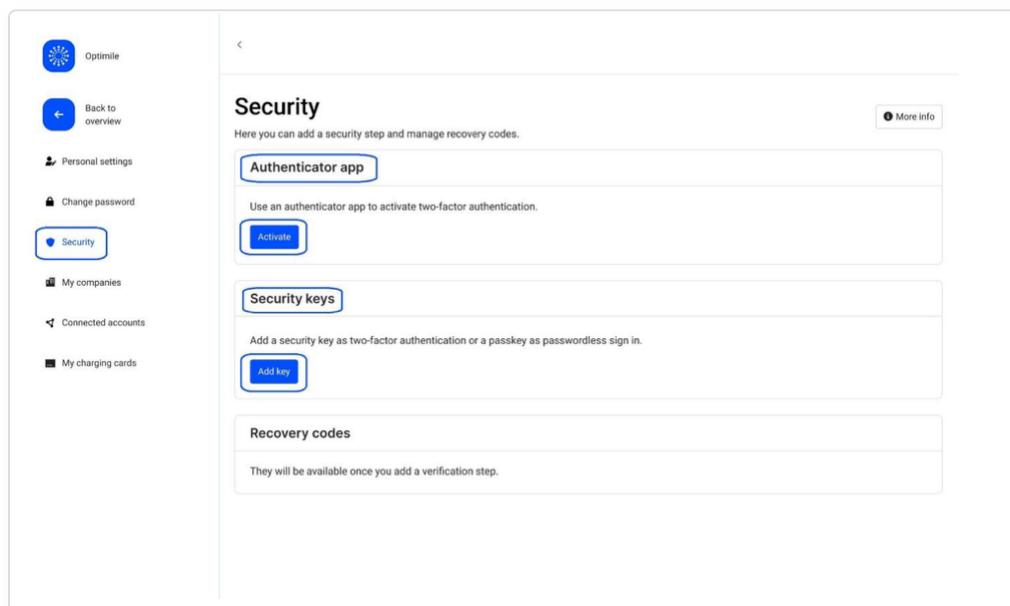


Activating MFA on your account

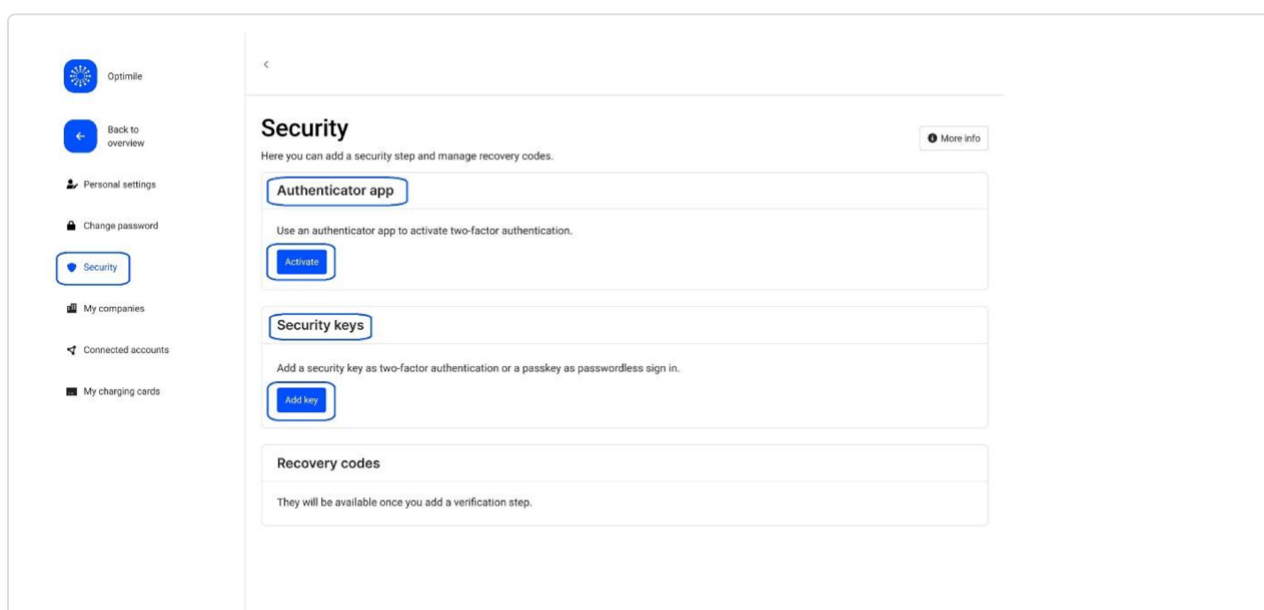
Before activating MFA you will need to ensure your basic personal information is fully and accurately completed under **Personal Settings**. This information may be required to verify your identity during account recovery if ever you lose access to your account.

Log in to your account and go to **Personal Settings > Security**. Choose your preferred authentication method:

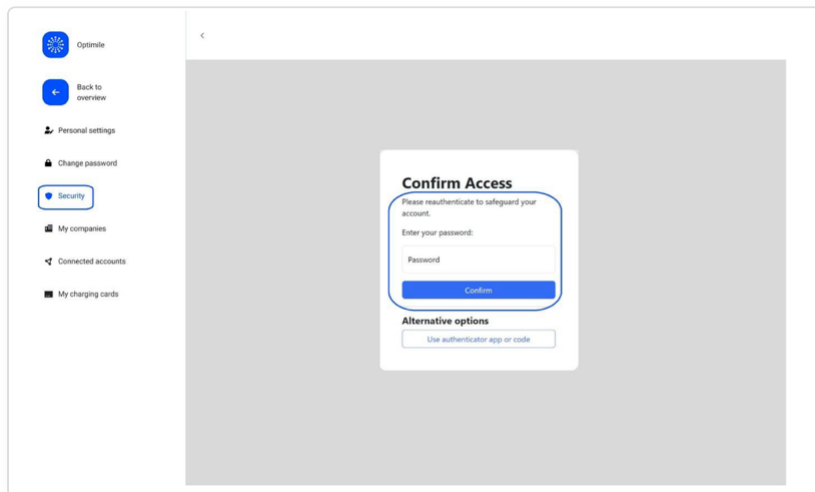


Option 1: Authenticator app

1. Click **Activate** below the Authenticator app option.



2. Re-authenticate by entering your password.



3. After successfully confirming access, **scan the QR code** with your authenticator app.

Open your authenticator app (e.g. Google Authenticator, Microsoft Authenticator) to proceed.

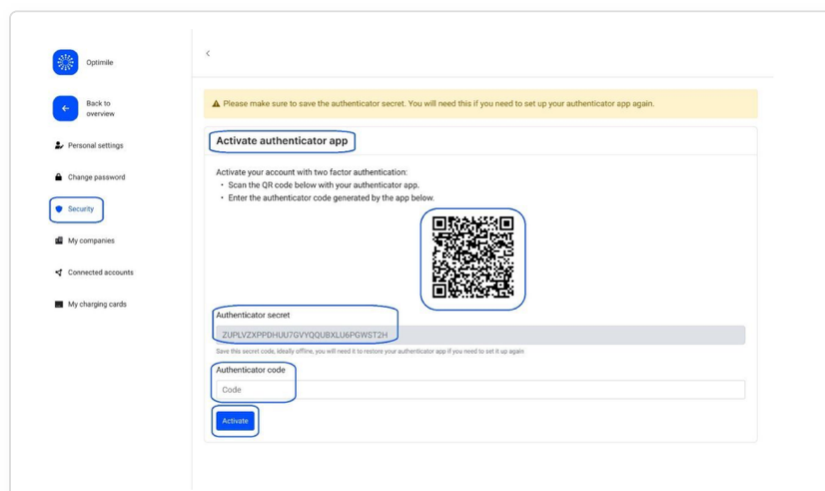
4. **Save the authenticator secret code**, preferably somewhere offline. You may need this if ever you need to set up your authenticator application again.

5. **Enter the generated code** from the app in the field labeled *Authenticator code*.

6. Click **Activate** to complete setup.

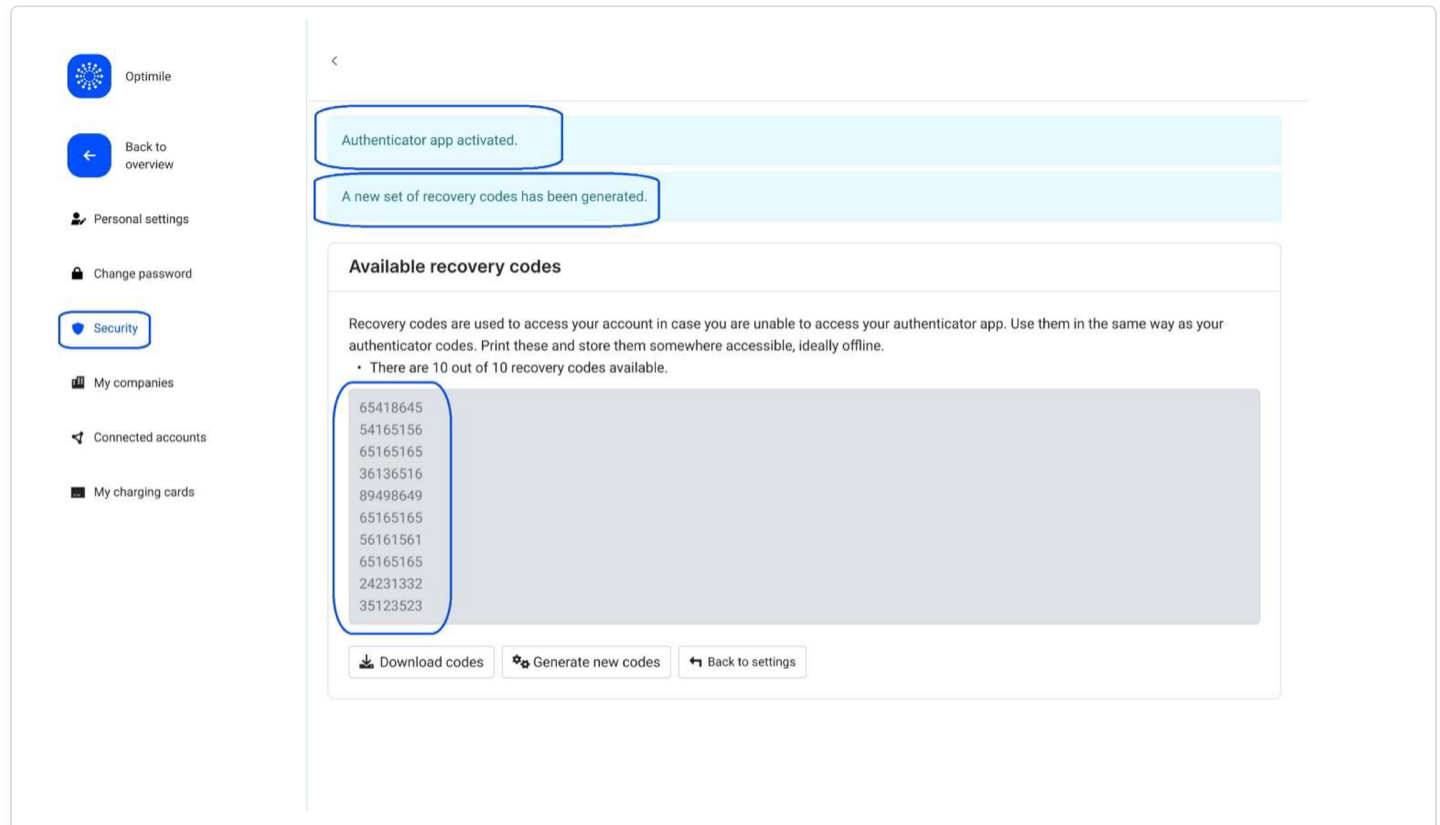
⚠ **CRITICAL: Save Your Recovery Codes Securely**

- **Store Externally:** You must save these recovery codes in a secure location separate from your current device (e.g., printed on paper, saved on an offline USB drive, or stored in a secure password manager). Storing them only on your phone or computer will result in lost account access if your device is damaged or misplaced.
- **Single-Use Only:** Each recovery code functions only once. Once used, it becomes invalid and cannot be reused.



Once successfully activated:

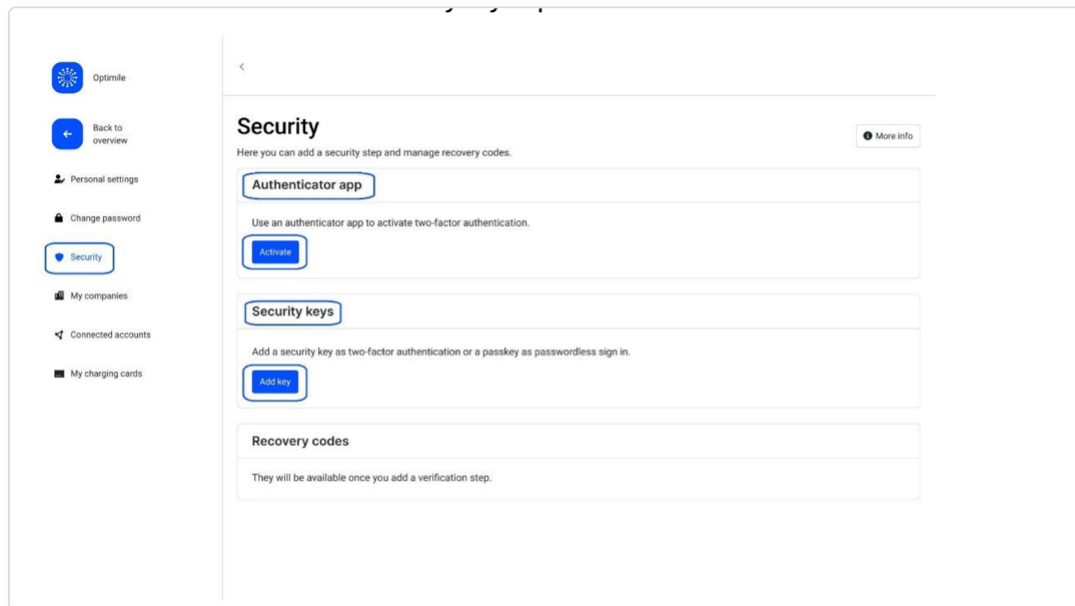
- A confirmation message will be displayed.
- Recovery codes will be generated automatically. Please download these and store them somewhere accessible.



Note: After enabling 2FA, the login process remains the same. Users will first enter their email and password, then be prompted to input a code from the authenticator app or a recovery code.

Option 2: Security keys

1. Click **Add** below the Security keys option.



Security

Here you can add a security step and manage recovery codes.

Authenticator app

Use an authenticator app to activate two-factor authentication.

Activate

Security keys

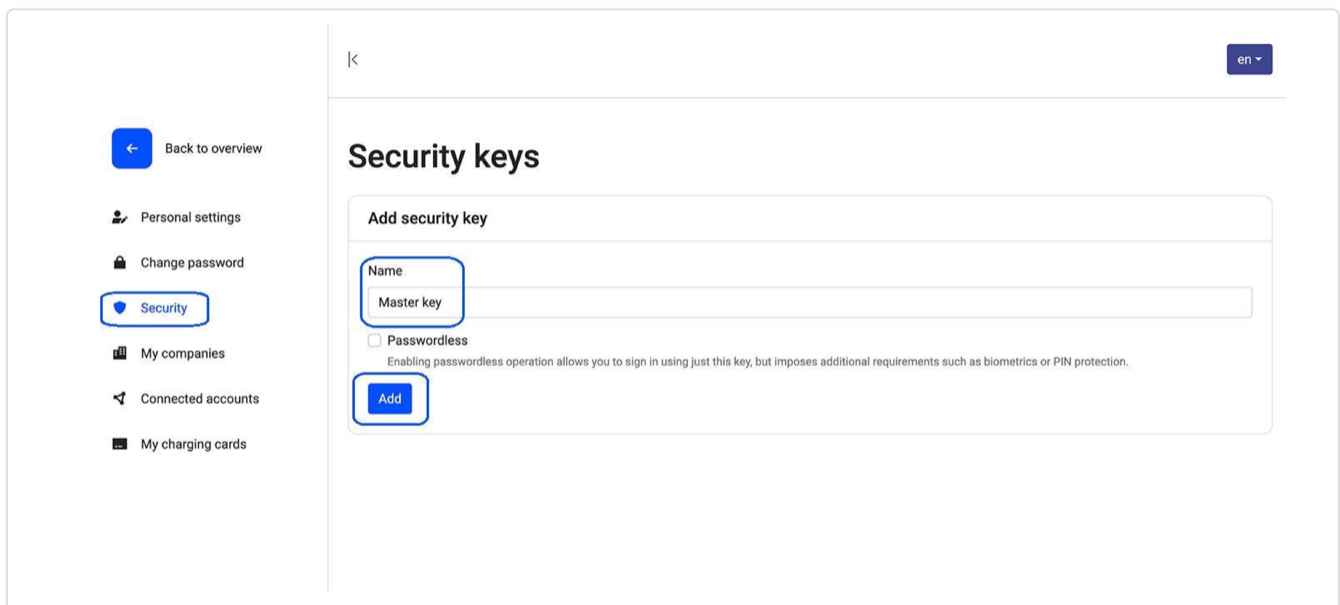
Add a security key as two-factor authentication or a passkey as passwordless sign in.

Add key

Recovery codes

They will be available once you add a verification step.

2. Enter a **name** of your choice for your security key (e.g. 'Master') - make sure it's something clear. This key will be used as part of your login process.



Security keys

Add security key

Name

Master key

☐ Passwordless

Enabling passwordless operation allows you to sign in using just this key, but imposes additional requirements such as biometrics or PIN protection.

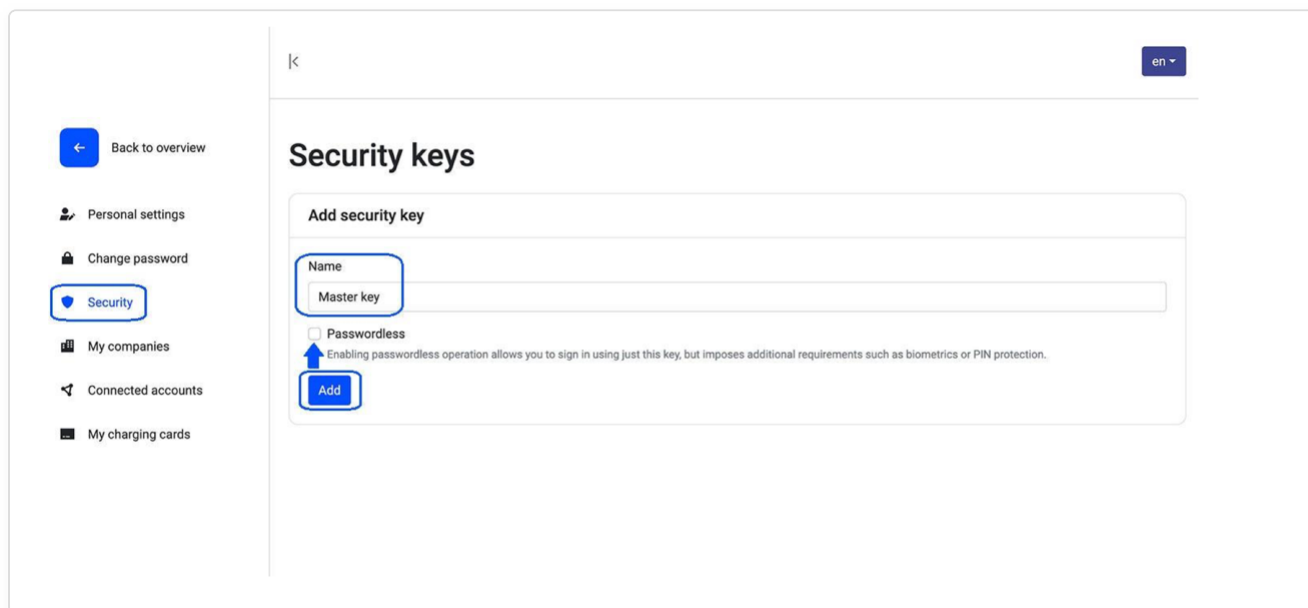
Add

3. **Preferred usage:** Decide how you want to use the security key:

Option A: Passwordless Login (Passkey)

Select this option to log in without using email or password each time.

- Tick the **Passwordless Login** checkbox.



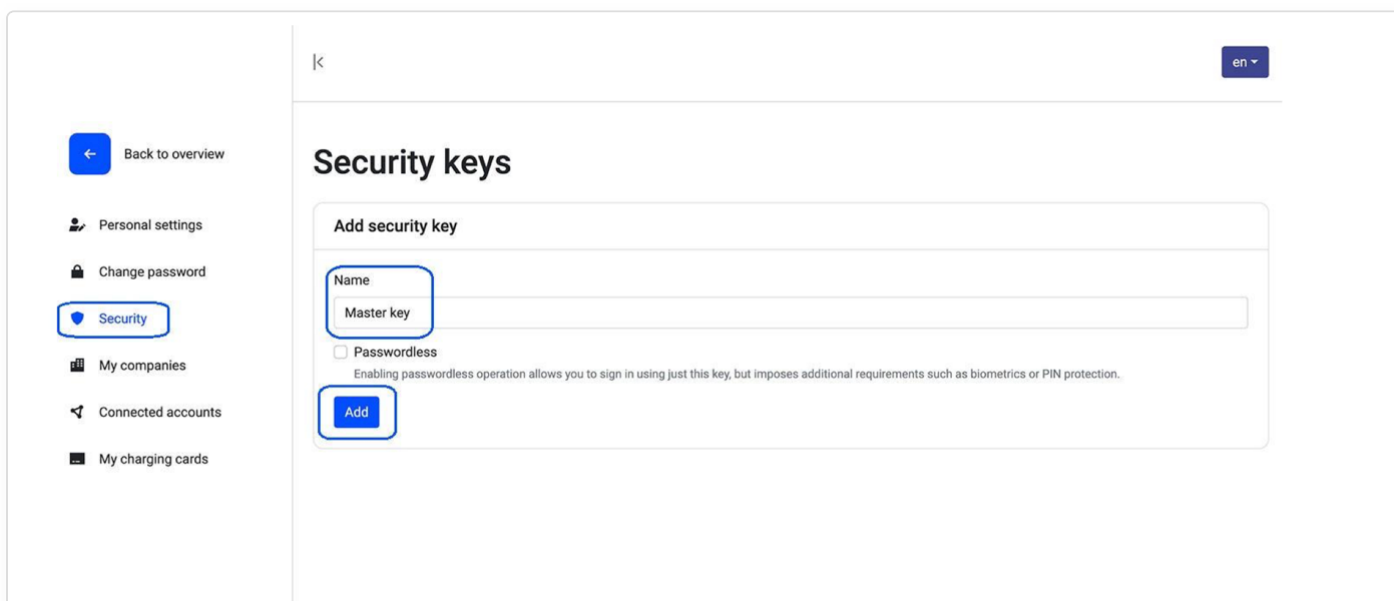
The screenshot shows the 'Security keys' settings page. On the left, a sidebar contains links: 'Back to overview', 'Personal settings', 'Change password', 'Security' (highlighted), 'My companies', 'Connected accounts', and 'My charging cards'. The main content area is titled 'Security keys' and contains an 'Add security key' form. The form has a 'Name' field with 'Master key' entered, a 'Passwordless' checkbox which is checked, and an 'Add' button. A blue arrow points to the 'Add' button.

During login, choose **Sign in with passkey** and authenticate using your device's built-in method (like PIN or fingerprint).

Option B: Two-factor authentication (Security key with password)

Select this option if you want to add an extra layer of security while still using your email and password.

- Leave the **Passwordless Login** option unchecked.



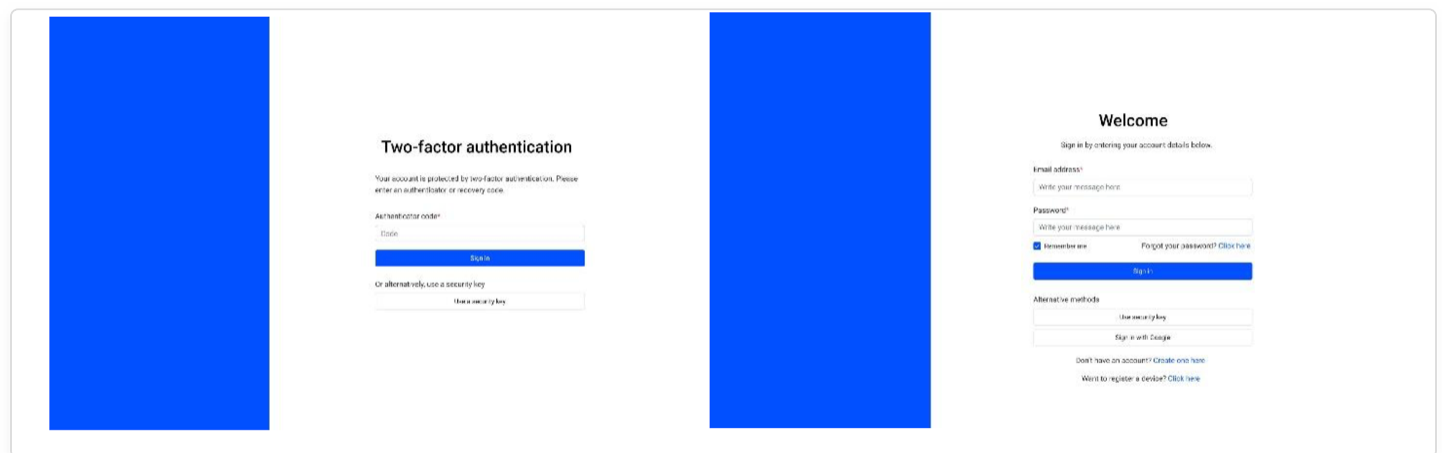
The screenshot shows the 'Security keys' settings page. On the left, a sidebar contains links: 'Back to overview', 'Personal settings', 'Change password', 'Security' (highlighted), 'My companies', 'Connected accounts', and 'My charging cards'. The main content area is titled 'Security keys' and contains an 'Add security key' form. The form has a 'Name' field with 'Master key' entered, a 'Passwordless' checkbox which is unchecked, and an 'Add' button.

During login:

- Enter your email and password.
- You'll be prompted to authenticate using your security key.
- Your device will then ask for your normal verification method (like PIN, fingerprint, etc.).

! NOTE: Device-Bound Authentication

This method is bound to your specific device. You can use verification methods like your PIN or fingerprint on the current device, but if you switch to a new or different device, this authentication method will no longer work.



Recovery Codes

Once you've activated either the authenticator app or a security key, recovery codes will be provided.

- These codes allow access to your account if you lose access to your MFA method.
- Use them in place of an authenticator code or security key during login.
- Print and store your recovery codes in a safe, accessible location.

Important: If you lose access to your MFA method and don't have your recovery codes, you'll need to contact your customer or platform admin for assistance.