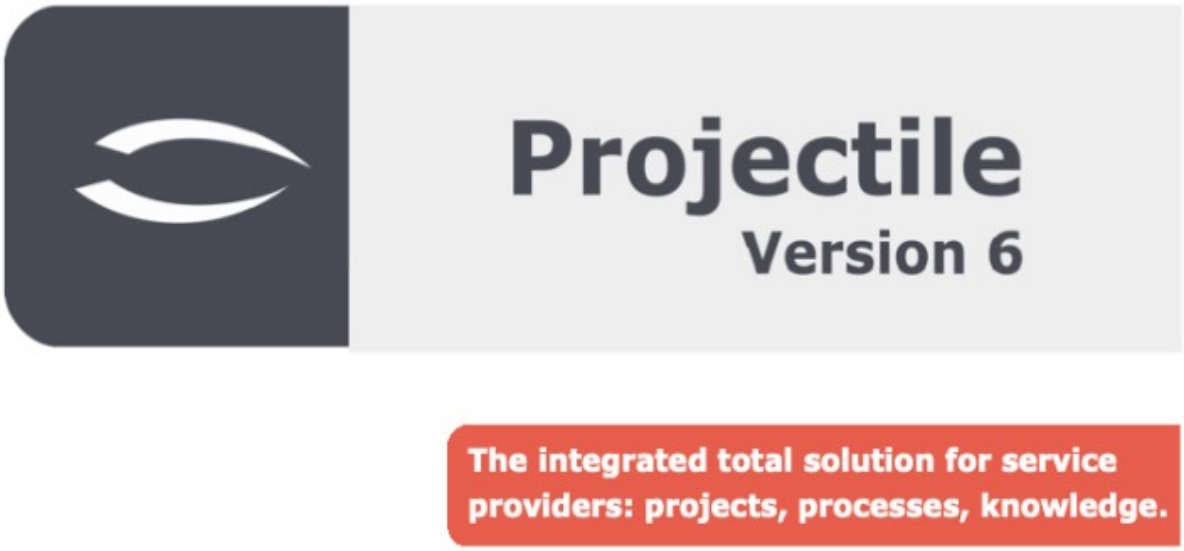


Multi-Factor Authentication with TOTP (Time Based One-Time Password)

© Information Desire Software GmbH

Multi-Factor Authentification with TOTP

Multi-factor authentification is used to make logging into Projectile more secure.

Normally you log in to a website (with login name and password). This happens over a network connection and this is the 1st factor. Since this network connection can be intercepted, it is now common to use a 2nd factor for security, which runs through another device, another connection. Usually one uses a cell phone or a special device for this purpose.

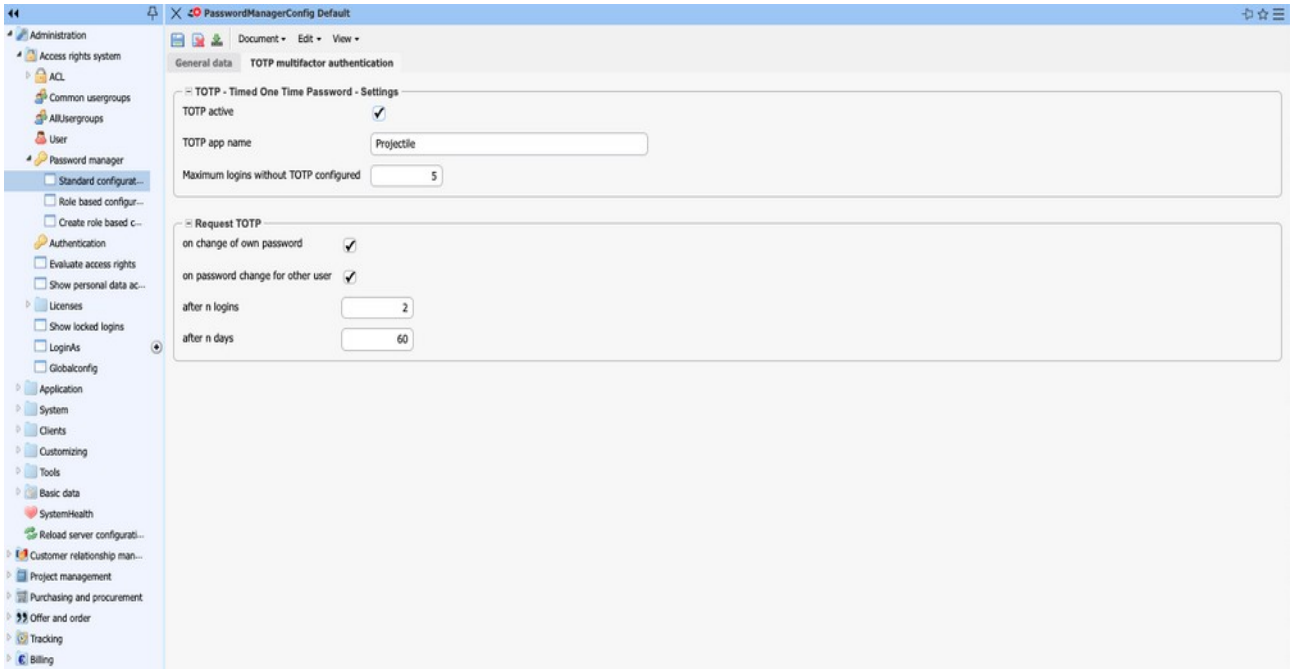
In the case of Projectile, there is an app on the cell phone called Authenticator.

A one-time password a password that is valid only once. Time-based means that it is calculated based on the current time.

Additionally, one has to register the cell phone beforehand. Through a QR code, the user is registered in the app and connected to Projectile and so the 2nd factor can give an additional security that only allowed people use Projectile.

Activating & Configuring the TOTP Module

A user with the appropriate authorization can configure the module in the password manager on the new "TOTP Multifactor Authentication" tab.



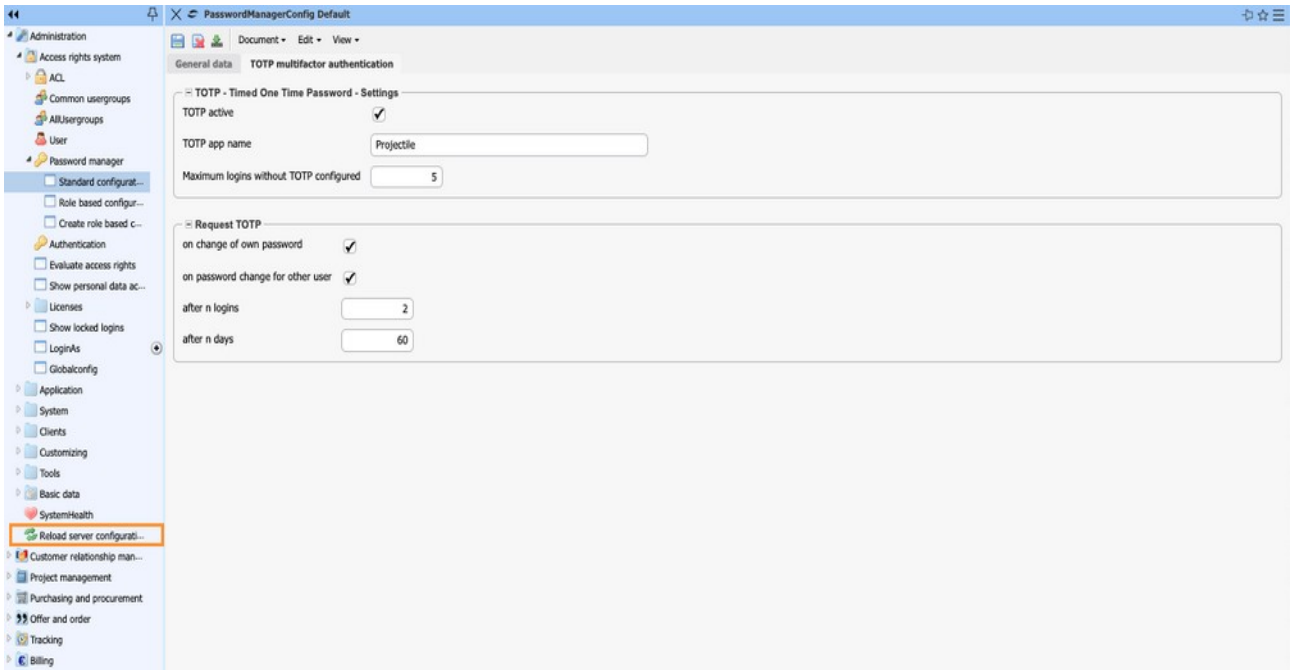
TOTP - Timed One Time Password - Settings:

- **TOTP active:** Here you can activate the module.
- **TOTP App Name:** The name that appears in the Authenticator app can be entered here. This facilitates the assignment if other programs are used that require this app.
- **Maximum logins without TOTP authentication configured:** How often can a user log in even without two-factor authentication.

Request TOTP:

- **on change of own password:** Here you can set whether two-factor authentication is required each time you change your own password.
- **on password change for other user:** Here you can set whether two-factor authentication is required when setting a password for another user.

- **after n logins:** At this point it is possible to set after how many logins the two-factor authentication is necessary.
- **after n days:** At this point it is possible to set after how many days the two-factor authentication is necessary.



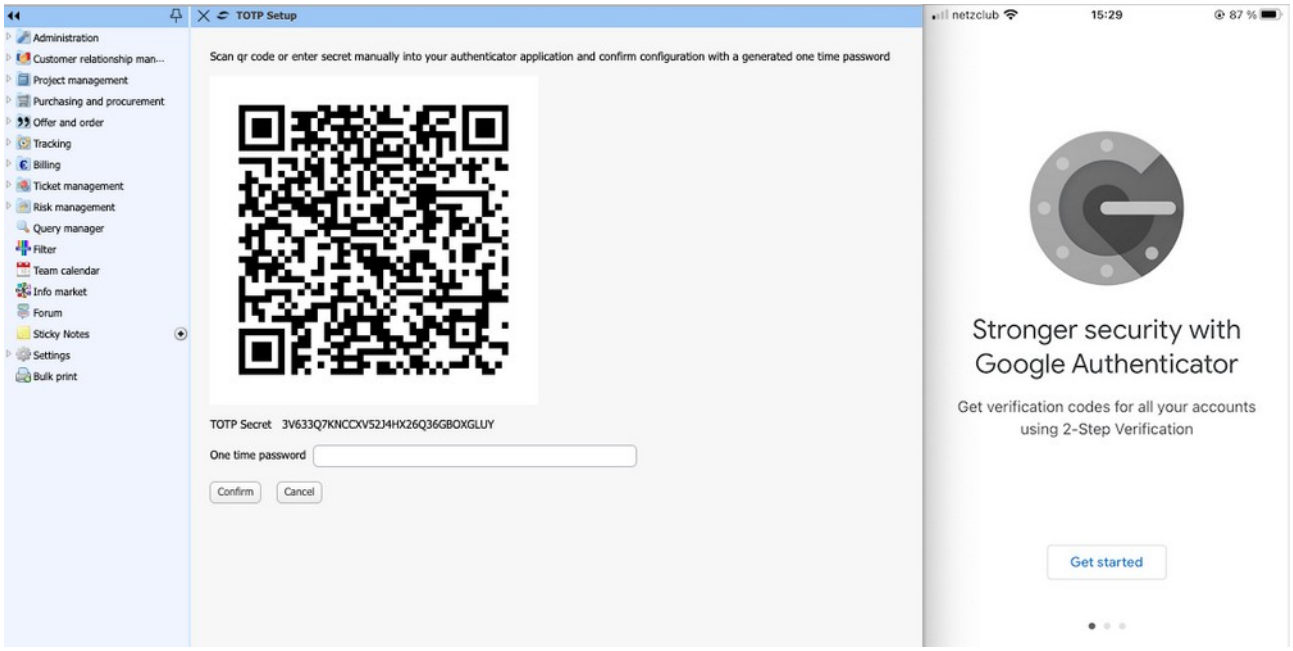
The module is now completely configured. Now it must be saved and the configuration must be reloaded. From the next login this module is active.

Setting Up Authentification

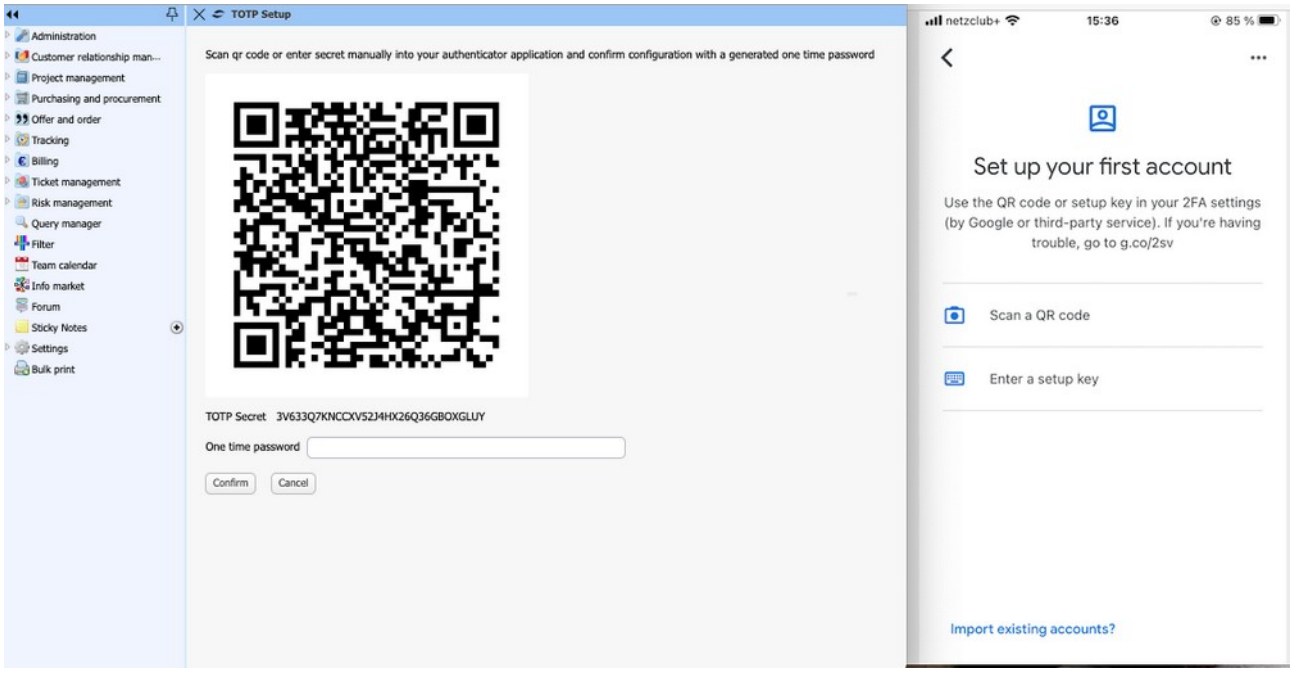
The user needs to set up the device for two-factor authentication only once. One needs to perform the setup process only once.

After logging in, a QR code appears in Projectile.

To the right you can see the Google Authenticator app on a smartphone.

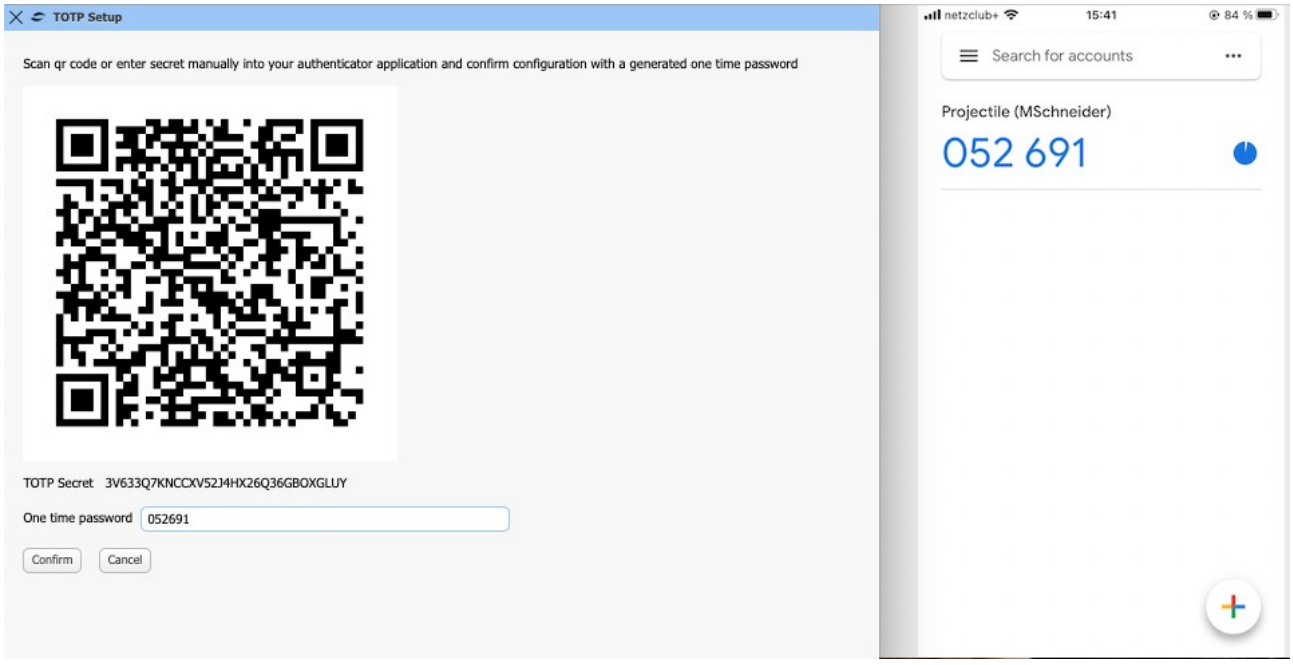


Now, to create an account on this app, you need to scan the QR code with your smartphone.

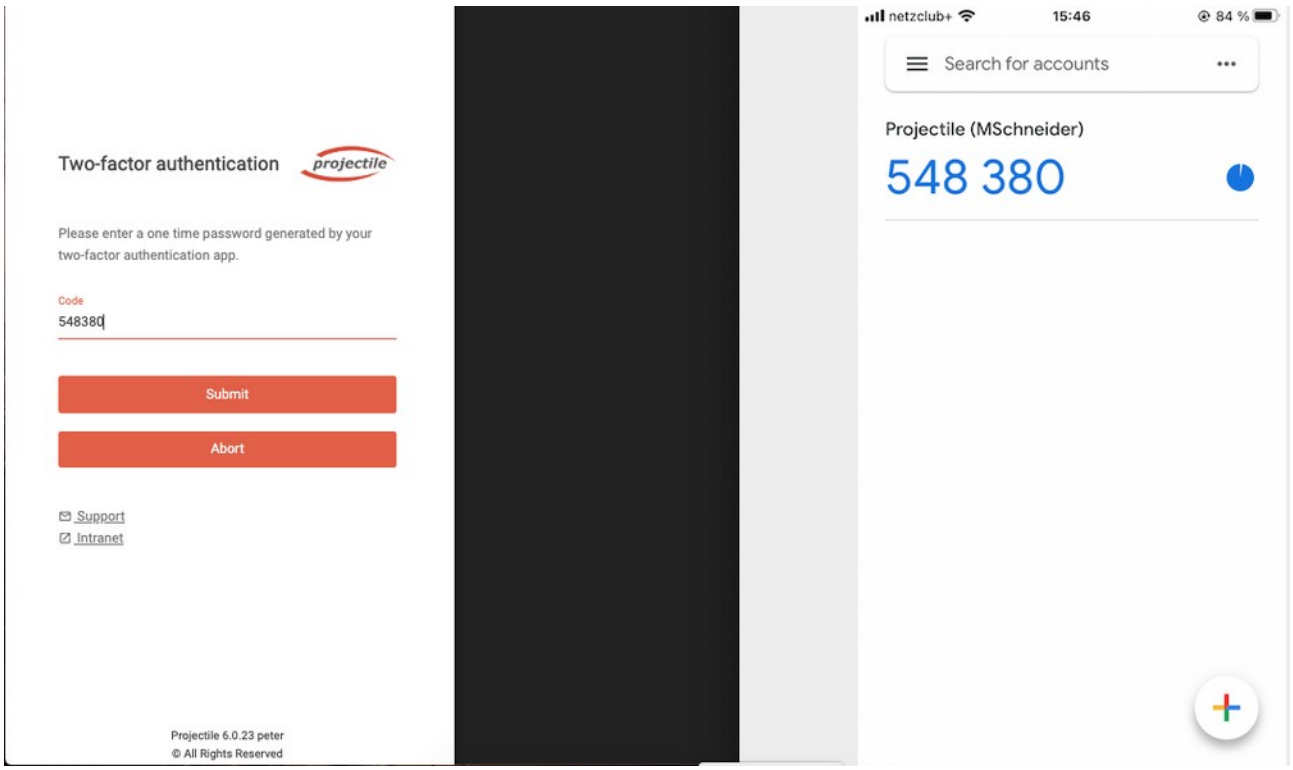


Now an account has been created. Here you can also see the TOTP application name that you set up during the module configuration and the user in brackets.

One must now enter the one-time password (here: 052 691) under the QR code.

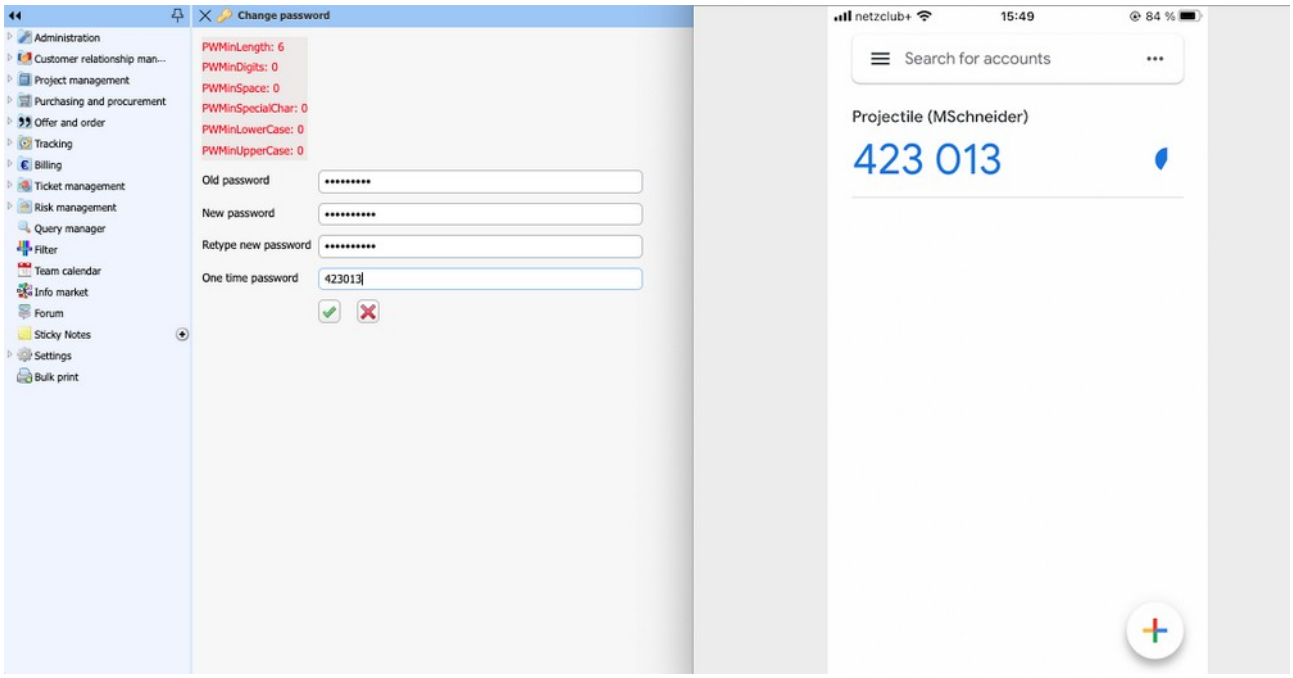


Now the smartphone has been set up for two-factor authentication. If you want to log in now, the following login screen appears.

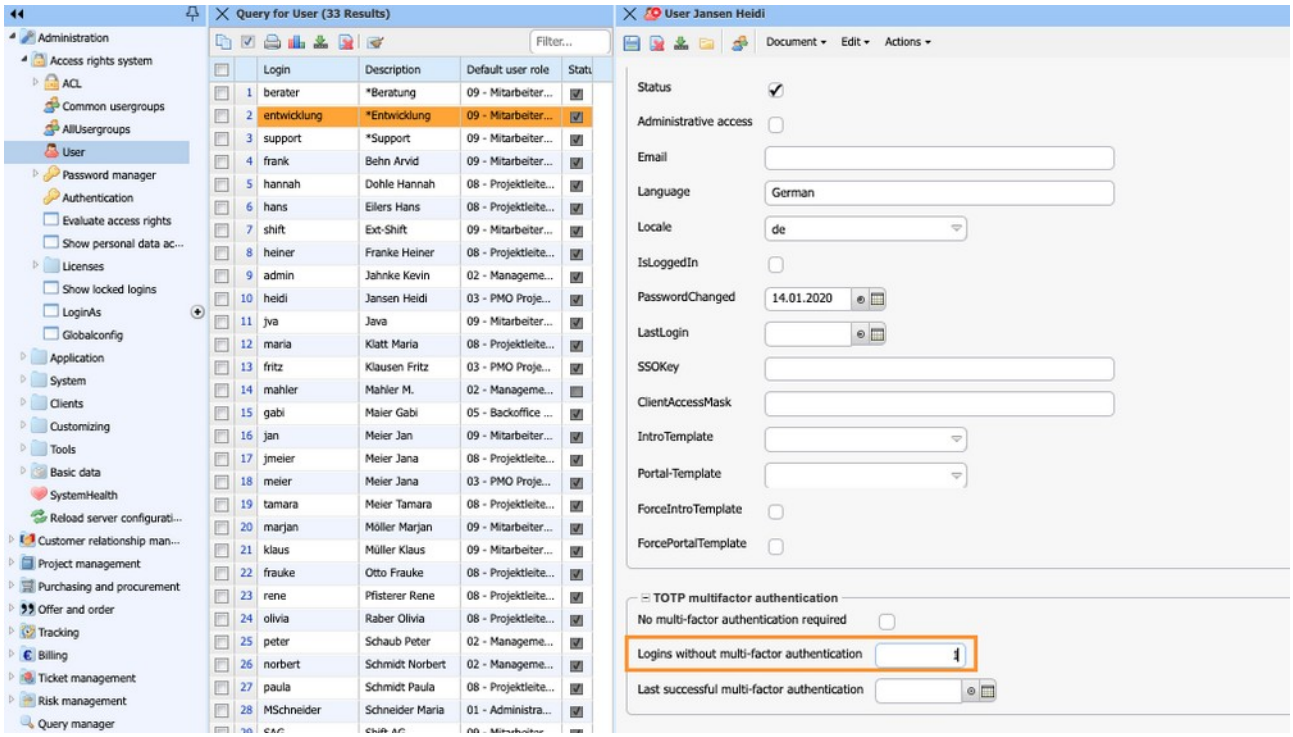


After entering the required one-time password, Projectile can be used as usual.

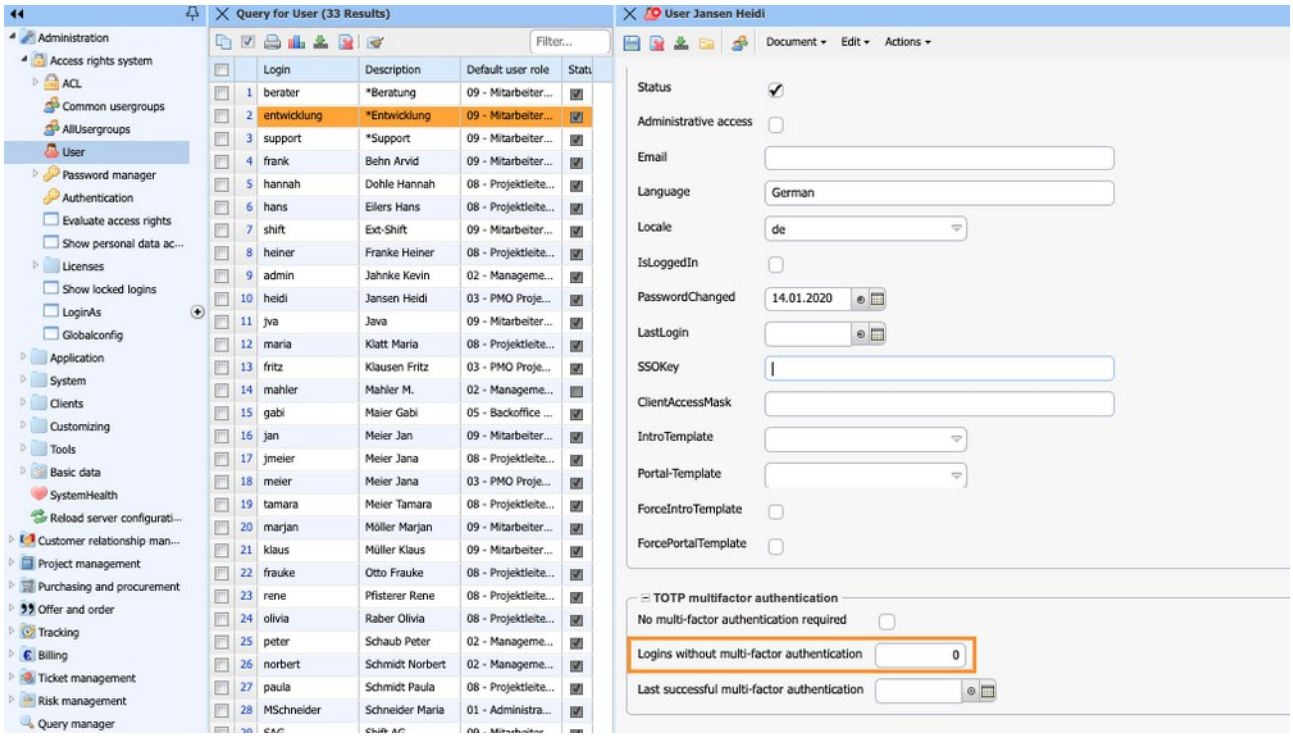
Here you can see once again that - if it was configured like this in the module - you have to enter a one-time password when you change the password.



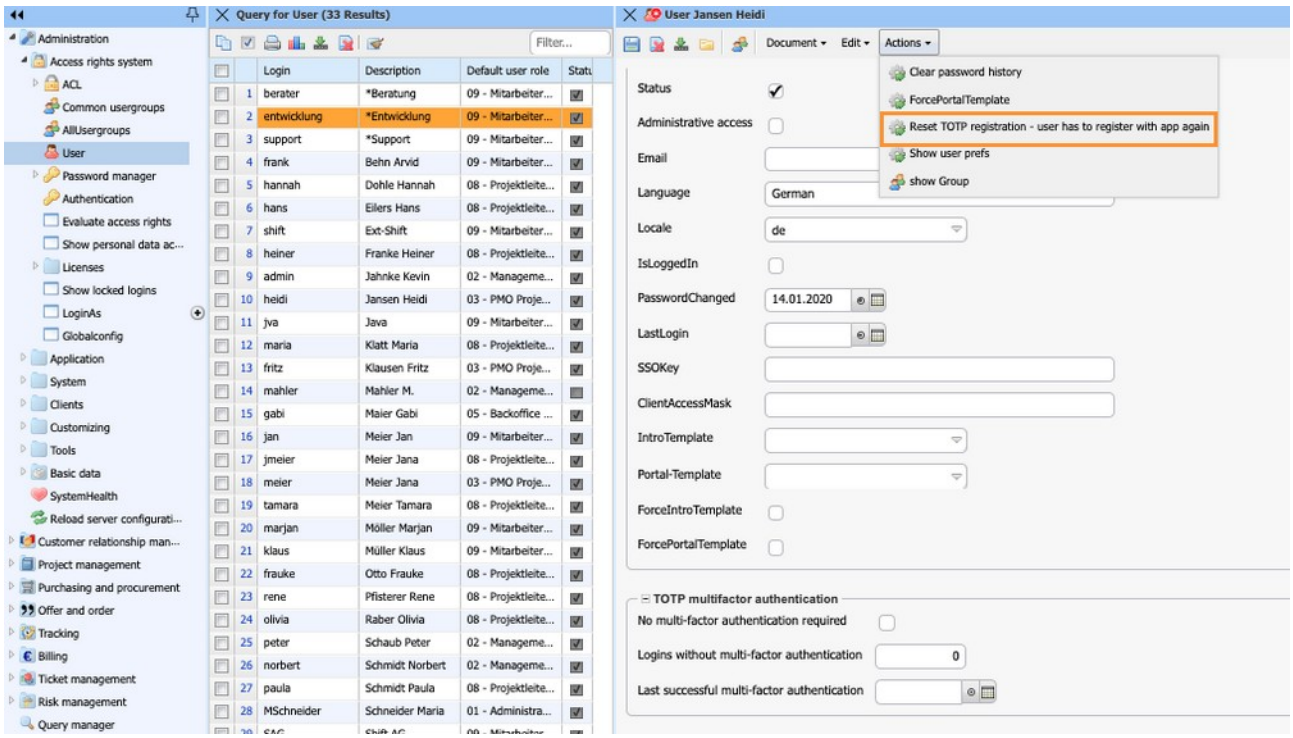
If the user has no access to his registered smartphone once, the admin can re-set the login attempts.



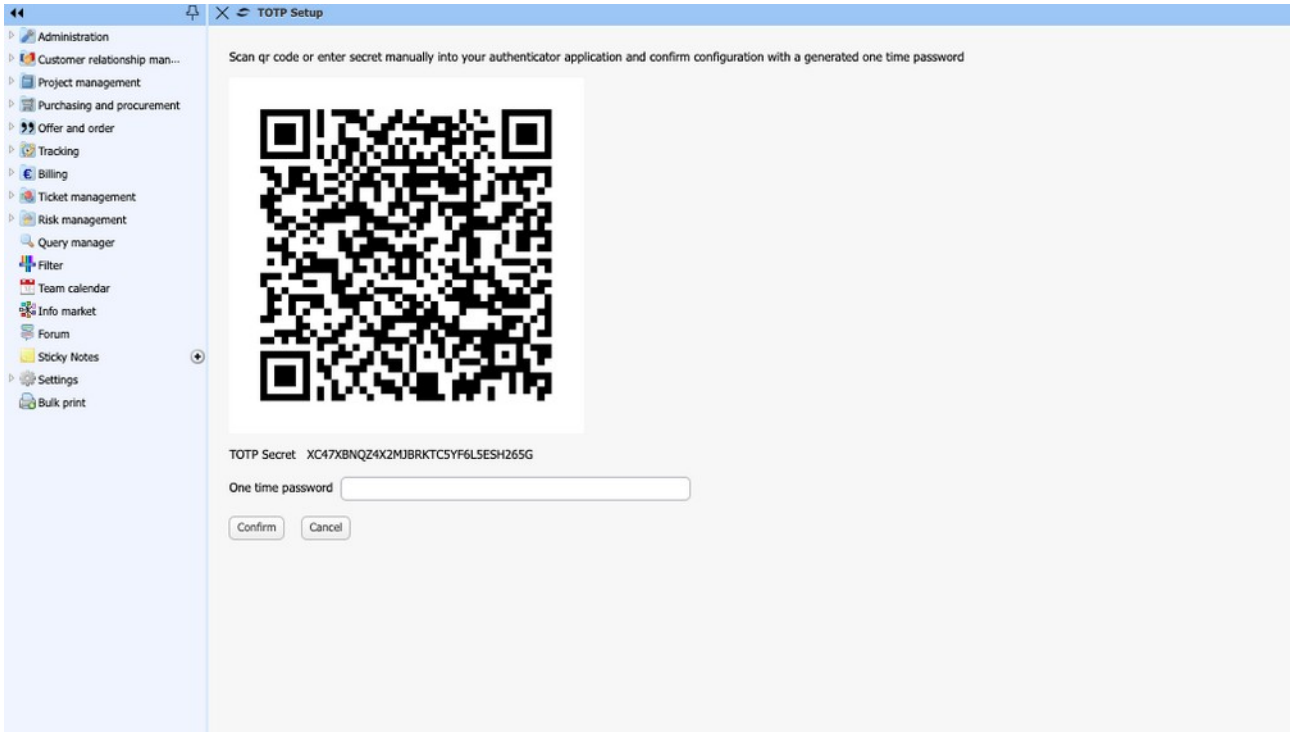
This enables the user to log in once without the two-factor authentication.



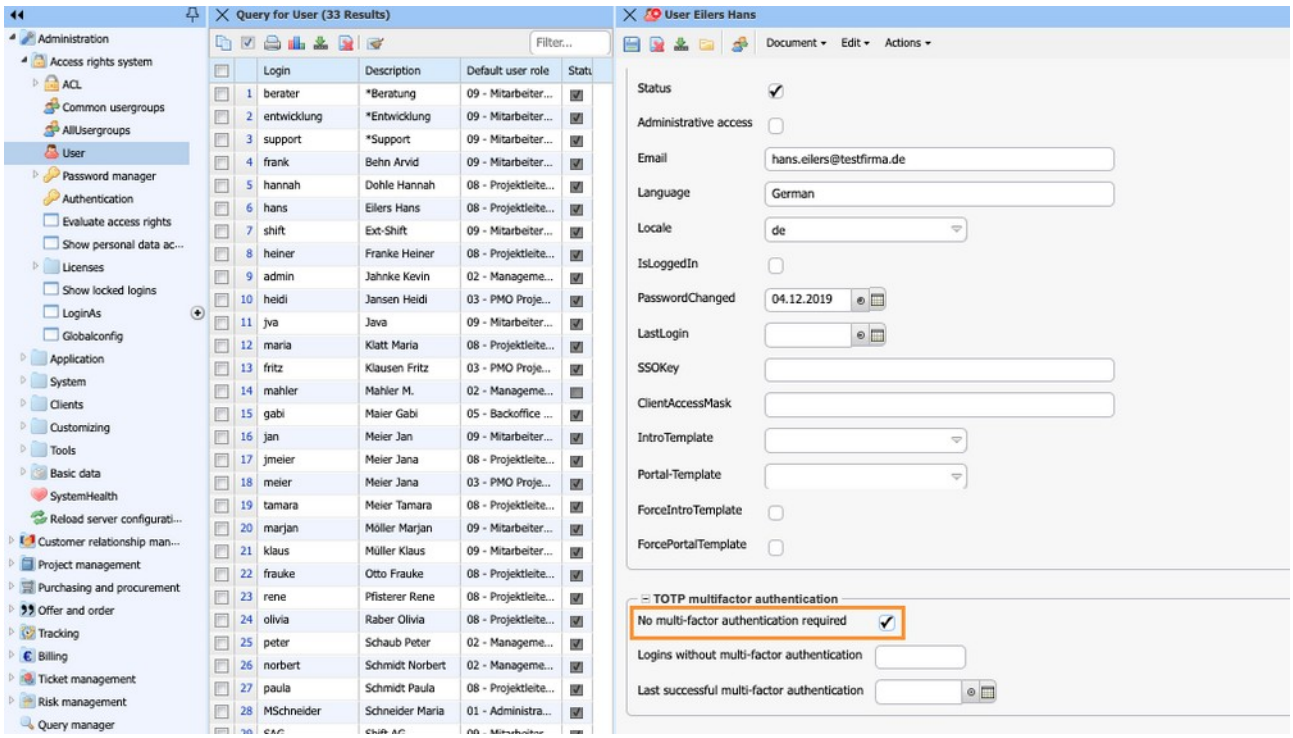
If the user has no access to his smartphone anymore, the admin has the possibility to delete the TOTP registration for this user.



At the next login, the QR code appears again and the user has to register a device again.



An admin can also exempt a particular user from multi-factor authentication by enabling "No multi-factor authentication required".


Administration
Access rights system
ACL
Common usergroups
AllUsergroups
User
Password manager
Authentication
Evaluate access rights
Show personal data ac...
Licenses
Show locked logins
LoginAs
Globalconfig
Application
System
Clients
Customizing
Tools
Basic data
SystemHealth
Reload server configurati...
Customer relationship man...
Project management
Purchasing and procurement
Offer and order
Tracking
Billing
Ticket management
Risk management
Query manager
Query for User (33 Results)
Filter...
Login
Description
Default user role
1 berater *Beratung 09 - Mitarbeiter...
2 entwicklung *Entwicklung 09 - Mitarbeiter...
3 support *Support 09 - Mitarbeiter...
4 frank Behn Arvid 09 - Mitarbeiter...
5 hannah Dohle Hannah 08 - Projektleite...
6 hans Eilers Hans 08 - Projektleite...
7 shift Ext-Shift 09 - Mitarbeiter...
8 heiner Franke Heiner 08 - Projektleite...
9 admin Jahnke Kevin 02 - Manageme...
10 heidi Jansen Heidi 03 - PMO Proje...
11 jva Java 09 - Mitarbeiter...
12 maria Klatt Maria 08 - Projektleite...
13 fritz Klausen Fritz 03 - PMO Proje...
14 mahler Mahler M. 02 - Manageme...
15 gabi Maier Gabi 05 - Backoffice ...
16 jan Meier Jan 09 - Mitarbeiter...
17 jmeier Meier Jana 08 - Projektleite...
18 meier Meier Jana 03 - PMO Proje...
19 tamara Meier Tamara 08 - Projektleite...
20 marjan Möller Marjan 09 - Mitarbeiter...
21 klaus Müller Klaus 09 - Mitarbeiter...
22 frauke Otto Frauke 08 - Projektleite...
23 rene Pfisterer Rene 08 - Projektleite...
24 olivia Raber Olivia 08 - Projektleite...
25 peter Schaub Peter 02 - Manageme...
26 norbert Schmidt Norbert 02 - Manageme...
27 paula Schmidt Paula 08 - Projektleite...
28 MSchneider Schneider Maria 01 - Administra...
User Eilers Hans
Document
Edit
Actions
Status
Administrative access
Email hans.eilers@testfirma.de
Language German
Locale de
IsLoggedIn
PasswordChanged 04.12.2019
LastLogin
SSOKey
ClientAccessMask
IntroTemplate
Portal-Template
ForceIntroTemplate
ForcePortalTemplate
TOTP multifactor authentication
No multi-factor authentication required
Logins without multi-factor authentication
Last successful multi-factor authentication