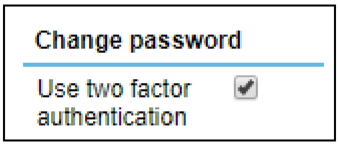
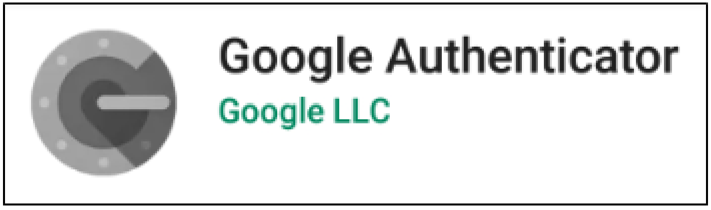
Two Factor Authentication

Two-factor authentication

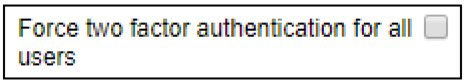
An additional **factor authentification** is an option available to each user, which enables functionality that requires a combination of two separate factors of identification in order to **log** into the system. Besides regular login credentials (operator code, login and password) the user has to obtain 6-digit authentification code to log into Leon. This functionality is a measure of additional security of the user account.

Enabling the two-factor authentication mechanism:

1. Mark the checkbox **Two-factor authentification** in the user's profile and confirm by updating the page. 
   Change password
   Use two factor authentication ☑
2. Check your work email INBOX for the new email from Leon. The email will include the change of password as well as the link that will allow you to **pair the mobile device with Leon** via **Google Authenticator** app.
3. Download a mobile app **Google Authenticator** (available for iOS and Android) or similar. 

4. Pair your app with Leon by using the QR code generated via “Pair your mobile device with Leon!” link received in an email.
5. Log into Leon as usual - when the pop-up window requiring authentification code comes up, use the code generated by the app.

It is possible to **mark two-factor authentication for all the users at once**. To do that, you need to go to the ' Settings' > 'General Settings' section and mark **'Force two factor authentication for all users'** checkbox. The checkbox is unticked by default.


Force two factor authentication for all users □

Each code is valid for 60 seconds only. After this time a new code will be issued. Make sure to enter the code and confirm before the 60 seconds period passes.