## Meta description

2FA implemented via Google Authenticator. Logging into the system requires additional key generated on your mobile device.

Two-factor authentification

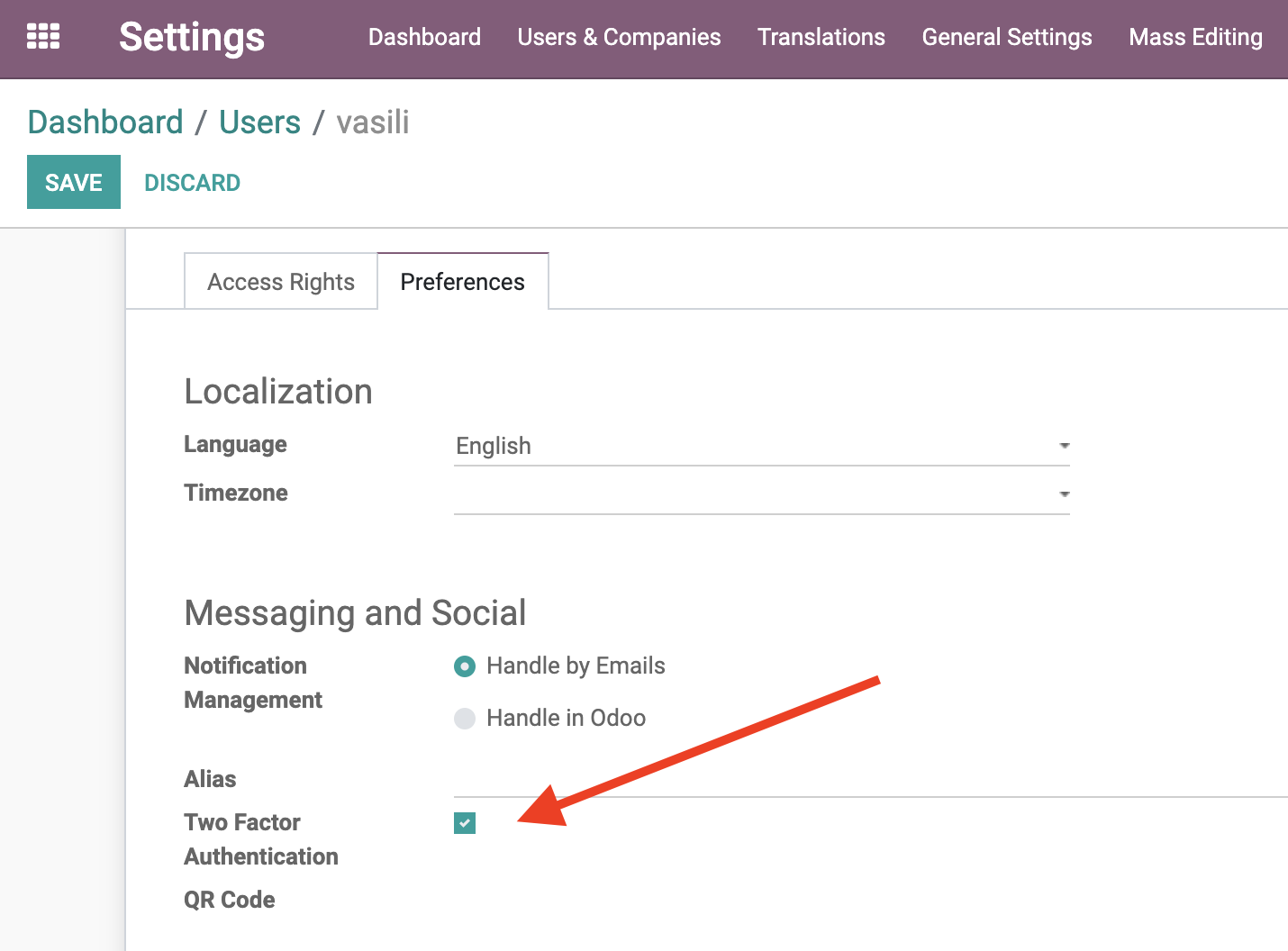
**TO AVOID ANY ISSUES, PLEASE, USE ALWAYS LATEST VERSION FROM** [OUR GITHUB REPOSITORY](https://github.com/ventor-tech/merp/tree/12.0)

The fact of having sensitive data on the web, and only protected by a single password is not acceptable from a data security point of view.

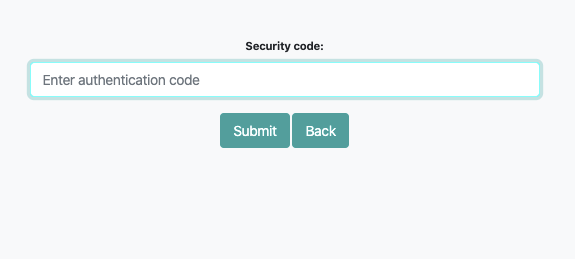
The risks are well known, loss of reputation, fines, legal action, partial or total loss of business, cost of recovery.

## The module functionality

You will be able to switch on the 2FA for every user

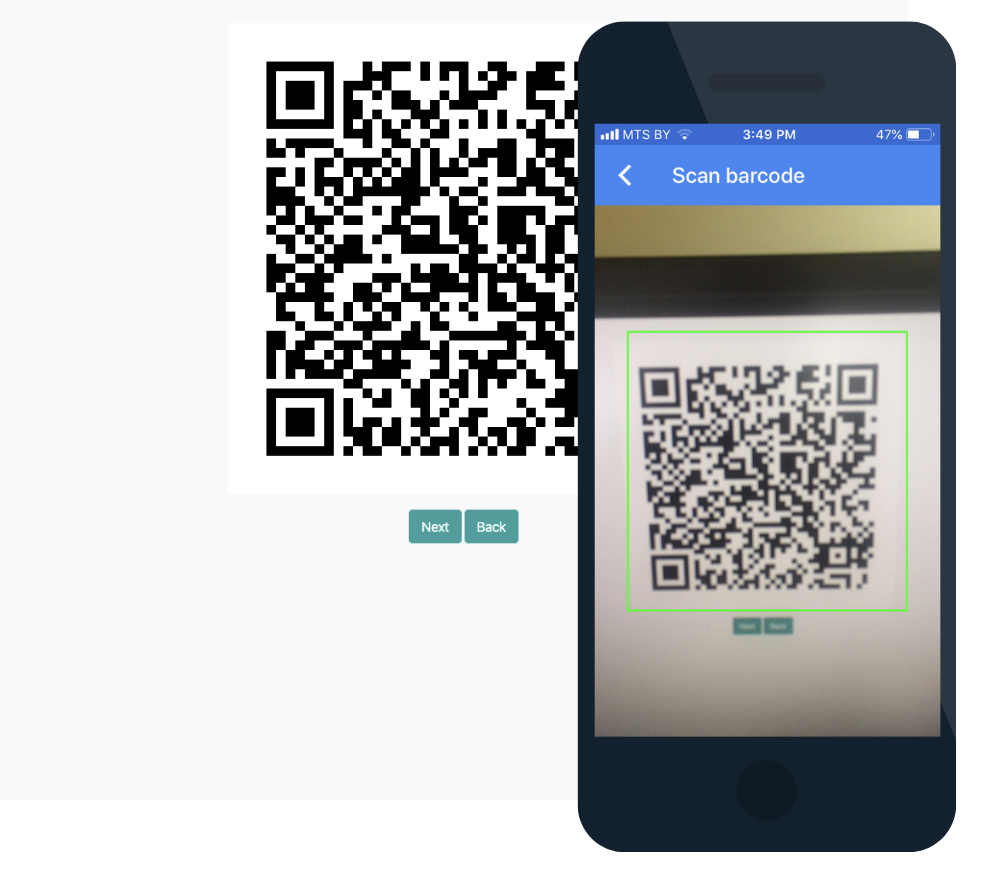


Then while logging they will be requested for an additional key

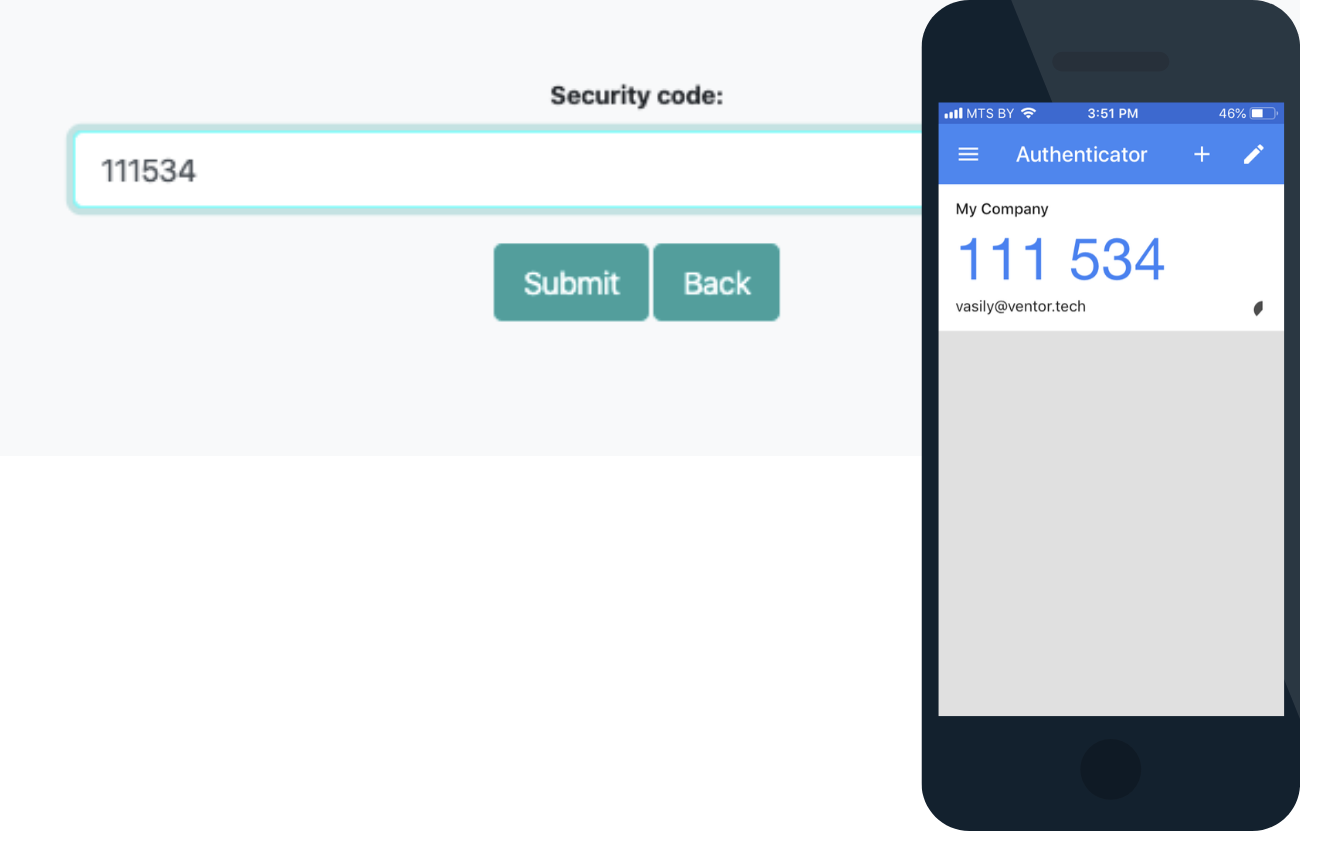


The key is generated by the Google Authenticator mobile app <https://www.google.com/landing/2step/#tab=how-it-works>

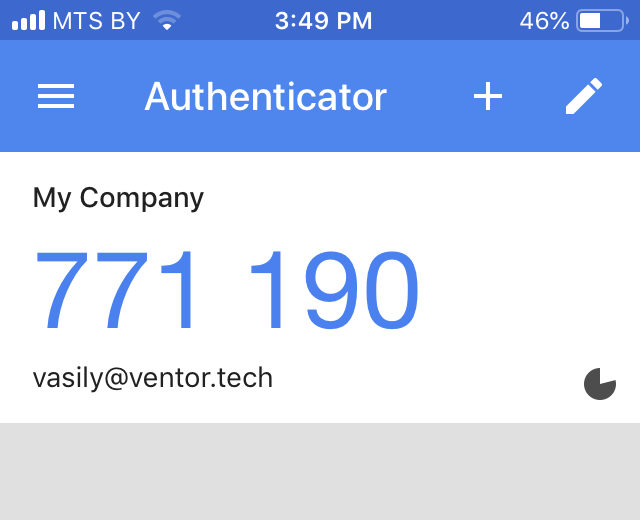
While the first login you need to scan a QR code using this app

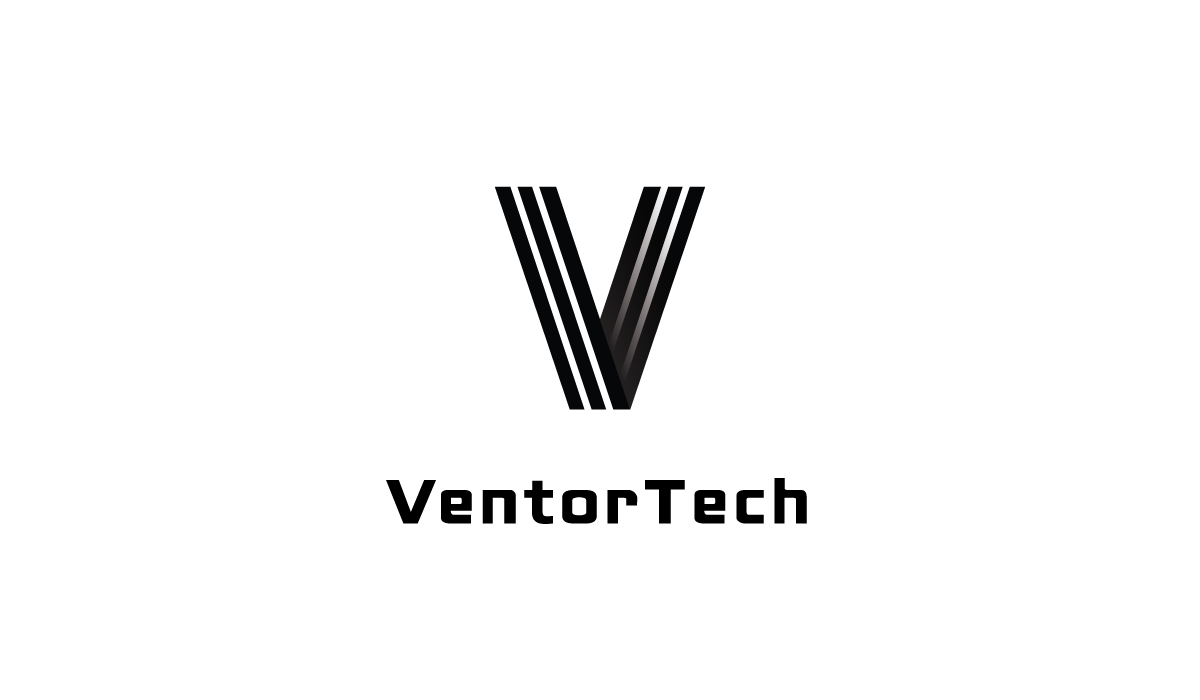


And the app shows you the key you need to insert into a related field



When you log in again the scanning isn’t required. The app resets the key about every minute and generates a new one





[ventor.tech](https://ventor.tech/)