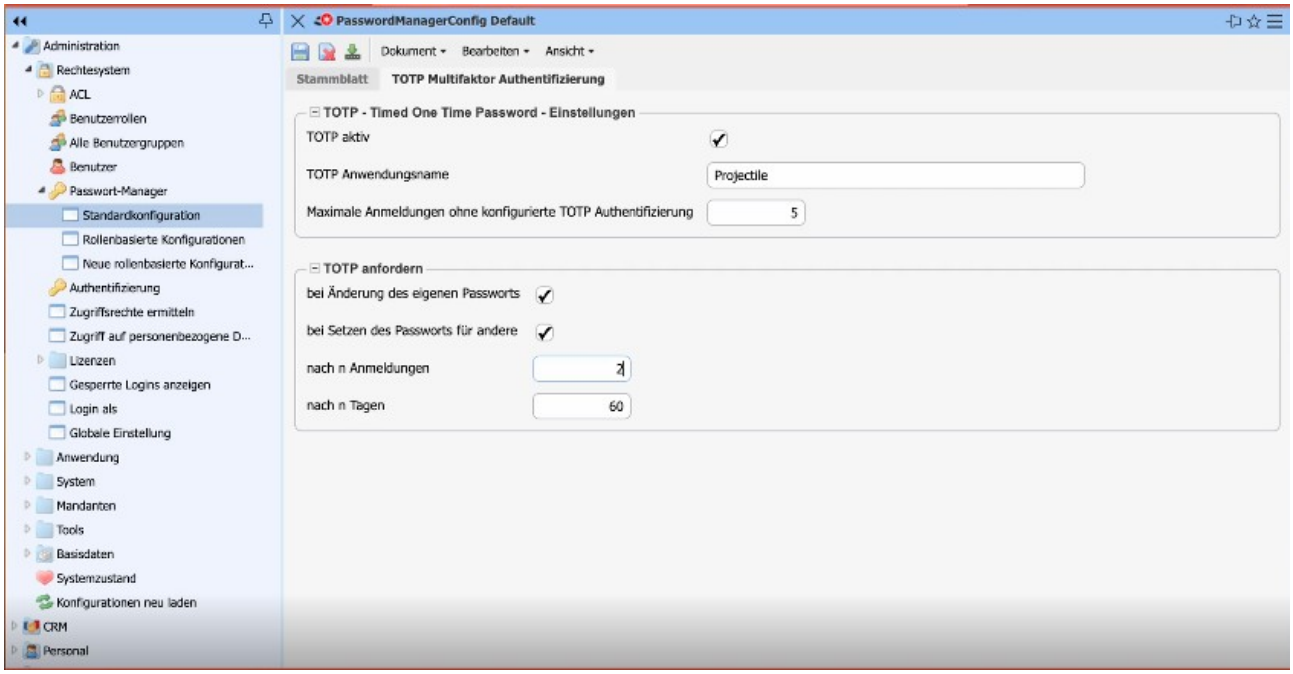
Im Fall von Projectile ist eine App auf dem Mobiltelefon, die sich *Authenticator* nennt.

Ein One-Time Passwort ein Passwort, das nur einmal gültig ist. *Time-based* bedeutet, dass es aufgrund der aktuellen Uhrzeit berechnet wird.

Zusätzlich muss man das Mobiltelefon vorher registrieren. Durch einen QR-Code wird der Nutzer in der App eingetragen und mit Projectile verbunden und so kann der 2. Faktor eine zusätzliche Sicherheit geben, dass nur erlaubte Personen Projectile verwenden.

Aktivieren & Konfigurieren des TOTP-Moduls

Ein Nutzer mit der entsprechenden Berechtigung kann im Passwortmanager auf dem neuen Reiter „TOTP Multifaktor Authentifizierung“ das Modul konfigurieren.



TOTP – Timed One Time Password – Einstellungen:

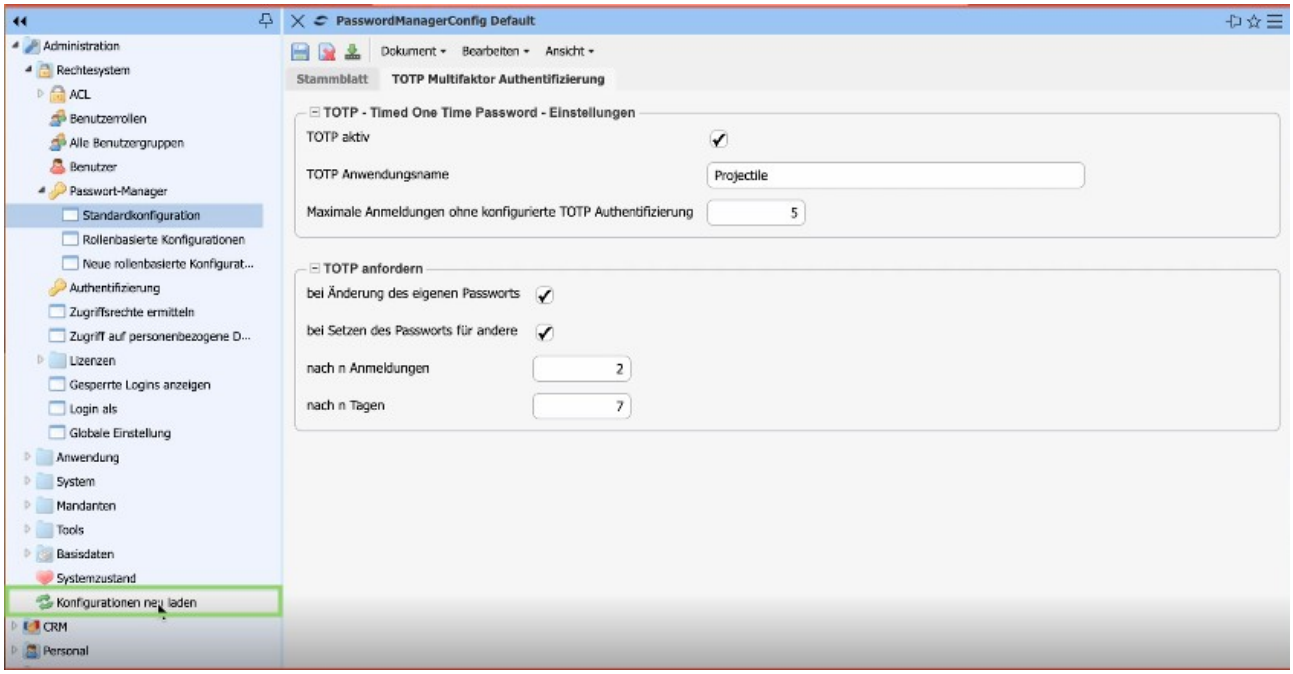
- **TOTP aktiv:** Hier kann man das Modul aktivieren.
- **TOTP Anwendungsname:** An dieser Stelle kann der Namen eintragen werden, der in der Authenticator-App erscheint. Dies erleichtert die Zuordnung, falls noch weitere Programme verwendet werden, die diese App benötigen.
- **Maximale Anmeldungen ohne konfigurierte TOTP Authentifizierung:** Wie oft kann sich ein Nutzer/eine Nutzerin auch ohne Zweifaktor-Authentifizierung anmelden.

TOTP anfordern:

- **bei Änderung des eigenen Passworts:** Hier kann eingestellt werden, ob bei jeder Änderung des eigenen Passworts die Zweifaktor-Authentifizierung notwendig ist.
- **beim Setzen des Passworts für andere:** Hier kann eingestellt werden,

ob beim Setzen eines Passworts für einen anderen Nutzer/eine andere Nutzerin die Zweifaktor-Authentifizierung notwendig ist.

- **nach n Anmeldungen:** An diesem Punkt kann eingestellt werden, nach wie vielen Anmeldungen die Zweifaktor-Authentifizierung notwendig ist.
- **nach n Tagen:** An dieser Stelle kann eingestellt werden, nach wie vielen Tagen die Zweifaktor-Authentifizierung notwendig ist.

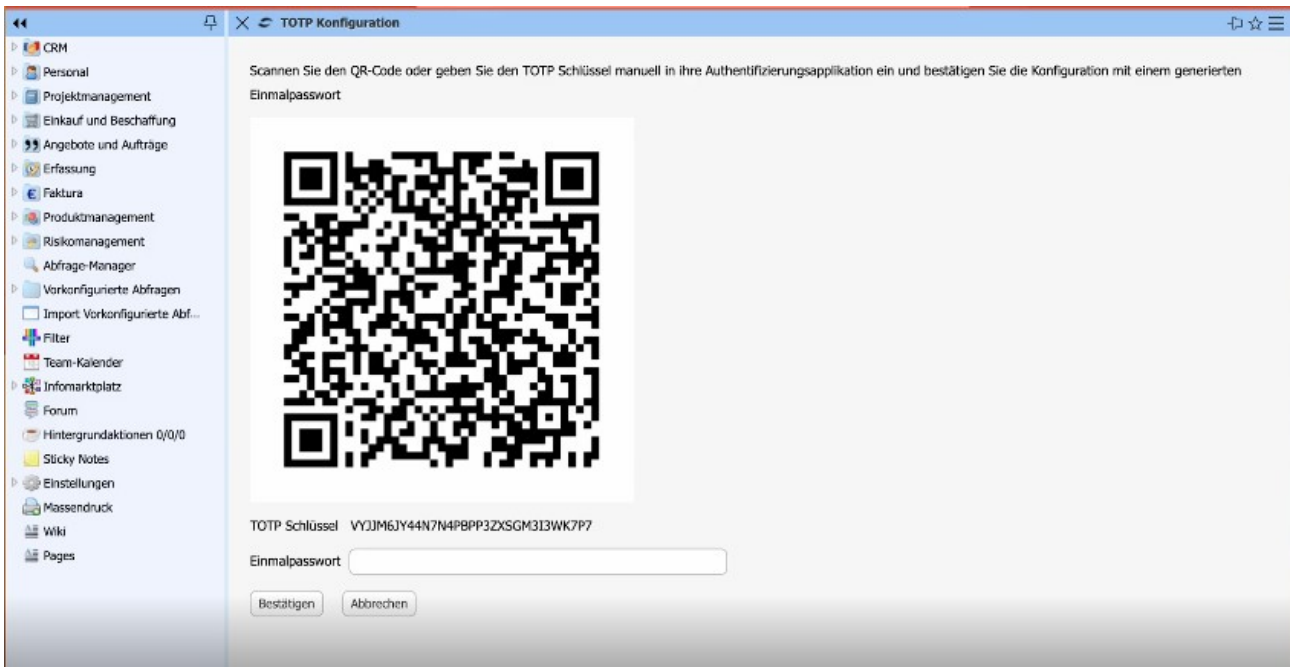


Somit ist das Modul vollständig konfiguriert. Jetzt muss es gespeichert und die Konfiguration neu laden werden. Ab dem nächsten Login ist dieses Modul aktiv.

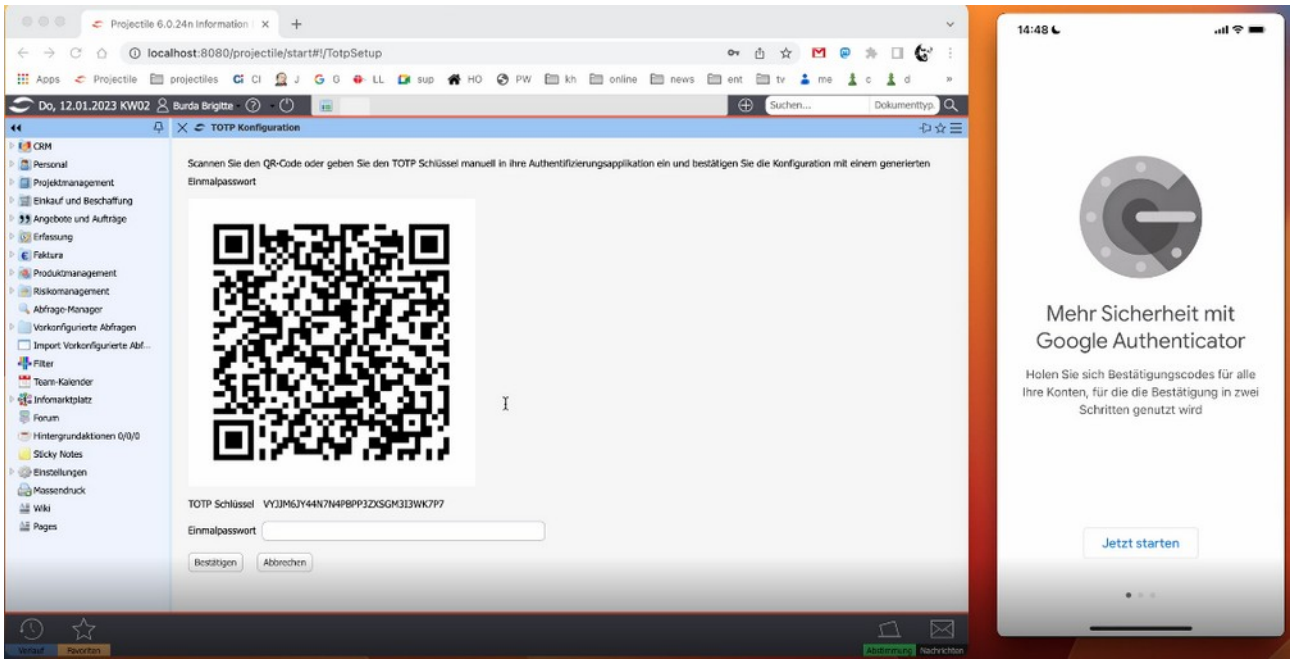
Einrichten der Authentifizierung

Der User muss das Gerät für die Zweifaktor-Authentifizierung nur einmalig einrichten. Man muss den Einrichtungsvorgang nur einmalig ausführen.

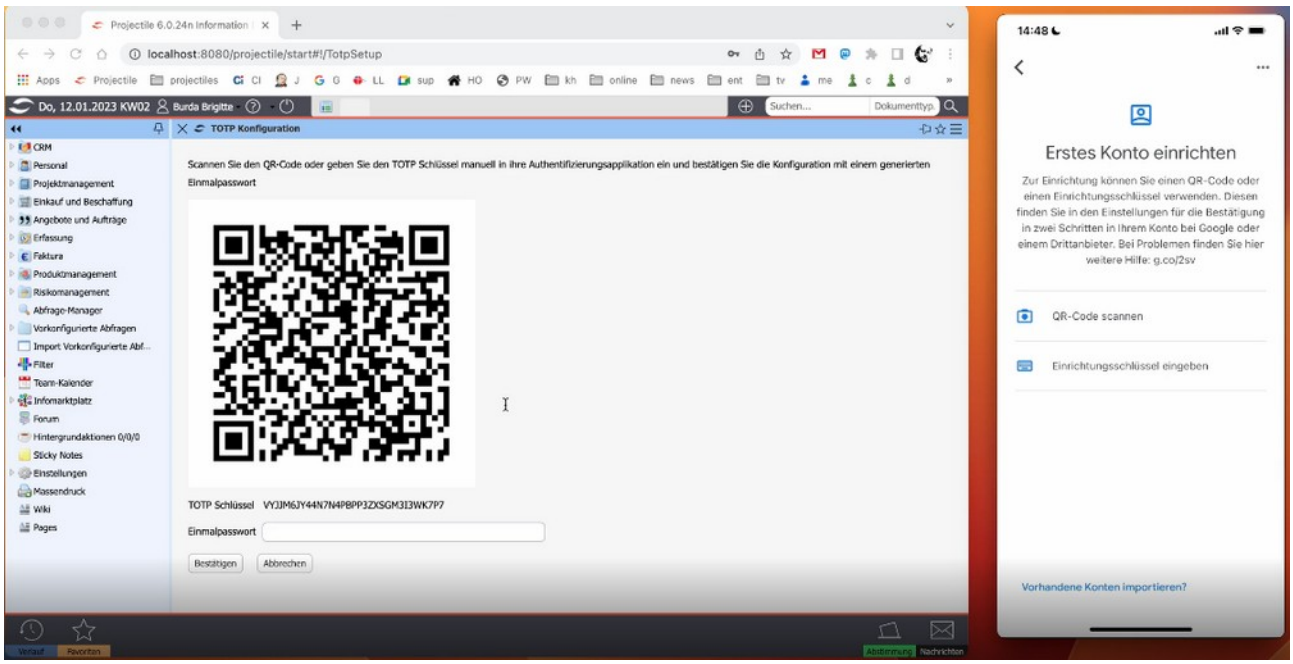
Nach dem Einloggen erscheint ein QR-Code in Projectile.



Rechts neben dem Bildschirm kann man hier die Google Authenticator App auf einem Smartphone gesehen.

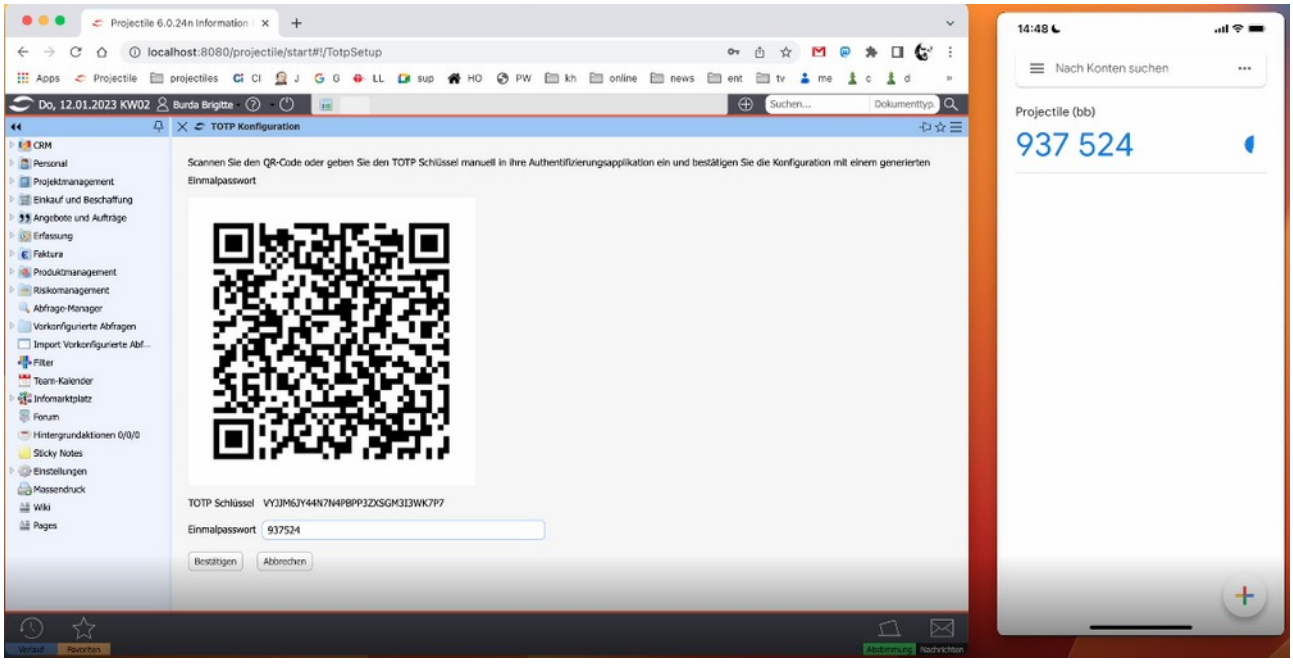


Um ein Konto auf dieser App einzurichten, muss man jetzt den QR-Code mit dem Smartphone scannen.

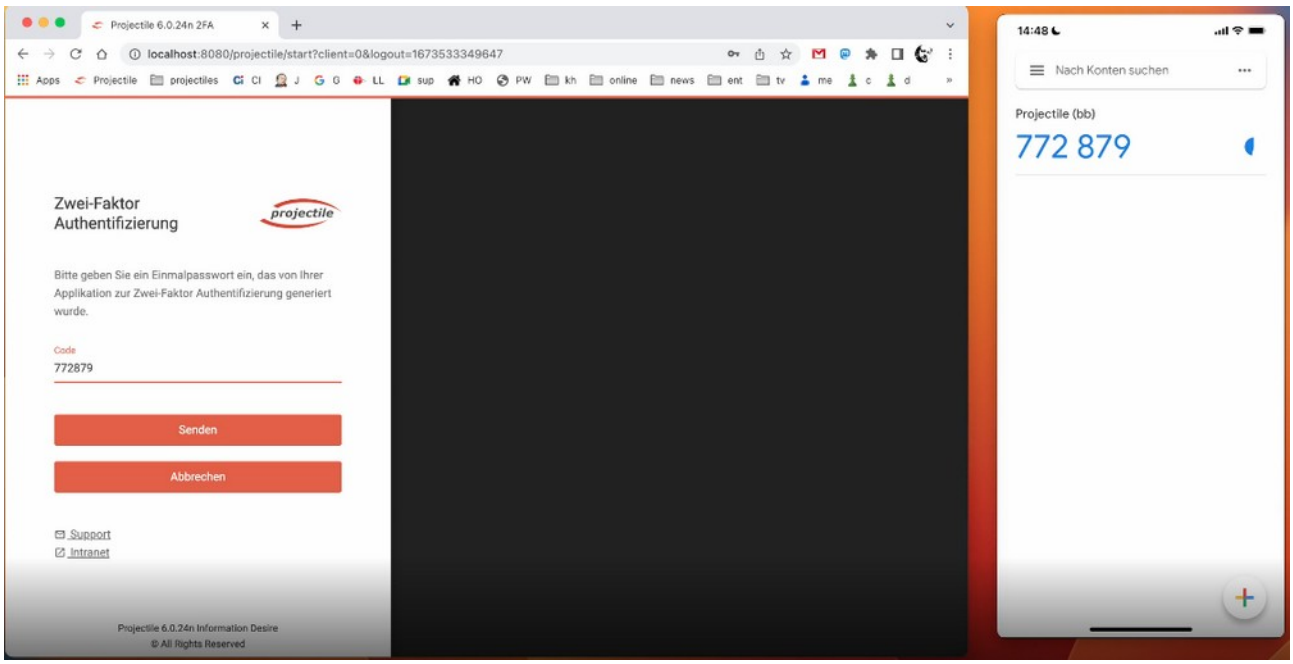


Jetzt wurde ein Konto erstellt. Hier sieht man auch den TOTP-Anwendungsnamen, den man während der Modulkonfiguration eingerichtet hat und den Benutzer in Klammern.

Man muss jetzt das Einmalpasswort (hier: 937 524) unter dem QR-Code eingeben.

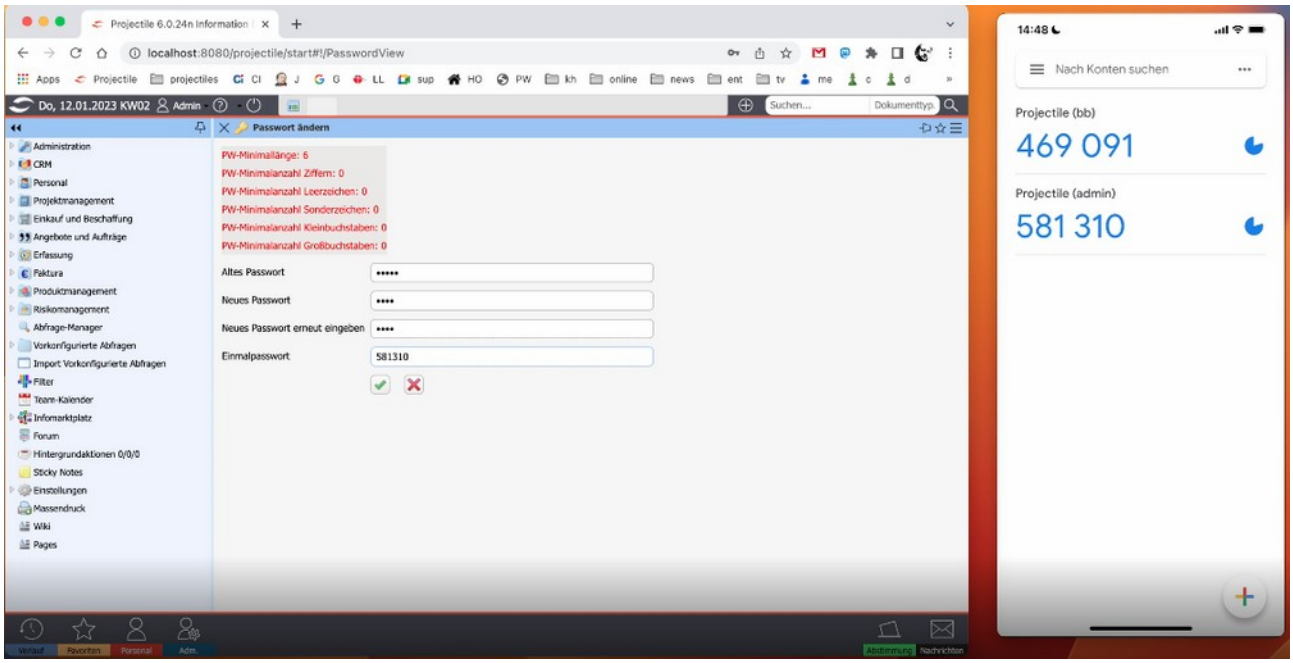


Nun wurde das Smartphone für die Zweifaktor-Authentifikation eingerichtet. Wenn man sich jetzt anmelden will, erscheint der folgende Login-Bildschirm.

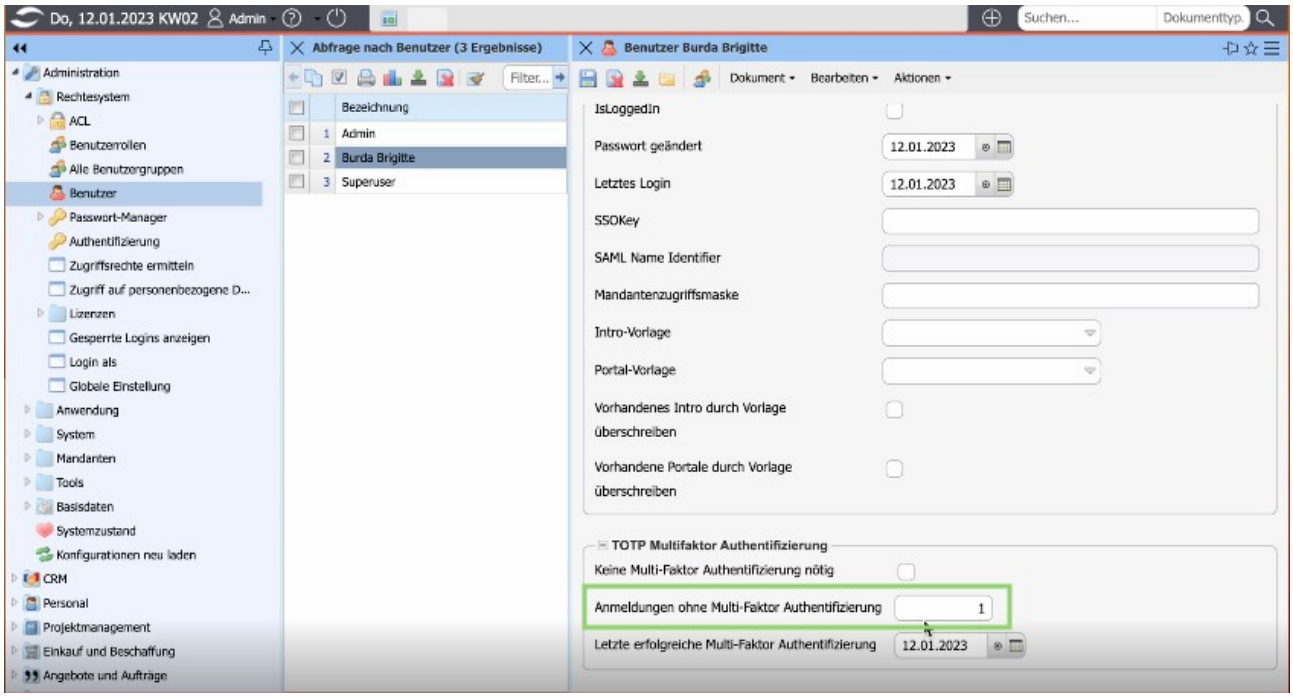


Nachdem man das verlangte Einmalpasswort eingegeben hat, kann Projectile wie gewohnt verwendet werden.

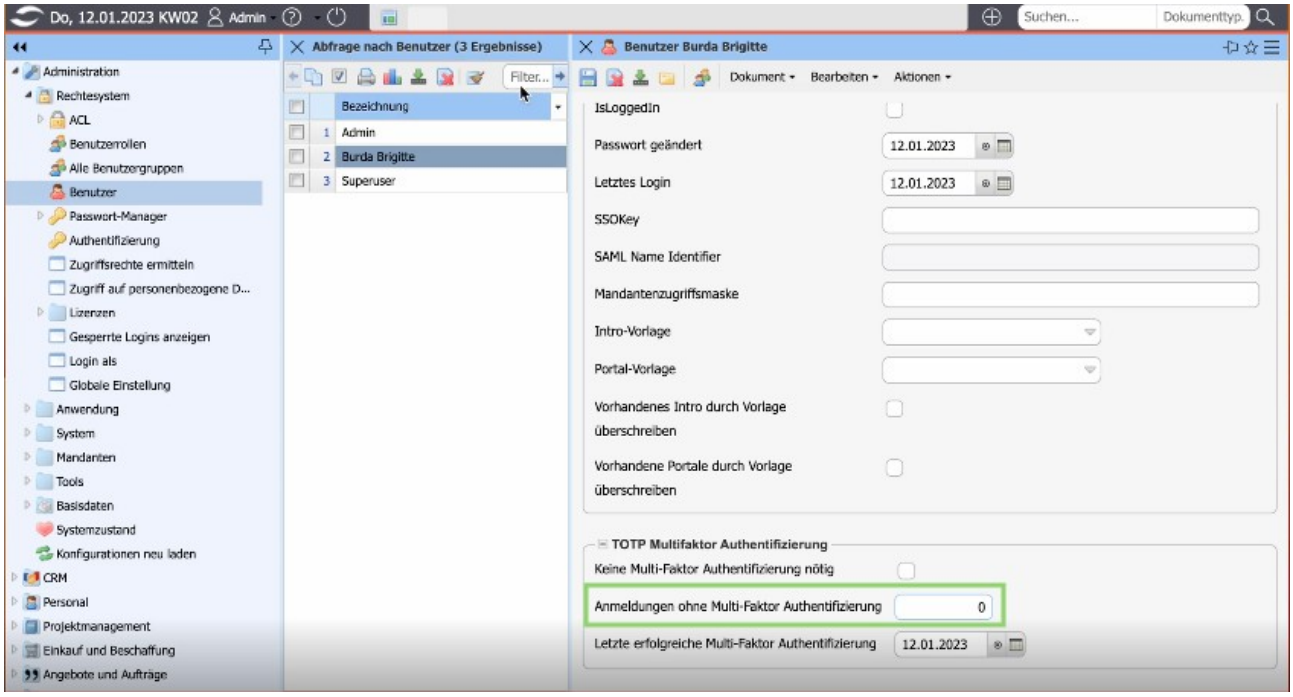
Hier kann man noch einmal sehen, dass man – wenn es so im Modul konfiguriert wurde – ein Einmalpasswort eingeben muss, wenn man das Passwort ändert.



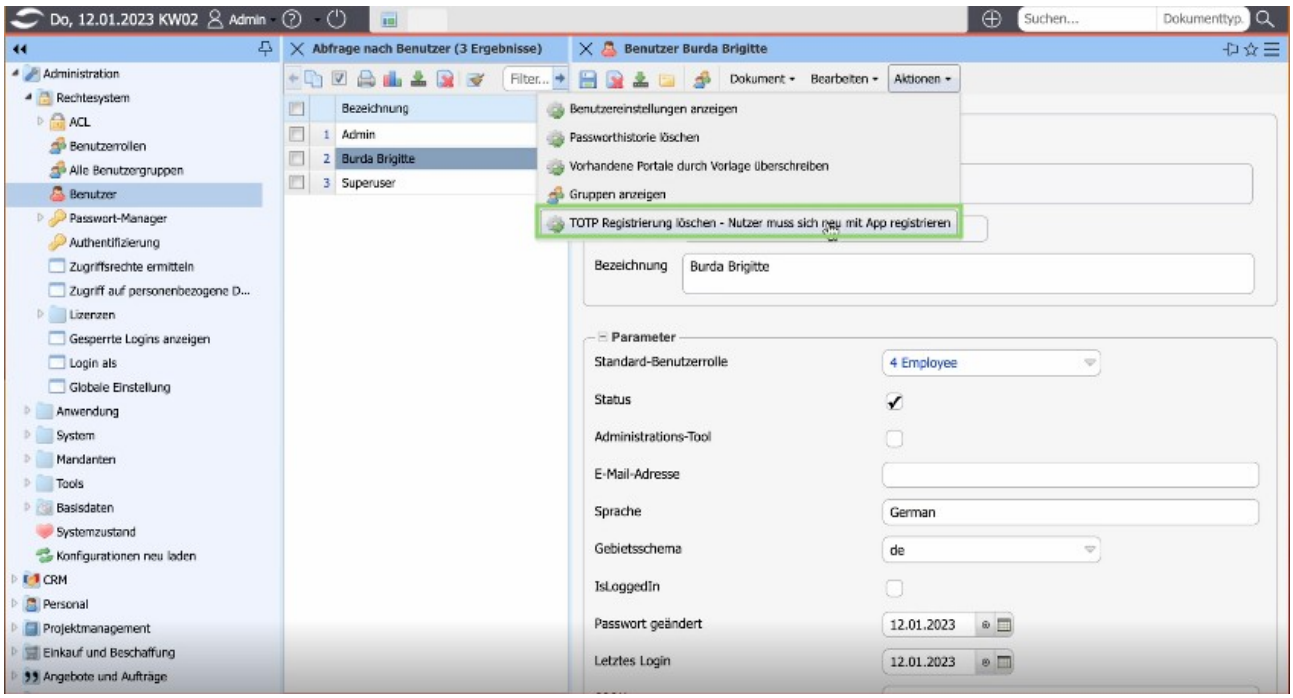
Hat der User einmalig keinen Zugriff auf sein registriertes Smartphone, kann der Admin die Anmeldeversuche zurücksetzen.



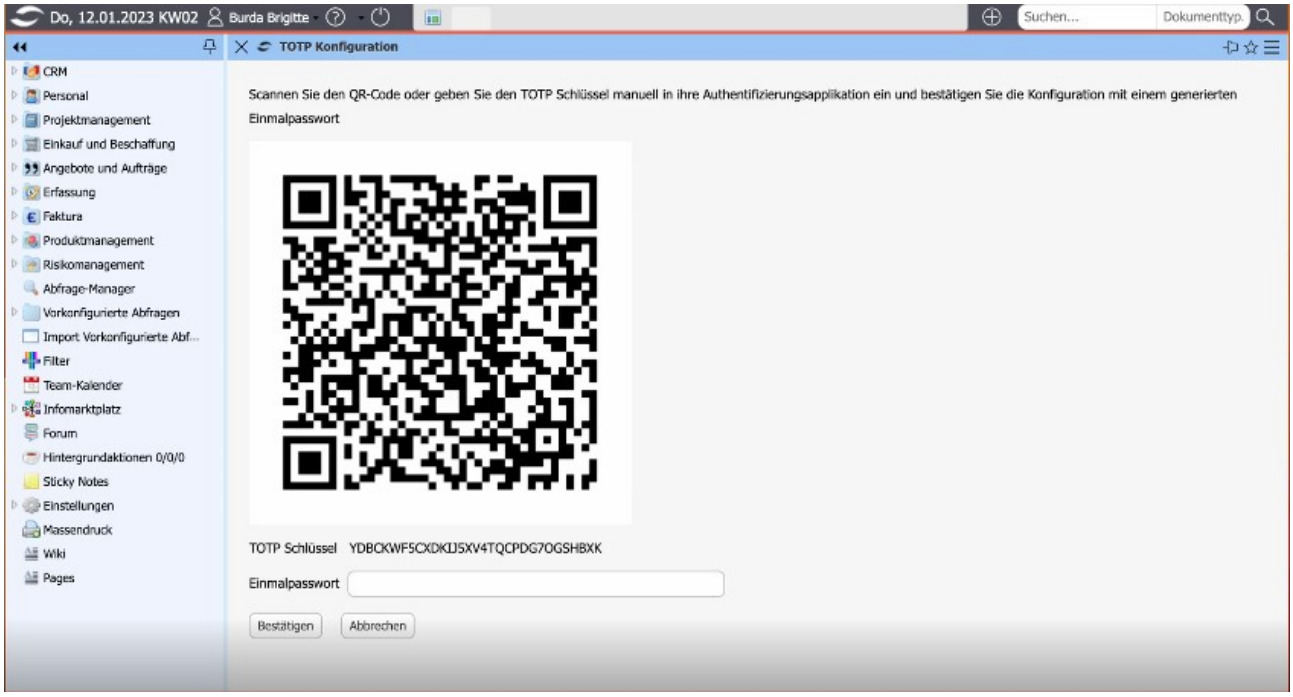
Somit kann der User sich einmalig ohne die Zweifaktor-Authentifizierung anmelden.



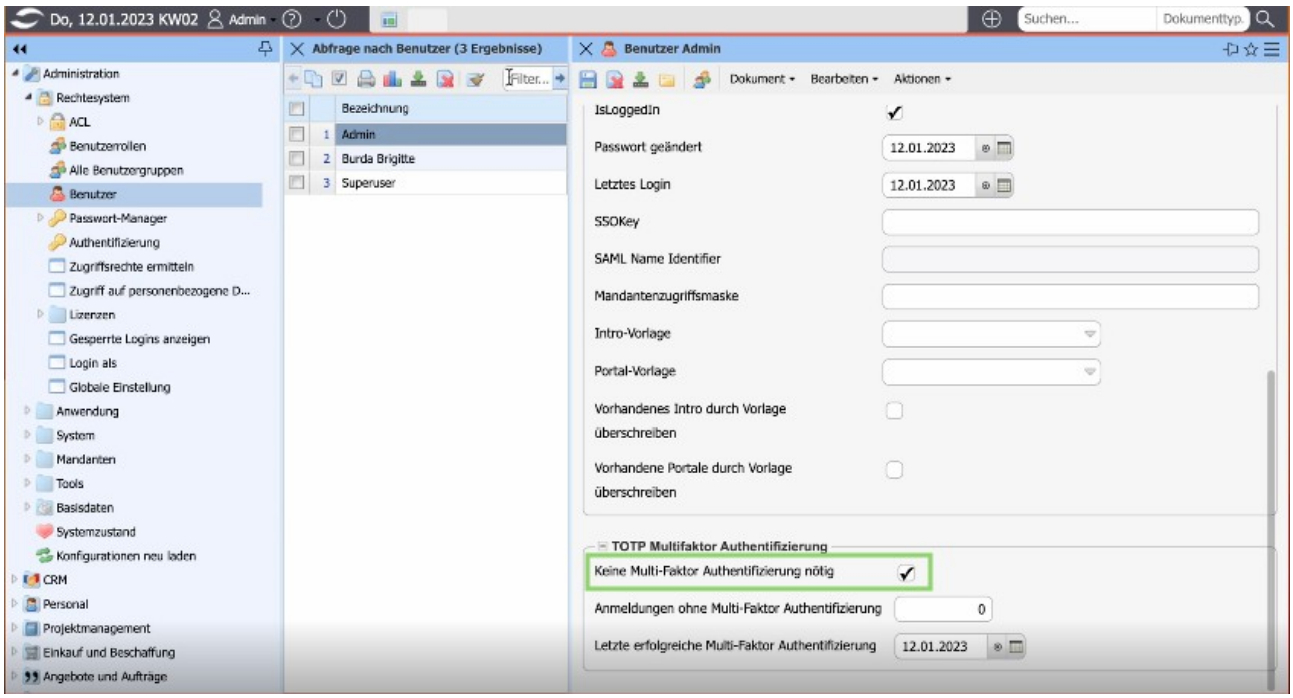
Hat der User gar keinen Zugriff mehr auf sein Smartphone, hat der Admin die Möglichkeit die TOTP-Registrierung für diesen User zu löschen.



Bei dem nächsten Login erscheint erneut der QR-Code und der User muss erneut ein Gerät registrieren.



Ein Admin kann einen bestimmten User auch von der Multi-Faktor Authentifizierung befreien, in dem „Keine Multi-Faktor Authentifizierung nötig" aktiviert wird.


Do, 12.01.2023 KW02
Admin
Suchen...
Dokumenttyp
Administration
Rechtesystem
ACL
Benutzerrollen
Alle Benutzergruppen
Benutzer
Passwort-Manager
Authentifizierung
Zugriffsrechte ermitteln
Zugriff auf personenbezogene D...
Lizenzen
Gesperrte Logins anzeigen
Login als
Globale Einstellung
Anwendung
System
Mandanten
Tools
Basisdaten
Systemzustand
Konfigurationen neu laden
CRM
Personal
Projektmanagement
Einkauf und Beschaffung
Angebote und Aufträge
Abfrage nach Benutzer (3 Ergebnisse)
Filter...
Bezeichnung
1 Admin
2 Burda Brigitte
3 Superuser
Benutzer Admin
Dokument
Bearbeiten
Aktionen
IsLoggedIn
Passwort geändert
12.01.2023
Letztes Login
12.01.2023
SSOKey
SAML Name Identifier
Mandantenzugriffsmaske
Intro-Vorlage
Portal-Vorlage
Vorhandenes Intro durch Vorlage überschreiben
Vorhandene Portale durch Vorlage überschreiben
TOTP Multifaktor Authentifizierung
Keine Multi-Faktor Authentifizierung nötig
Anmeldungen ohne Multi-Faktor Authentifizierung
0
Letzte erfolgreiche Multi-Faktor Authentifizierung
12.01.2023