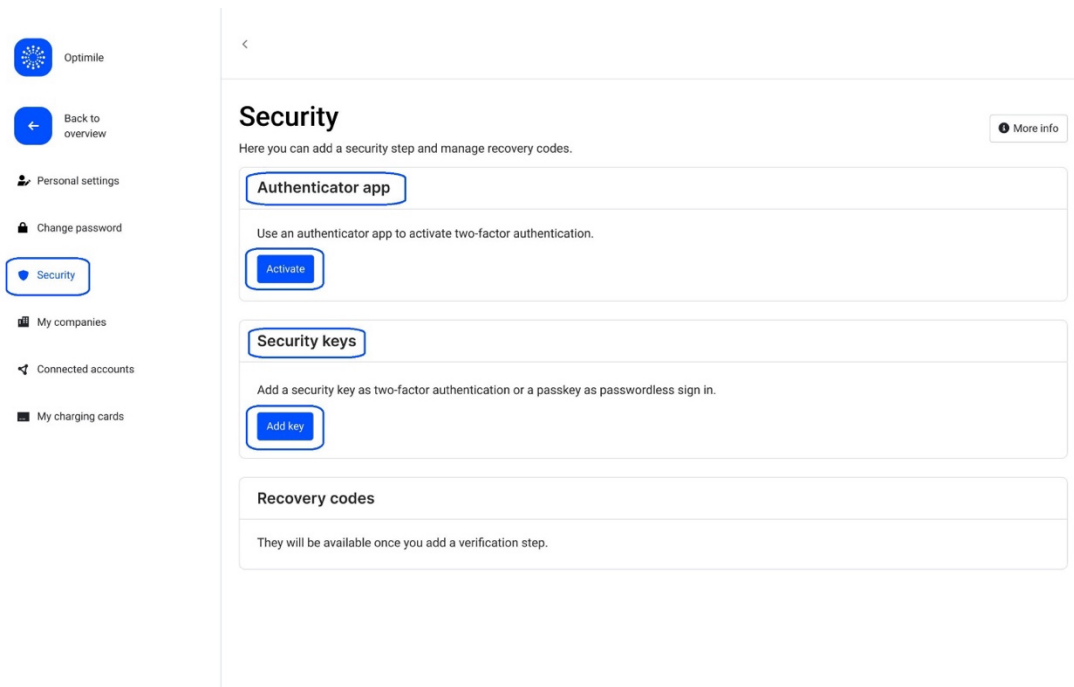




For users: Activating MFA on your account:

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:



 Optimize

 Back to overview

 Personal settings


 Change password

Security

 My companies

 Connected accounts

 My charging cards



Security

More info

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.

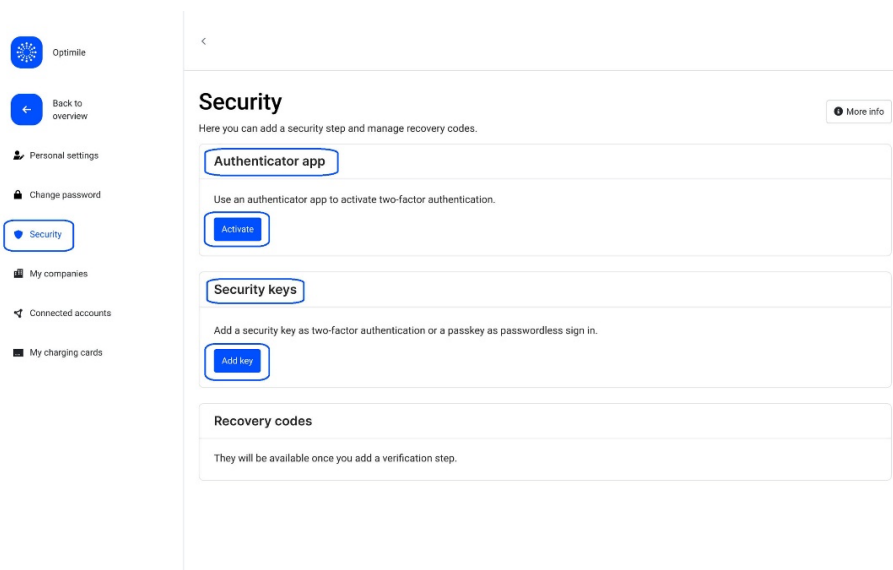
Add key


Recovery codes


They will be available once you add a verification step.

Option 1: Authenticator app

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



 Optimize

 Back to overview

 Personal settings


 Change password

Security

 My companies

 Connected accounts

 My charging cards



Security

More info

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

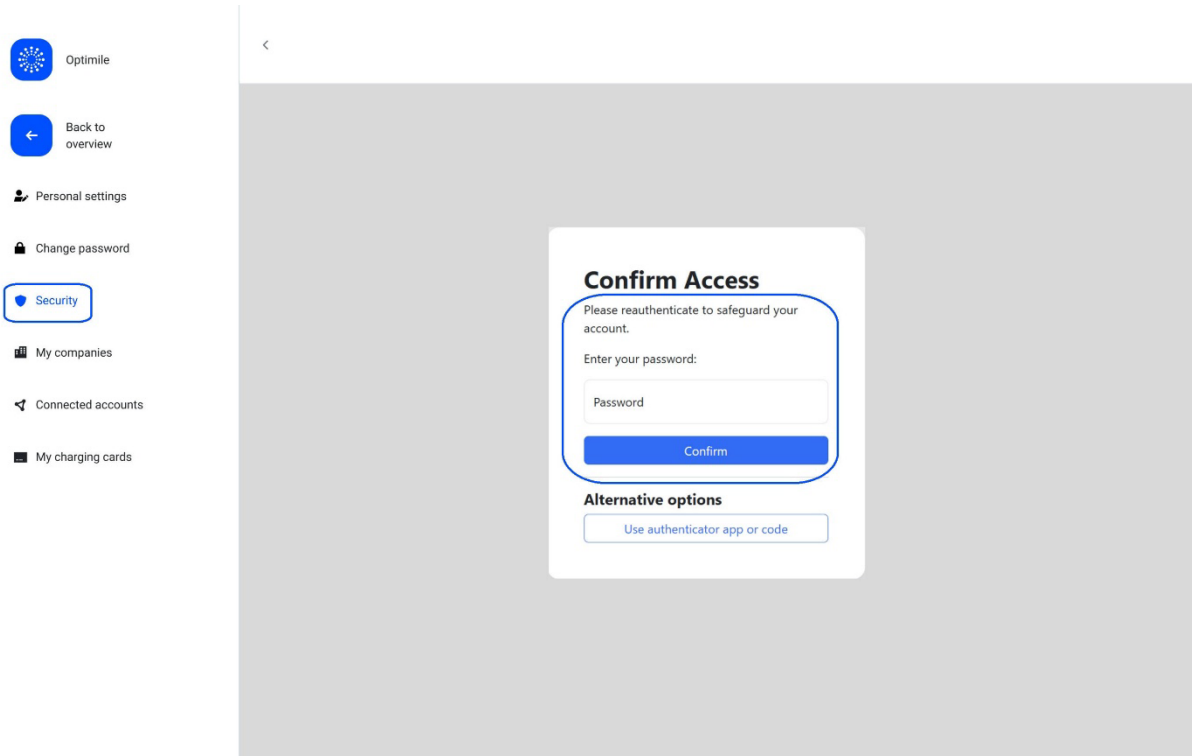
Add a security key as two-factor authentication or a passkey as passwordless sign in.

Add key

Recovery codes

They will be available once you add a verification step.

2. 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.


- Optimile
- Back to overview
- Personal settings
- Change password
- Security**
- My companies
- Connected accounts
- My charging cards

Please make sure to save the authenticator secret. You will need this if you need to set up your authenticator app again.

Activate authenticator app

Activate your account with two factor authentication:

- Scan the QR code below with your authenticator app.
- Enter the authenticator code generated by the app below.



Authenticator secret

ZUPLVZXPPDHUU7GVYQQUBXLU6PGWST2H

Save this secret code, ideally offline, you will need it to restore your authenticator app if you need to set it up again

Authenticator code

Code

Activate

Once successfully activated:

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

- Optimile
- Back to overview
- Personal settings
- Change password
- Security**
- My companies
- Connected accounts
- My charging cards

Authenticator app activated.

A new set of recovery codes has been generated.

Available recovery codes

Recovery codes are used to access your account in case you are unable to access your authenticator app. Use them in the same way as your authenticator codes. Print these and store them somewhere accessible, ideally offline.

- There are 10 out of 10 recovery codes available.

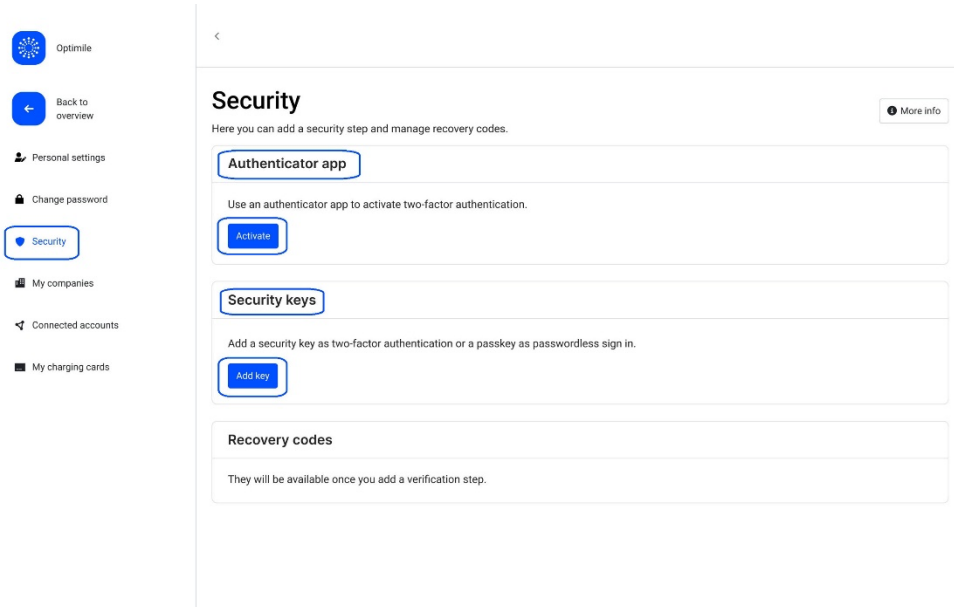
65418645
54165156
65165165
36136516
89498649
65165165
56161561
65165165
24231332
35123523

Download codes Generate new codes Back to settings

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.

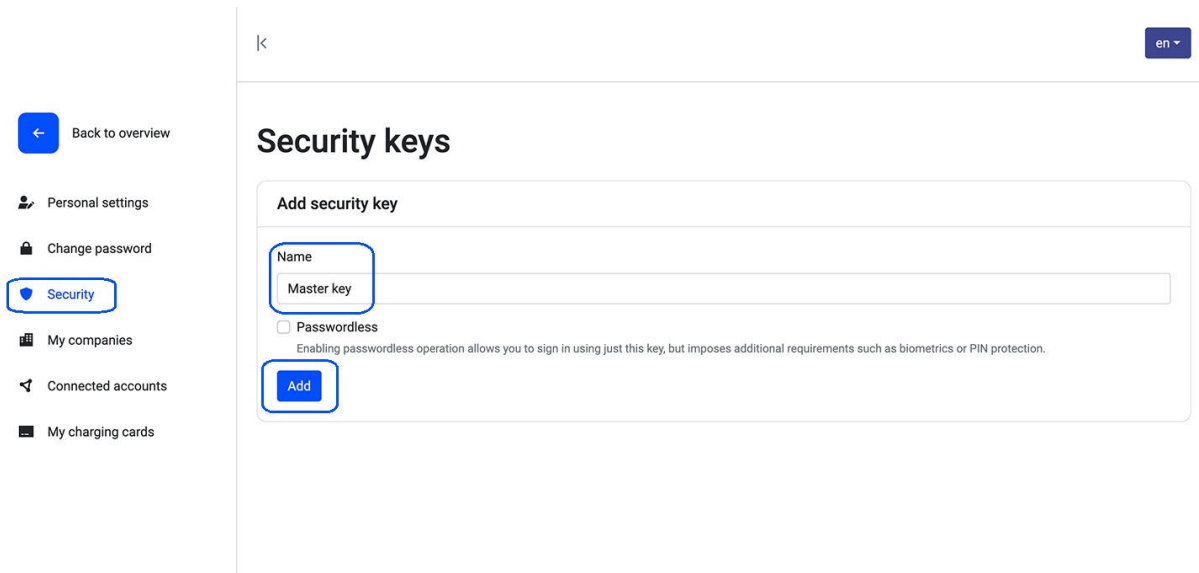
Option 2: Security keys

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



The screenshot shows the 'Security' settings page. On the left is a sidebar with navigation options: Optimize, Back to overview, Personal settings, Change password, Security (highlighted), My companies, Connected accounts, and My charging cards. The main content area is titled 'Security' and includes a sub-header 'Here you can add a security step and manage recovery codes.' Below this are three sections: 'Authenticator app' with an 'Activate' button, 'Security keys' with an 'Add key' button, and 'Recovery codes' with a note that they will be available once a verification step is added.

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.

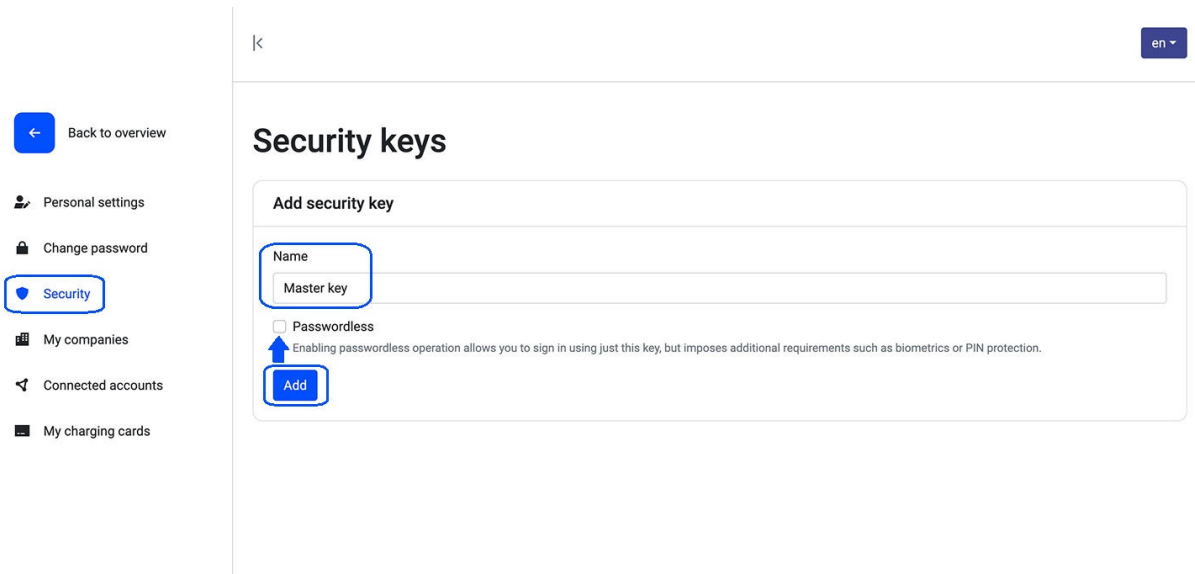


The screenshot shows the 'Security keys' page. The sidebar is the same as in the previous screenshot, but 'Back to overview' is now highlighted. The main content area is titled 'Security keys' and features a form titled 'Add security key'. The form has a 'Name' field with the text 'Master key' entered, a 'Passwordless' checkbox which is unchecked, and an 'Add' button. A note below the checkbox states: 'Enabling passwordless operation allows you to sign in using just this key, but imposes additional requirements such as biometrics or PIN protection.'

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.

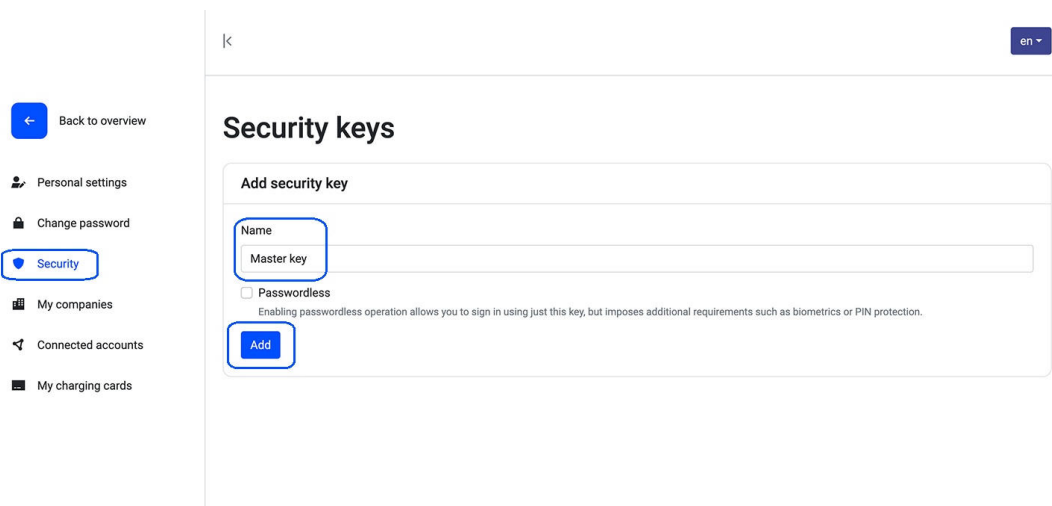


The screenshot shows the 'Security keys' settings page. On the left is a sidebar with navigation links: 'Back to overview', 'Personal settings', 'Change password', 'Security' (highlighted), 'My companies', 'Connected accounts', and 'My charging cards'. The main content area is titled 'Security keys' and contains a form to 'Add security key'. The form has a 'Name' field with 'Master key' entered. Below the name field is a checkbox labeled 'Passwordless', which is checked. A blue arrow points to the checkbox with the text: 'Enabling passwordless operation allows you to sign in using just this key, but imposes additional requirements such as biometrics or PIN protection.' At the bottom of the form is a blue 'Add' button.

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

4. **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.



This screenshot is identical to the one above, showing the 'Security keys' settings page. However, in this scenario, the 'Passwordless' checkbox is unchecked. The rest of the interface, including the sidebar and the 'Add' button, remains the same.

- 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.).



Two-factor authentication

Your account is protected by two-factor authentication. Please enter an authenticator or recovery code.

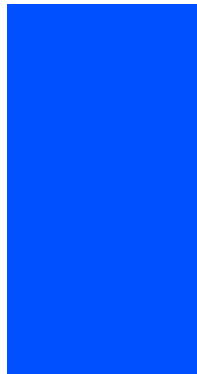
Authenticator code*

Code

Sign in

Or alternatively, use a security key

Use a security key



Welcome

Sign in by entering your account details below.

Email address*

Write your message here

Password*

Write your message here

☒ Remember me

Forgot your password? Click here

Sign in

Alternative methods

Use security key

Sign in with Google

Don't have an account? Create one here

Want to register a device? Click here

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.