Guideline

MFA:

Multi-Factor Authentication for the End-user

Prepared for ALL CUSTOMERS	**Date:** 17 November 2023
	Prepared by: Robert de Vries

Content

MFA explained

What is Multi-Factor Authentication?

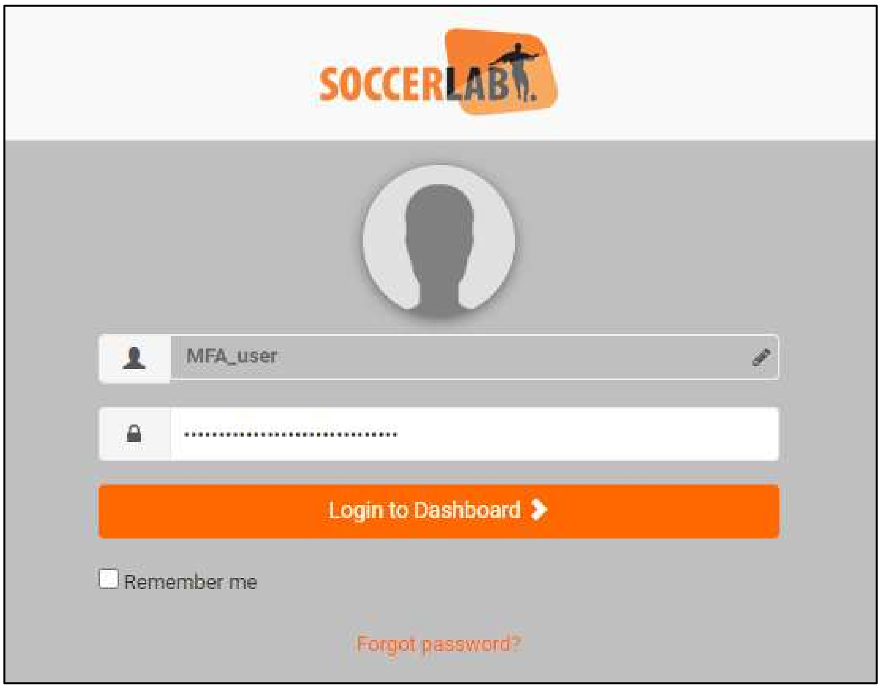
Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.

Why is MFA important?

The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

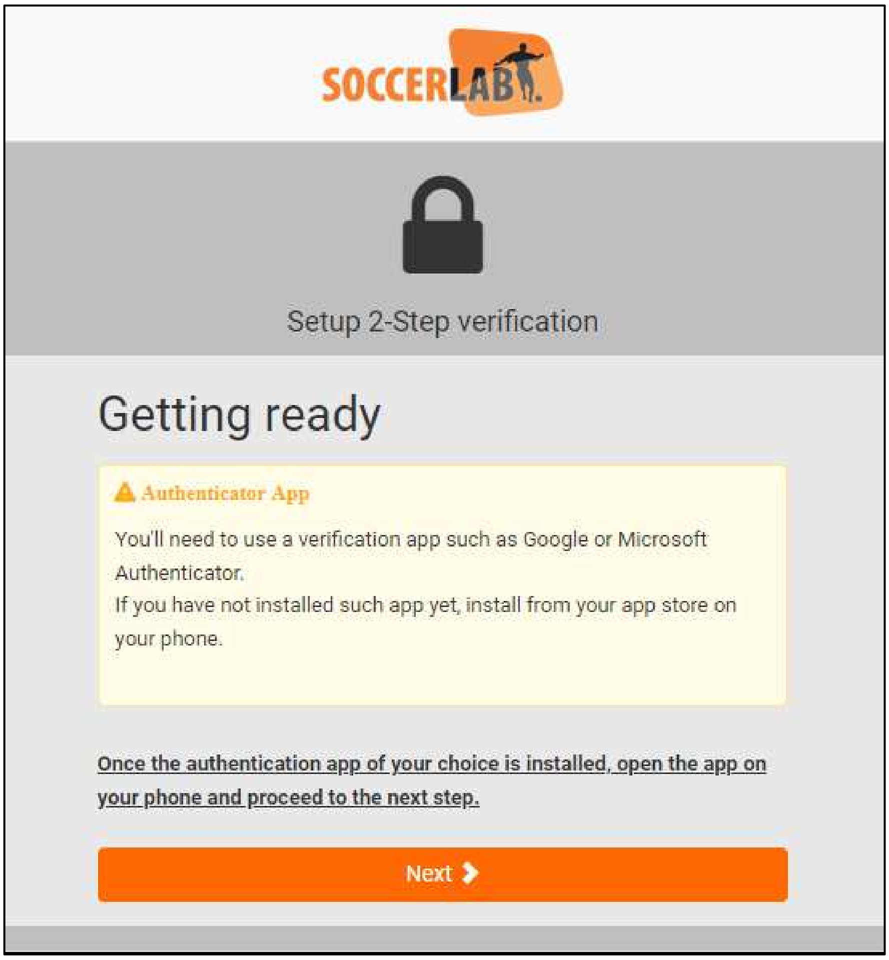
MFA for the end-user

Login, using your normal Username and Password



Users being marked as REQUIRED to use MFA by the Admin.

Now a pop-up shows, explaining to install an Authenticator App



Getting ready

Authenticator App

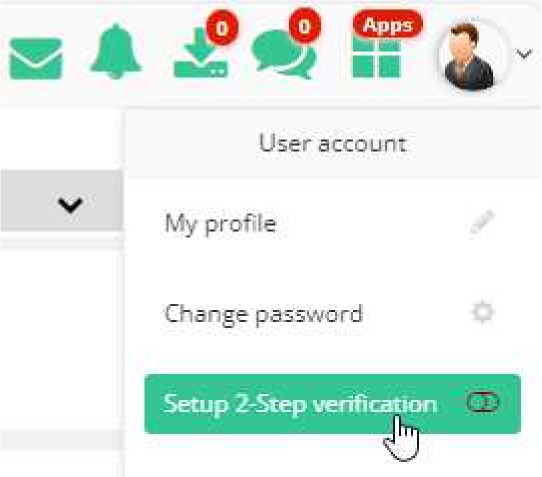
You'll need to use a verification app such as Google or Microsoft Authenticator.
If you have not installed such app yet, install from your app store on your phone.

Once the authentication app of your choice is installed, open the app on your phone and proceed to the next step.

User activates MFA himself/herself

If MFA is not (yet) activated by the Admin, and End-user can also activate MFA after login to the clubbrowsing.

This can be done by setting the "Slider -> Setup 2-Step verification" to TRUE

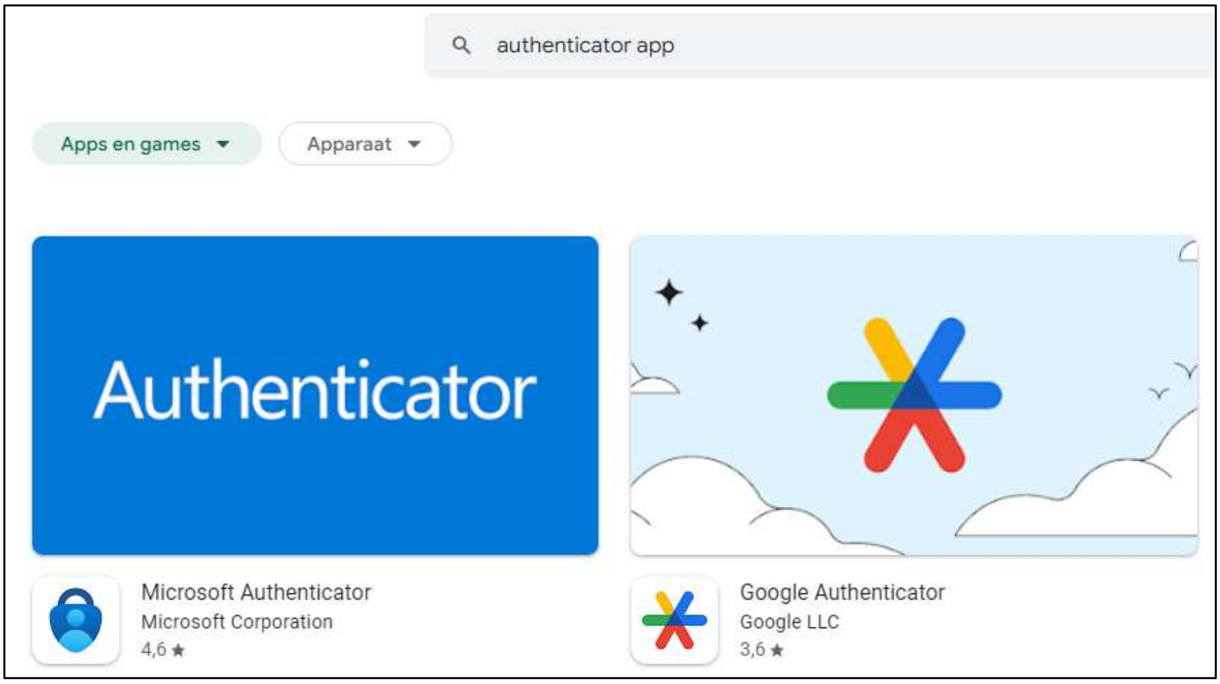


After this the following step need to be followed, after the user logged out from clubbrowsing and logged in again.

Authenticator App on Android

So good examples of a good Authenticator app are; Google Authenticator and Microsoft Authenticator, an end-user dan download it inside the Google Play store.

For IOS



uthenticator App on Apple

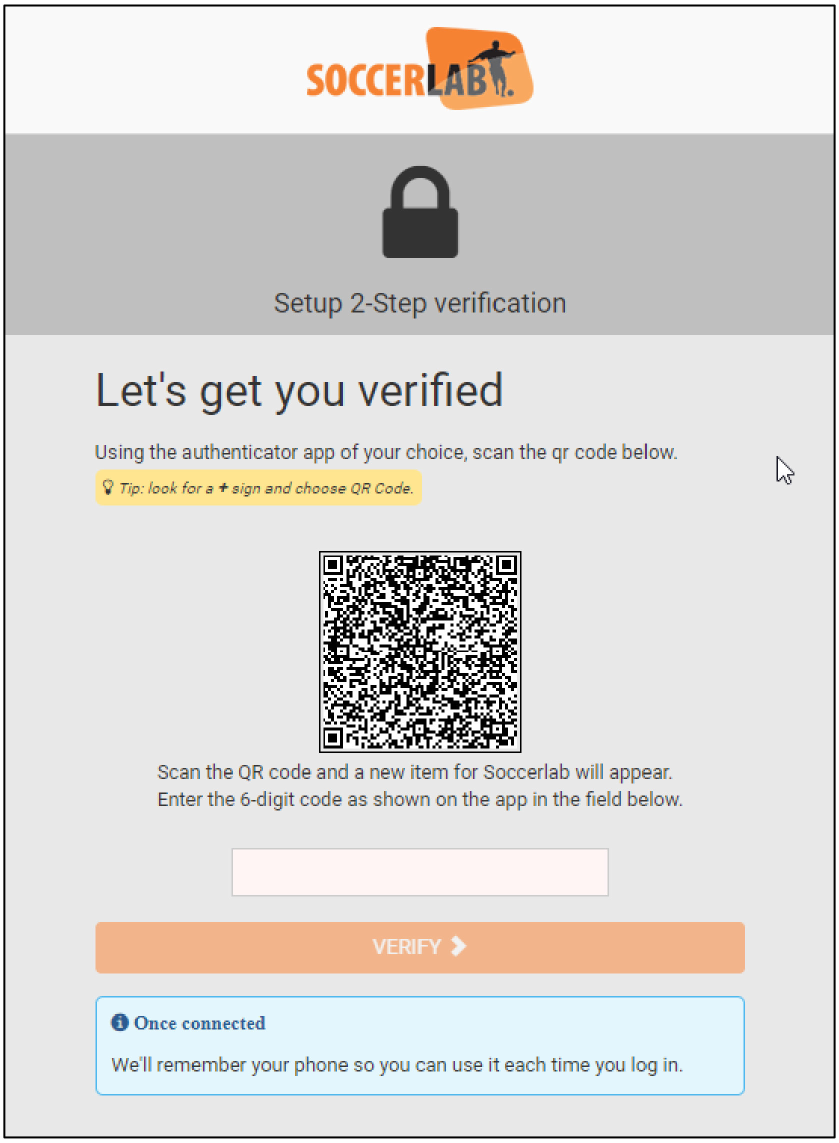
If you have an iPhone, iPad, the easiest way to get into authenticators is by using Apple's built-in tool; **Keychain**, the company's password manager.

Setting up 2FA verification codes directly in this tool is a convenient option to increase the security of your accounts. Codes are encrypted by your iCloud password, and the service supports autofill across Apple devices. That means you can AutoFill your password, then autofill your 2FA code when prompted, speeding through logins.

Again, the most secure solution is to use a separate app, but since iCloud Keychain is protected by both the iCloud password and its own 2FA, and it offers a free and convenient way to set up 2FA for your various accounts.

Scan the code

Once the Authenticator app is installed you can scan the QR code



Setup 2-Step verification

Let's get you verified

Using the authenticator app of your choice, scan the qr code below.

Tip: look for a + sign and choose QR Code.

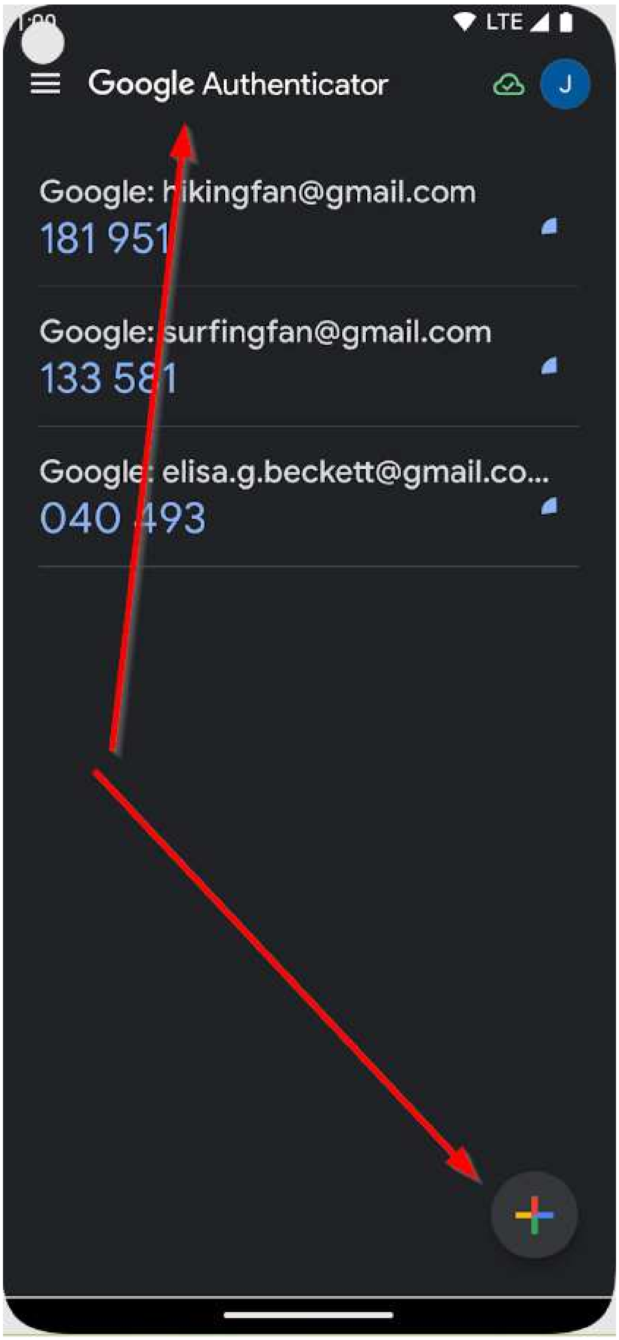
Scan the QR code and a new item for Soccerlab will appear.
Enter the 6-digit code as shown on the app in the field below.

Once connected

We'll remember your phone so you can use it each time you log in.

Google Authenticator app

Example of the Google Authenticator app
Open the app and click the "+" button



1:00

Google Authenticator

Google: hikingfan@gmail.com
181 951

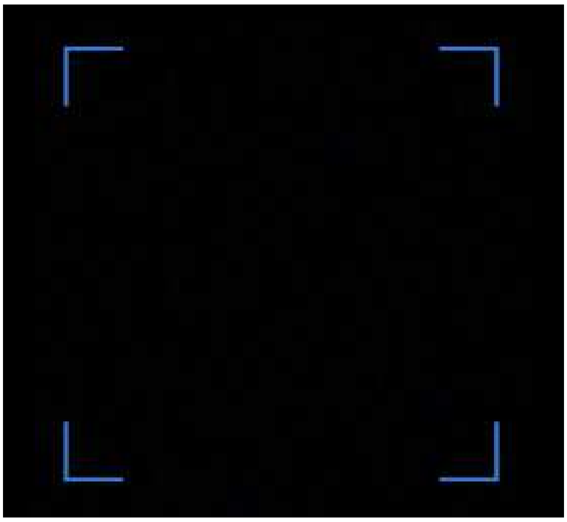
Google: surfingfan@gmail.com
133 581

Google: elisa.g.beckett@gmail.co...
040 493

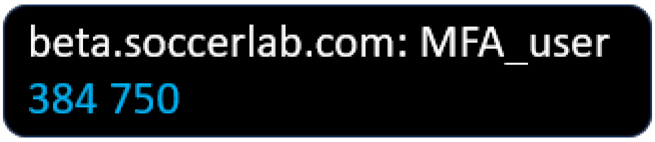
Select: Scan new code

Scan QR code

Focus with the phone on the QR code:



Now a new line will be added to the Authenticator app showing the SoccerLAB application URL and your Username and the code below:

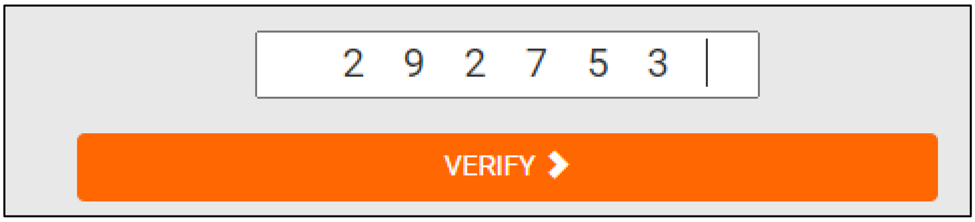


beta.soccerlab.com: MFA_user
384 750

Fill in the code

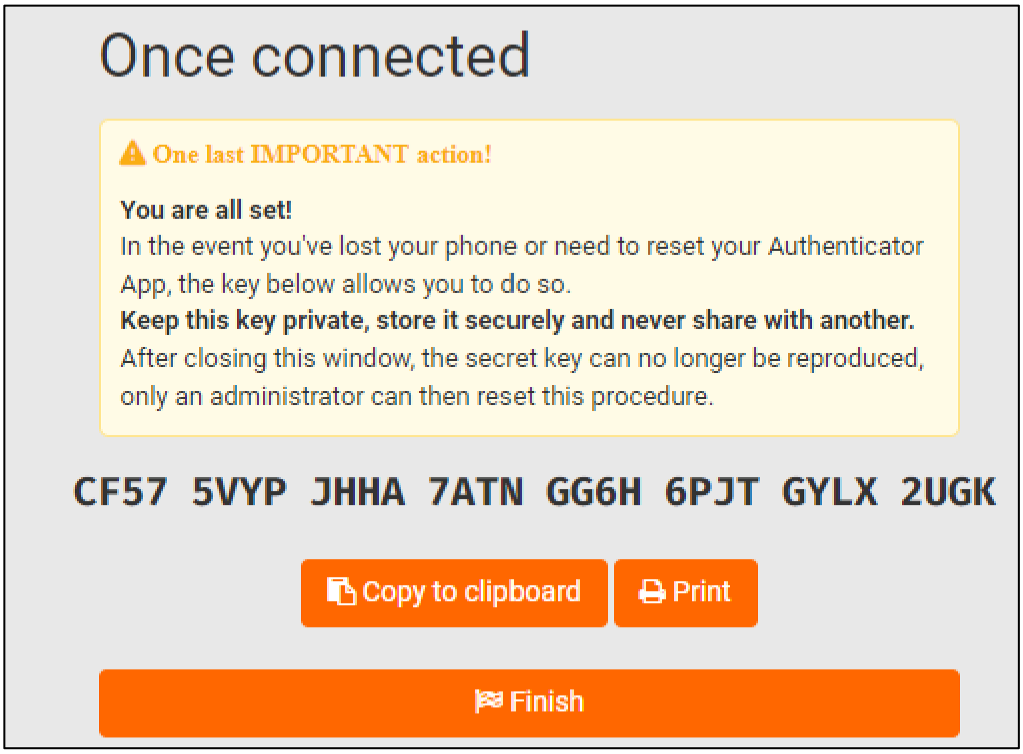
You can use this code to proceed to login.
This code will refresh each "x" seconds

Fill in the code and click Verify



Security key

The first time you use the Authenticator app, a Key will be generated.
Store this key in a safe place, you might need it to restore it after change of phone.



Once connected

⚠ One last IMPORTANT action!

You are all set!
In the event you've lost your phone or need to reset your Authenticator App, the key below allows you to do so.
Keep this key private, store it securely and never share with another.
After closing this window, the secret key can no longer be reproduced, only an administrator can then reset this procedure.

CF57 5VYP JHHA 7ATN GG6H 6PJT GYLX 2UGK

Click Finish to proceed.

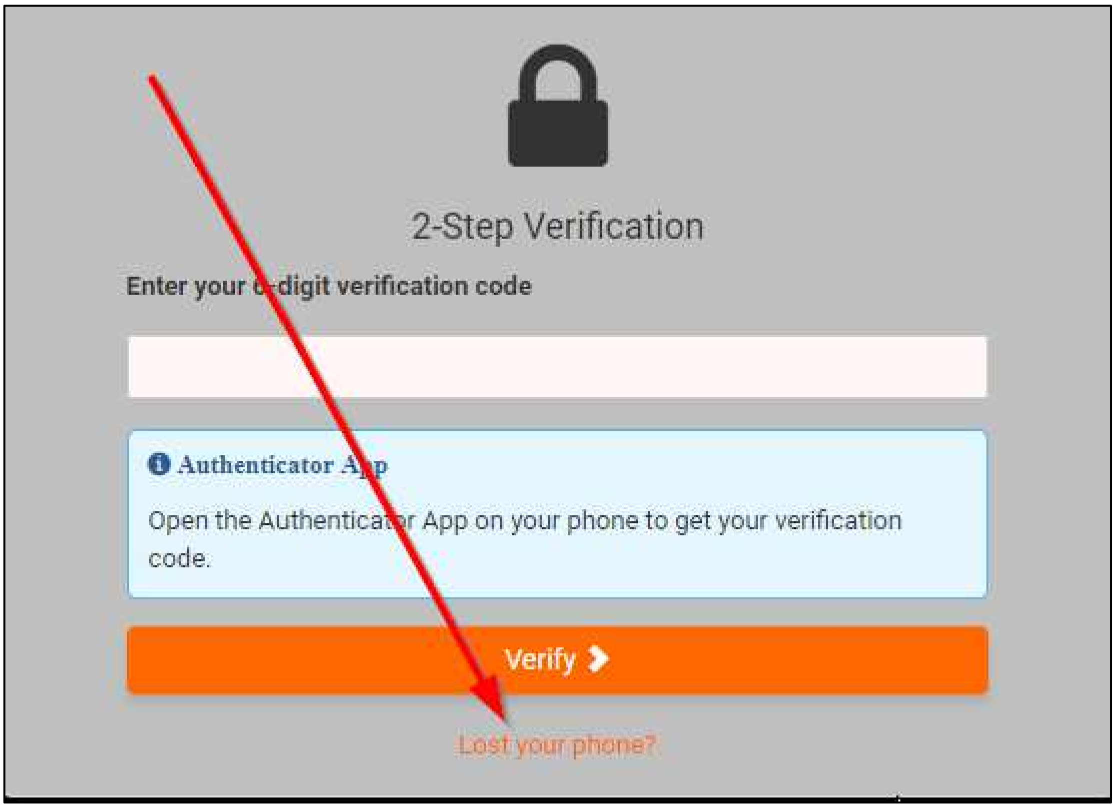
*so this only shows after 1st time!

After successful registration

Next time you login to the application, only the Code is needed from your authenticator app.
Each time you logout to the application, you need to re-enter a 6-diget code coming from the Authenticator app.

Lost or new phone

The security key from the above screenshot can be used when the end-user has a new phone.
Click the

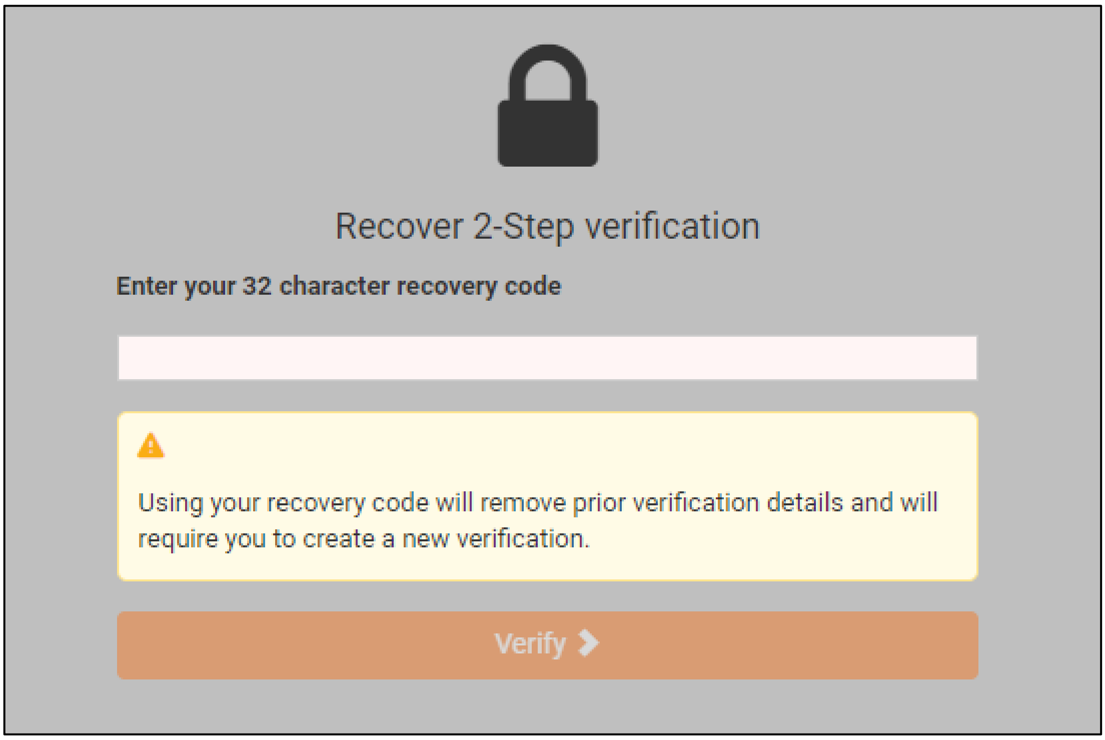


2-Step Verification

Enter your 6-digit verification code

Open the Authenticator App on your phone to get your verification code.

Copy the Security key and click "Verify"



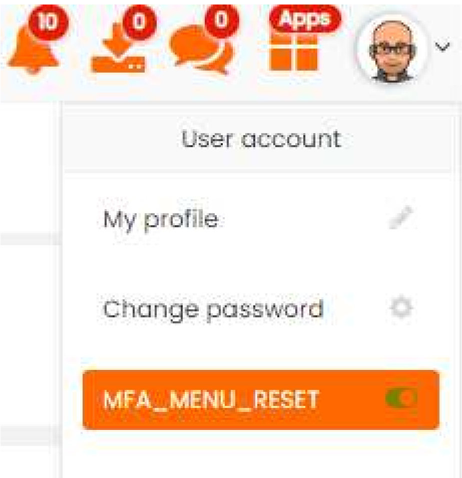
Recover 2-Step verification

Enter your 32 character recovery code

Using your recovery code will remove prior verification details and will require you to create a new verification.

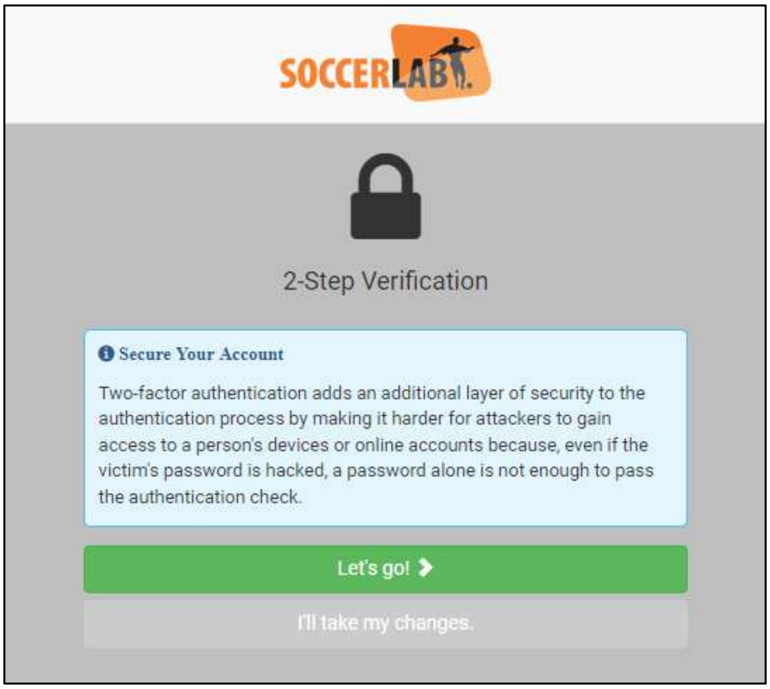
Completely reset MFA

In case you want to completely reset the MFA, you can login to the clubbrowsing and switch off the MFA.
Then you can start the process from scratch.



User NOT having MFA

When the checkbox for "Require 2-step verification" is disabled, the user still gets a warning after login to the application.
So the user can select "I'll take my changes", but we still strongly recommend to start using MFA.



Secure Your Account

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

We keep pushing this information each time the user logs in.

ALWAYS A STEP AHEAD

QuESD NV
Corda Campus
BE, Hasselt

www.soccerlab.com
sales@soccerlab.com

SOCCERLAB