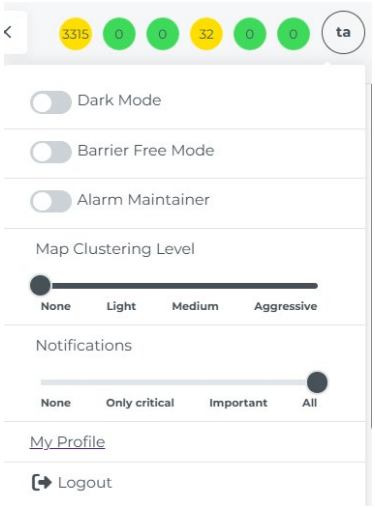
Multi Factor Authentication (MFA)

The Two Factor Authentication adds an additional verification layer when accessing your MyCity account.

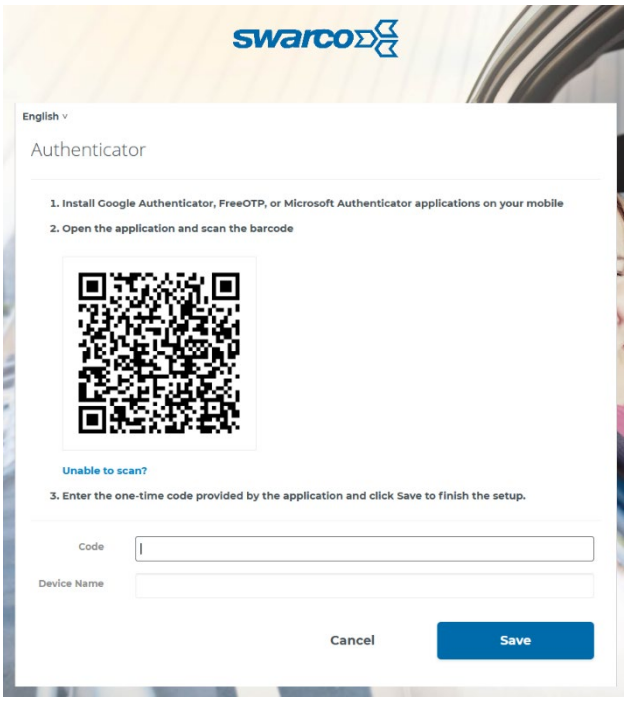
To minimize risks and follow security requirements of legislations (NIS2, KRITIS, etc.), activation of MFA on their MyCity account is mandatory for all users.

To activate two factor authentication for your account, follow these steps:

1. Log in to MyCity with your username and password.
2. Select the user icon on the top right side of the screen, and then select **'MyProfile'.**
3. Select the **'Sessions'-Tab**.
4. Click the [**Activate 2FA**] button in the 'Two Factor Authentication' section. A new **Authenticator** window is opened.



5. Install on your (mobile) device (phone, laptop, etc.) either one of the following:
   - a one-time password (OTP) generating app: Google Authenticator, FreeOTP, or Microsoft Authenticator.
   - use a Password-Manager App supporting one of the mentioned Authenticator Apps (e.g. KeePass, Keeper) directly on your desk/laptop.
6. Open the application and scan the (for MyCity) displayed QR code with your mobile device or with the mask provided by the used Passwort Manager.



If you are unable to scan the displayed QR code with your device/Password Manager, select **Unable to scan?** to add the key manually in your application:

7. Enter the code displayed in the application in the **Code** field. Optionally, you can also add in the **Device** name field the name of the device you are logging in from.
8. Select **Save** to configure your two-factor authentication.