Author : **FLU** date aout 2026

This document is **Public**

Two-Factor Authentication (2FA) Guide

Activation, sign-in, and managing verification methods

Document intended for end users

Purpose of this document

This guide explains in simple terms how two-factor authentication works in the application: first sign-in, receiving codes, choosing your preferred method, and updating your verification details.

1. Why enable 2FA?

Two-factor authentication, also known as 2FA, strengthens the security of your application account.

In addition to your usual password, a verification code may be requested when signing in. This code is sent to the email address or phone number associated with your account.

This additional check helps better protect access to your data, even if your password were to become known to an unauthorized person.

> **Key point**
>
> 2FA adds a security step when signing in, but it remains simple to use: you sign in, you receive a code, then you validate access.

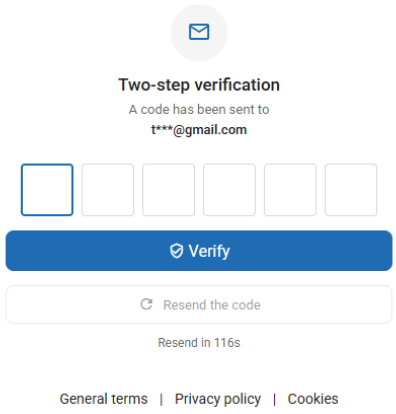
2. Activating 2FA

2FA is activated either by an administrator of your organization or by you, if your organization's configuration allows it.

3. First sign-in after activation

During your first sign-in after 2FA is activated:

1. Sign in with your usual username and password.
2. A verification code is sent by email, the default method used for the first sign-in.
3. Enter the code you received on the screen provided for this purpose.
4. Your sign-in is then validated.



Example of the 2FA code verification screen.

4. Subsequent sign-ins

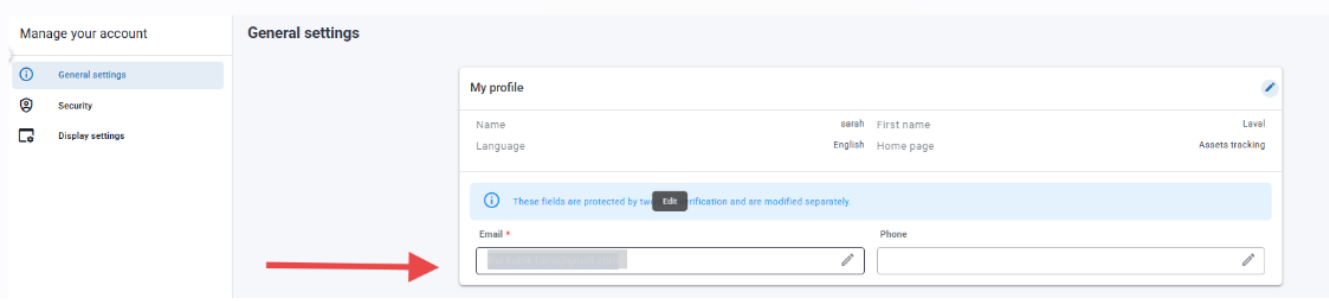
After a successful authentication, the application can remember the validation for 10 days.

After this period, a new verification code may be requested. If several methods are configured, the preferred method will be selected by default, but another active method can be used if needed.

5. Managing your verification details

The details used to receive codes can be viewed and updated from the user settings.

This information is available on the General Settings screen.

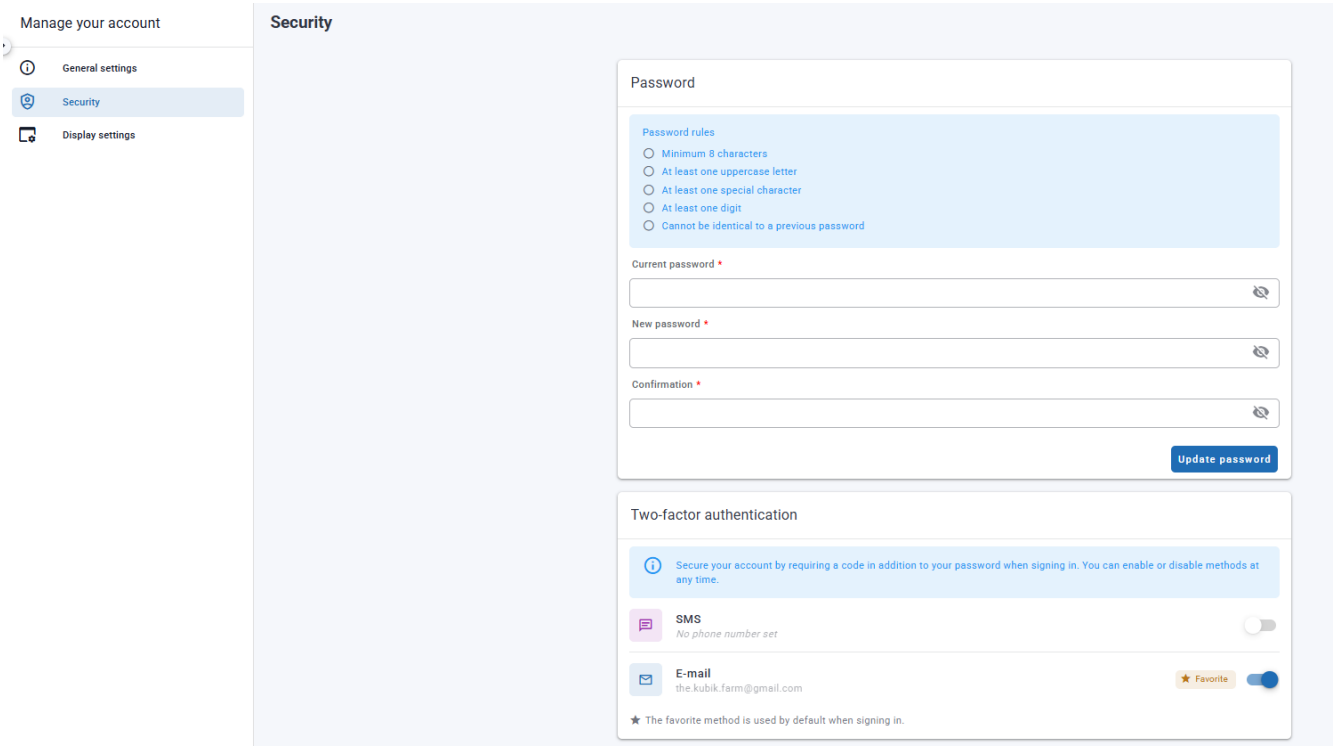


Example of accessing user profile information.

6. Choosing your preferred verification method

The default method is configured from the Security screen in the user settings.

Depending on the information provided on the account, several methods may be available, for example email or phone.

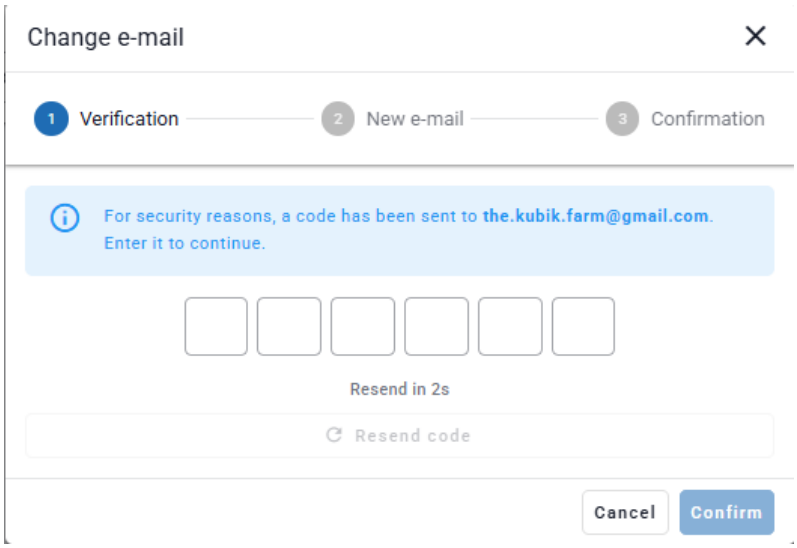


Example of the security methods configuration screen.

7. Changing an email address or phone number

To protect your account, any change to an email address or phone number must be confirmed.

When a verification method already exists, a code will be sent to the old method. Once the new value has been entered, a code is sent to the new address or number to confirm the change.



Example of updating a verification detail.

8. Adding or disabling a method

To activate an authentication method, start by entering the necessary information in your user profile (for example, a phone number or an email address). Once this information is saved, turn on the **toggle switch** for the desired method, then enter the verification code you receive to confirm activation.

To disable an authentication method, simply turn off the **toggle switch** next to the relevant method. That method will then no longer be available for two-factor authentication.

> **Good to know**
>
> At least one authentication method must remain active to keep your account secure.

9. Quick reference

Situation	What to do
First sign-in after activation	Sign in as usual, then enter the code received by email or phone.
Code requested after a few days	Enter the code received via your preferred verification method.
Phone number or email to update	Update the information in your profile, then confirm the change with the code received.
Preferred method to change	Go to the Security screen and select the desired method.
Method to remove	Click to turn off the toggle switch.

> **Need help?**
>
> If you have any difficulty signing in, receiving a code, or changing a verification method, contact you're the helpdesh.