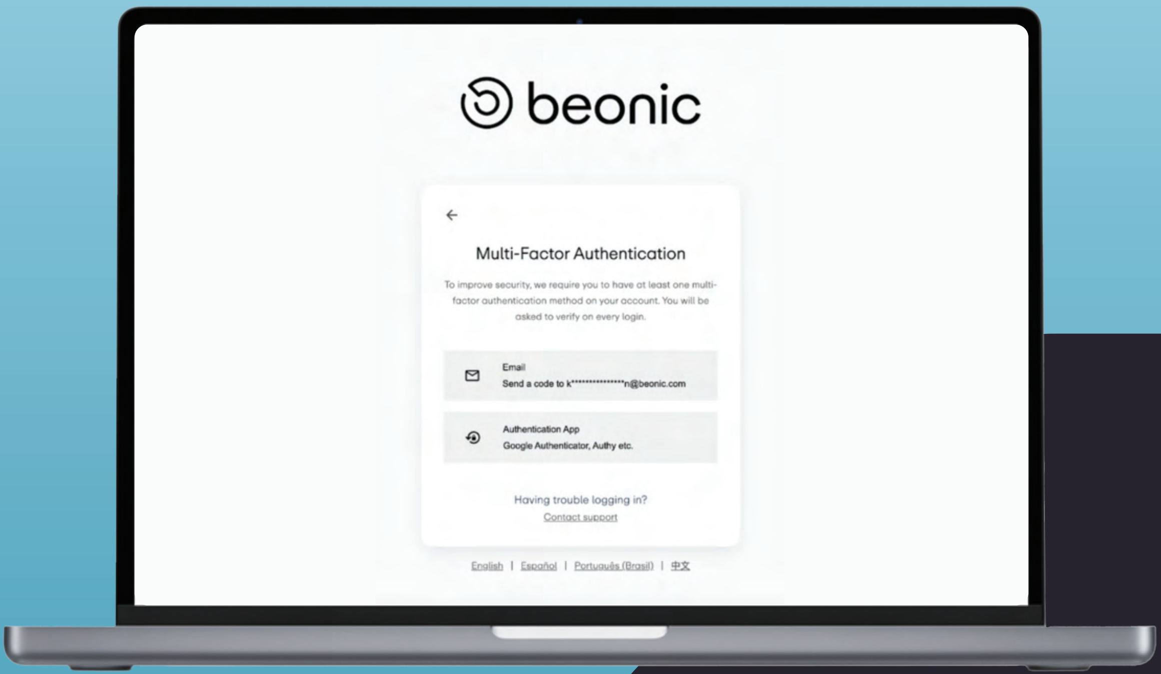
beonic

Multi-Factor Authentication User Guide



beonic

←

Multi-Factor Authentication

To improve security, we require you to have at least one multi-factor authentication method on your account. You will be asked to verify on every login.

Email
Send a code to k***************n@beonic.com

Authentication App
Google Authenticator, Authy etc.

Having trouble logging in?
Contact support

English | Español | Português (Brasil) | 中文

Summary

Multi-Factor Authentication (MFA) is a security feature that adds an extra layer of protection to user accounts by requiring multiple forms of verification during login. This helps prevent unauthorised access, even if a password is compromised.

This guide will walk you through the process of setting up MFA on your account.

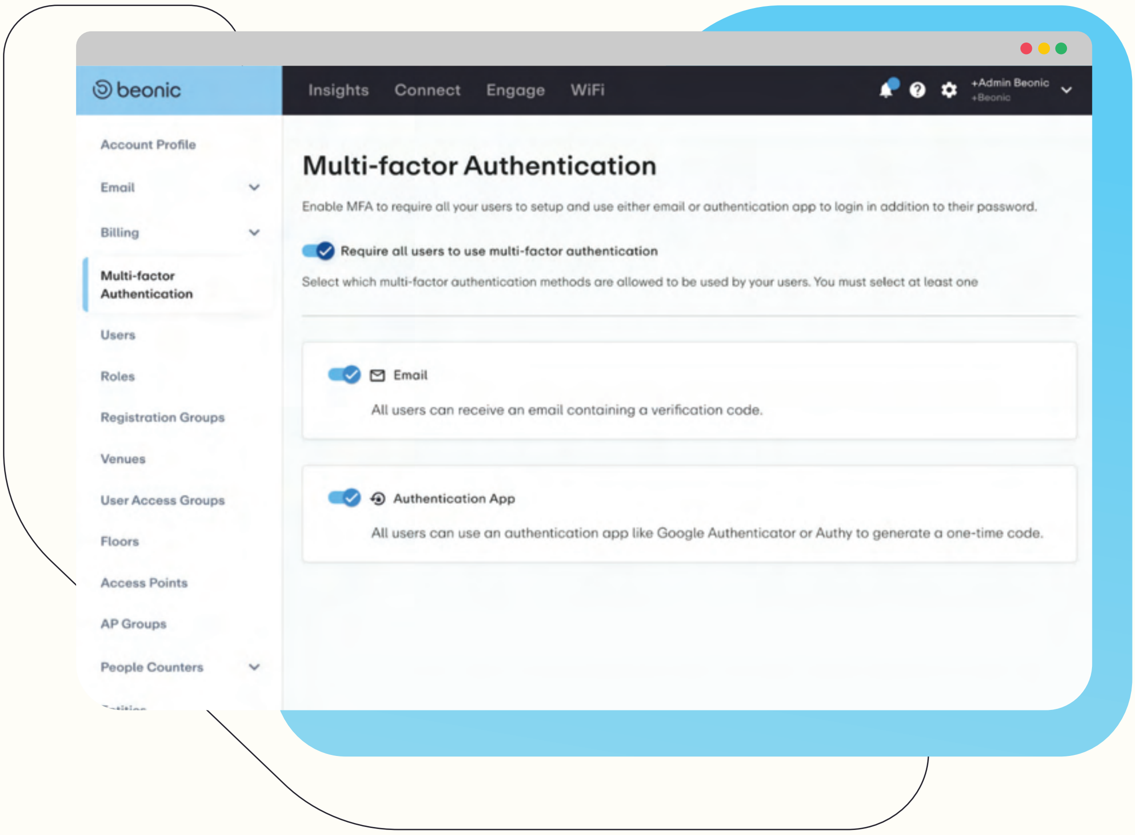
How it works

With MFA enabled, users will need to verify their identity using an additional authentication method, such as a one-time passcode (OTP) sent to their email address or an authenticator app. This will be required when:

- Logging in to the platform
- Changing password
- “Forgot your password?”

For Account Admins - Managing MFA for all users on an account

1. Log in to your Beonic account.
2. Navigate to the Multi-Factor Authentication settings under the Account Settings menu.
3. To enforce MFA for all users on your account, toggle on “**Require all users to use Multi-Factor Authentication”.**



Multi-factor Authentication

Enable MFA to require all your users to setup and use either email or authentication app to login in addition to their password.

☑ Require all users to use multi-factor authentication

Select which multi-factor authentication methods are allowed to be used by your users. You must select at least one

☑ Email

All users can receive an email containing a verification code.

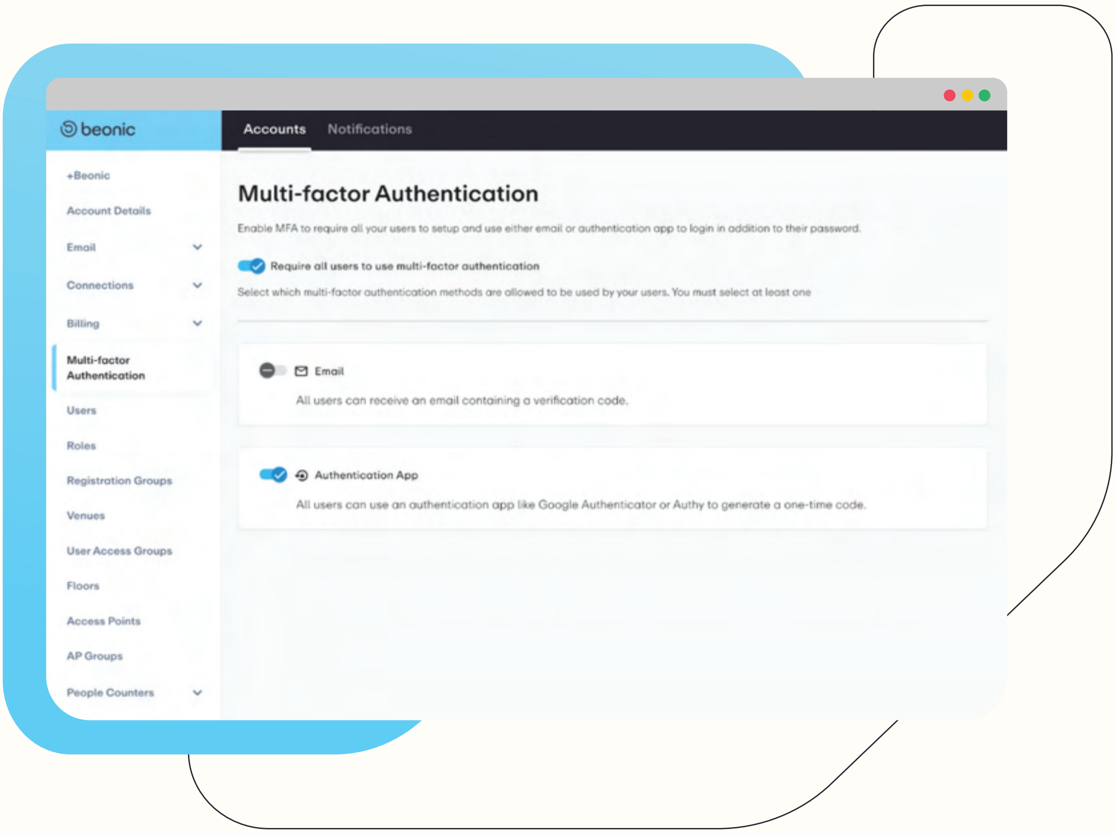
☑ Authentication App

All users can use an authentication app like Google Authenticator or Authy to generate a one-time code.

4. Choose the preferred authentication method(s) for all users:

- Email-based OTP
- Authenticator app (e.g. Google Authenticator, Authy, Microsoft Authenticator, etc)

By default, both methods are enabled, meaning the users can choose to set up one or both methods. If you would like all users to use the same MFA method, simply toggle off one of the available options. Please note that if MFA is required on the account, then at least one method must be enabled.



Multi-factor Authentication

Enable MFA to require all your users to setup and use either email or authentication app to login in addition to their password.

☑ Require all users to use multi-factor authentication

Select which multi-factor authentication methods are allowed to be used by your users. You must select at least one

○ Email
All users can receive an email containing a verification code.

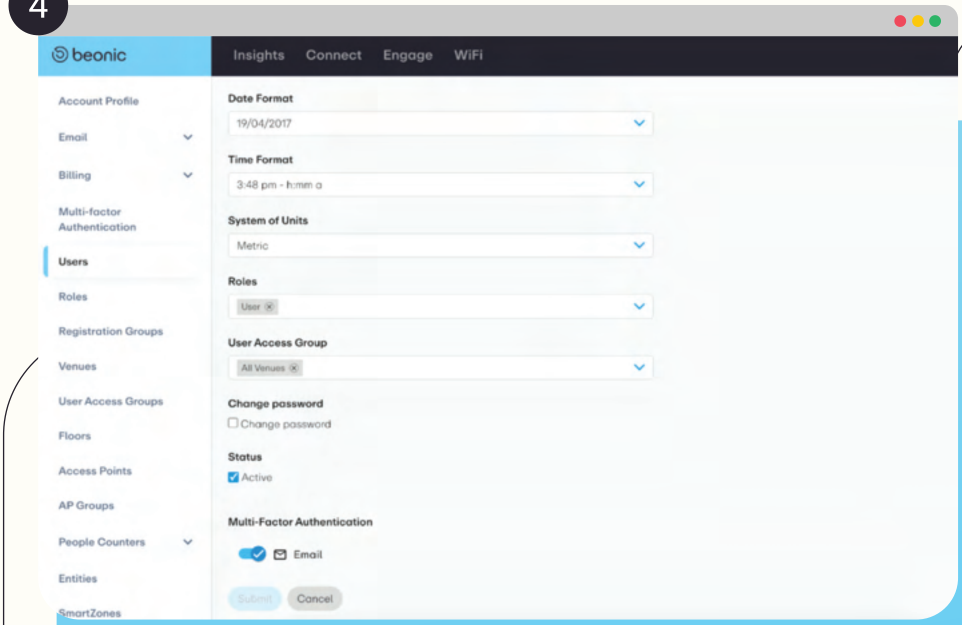
☑ Authentication App
All users can use an authentication app like Google Authenticator or Authy to generate a one-time code.

5. To disable MFA for all users, simply toggle off "Require all users to use multi-factor authentication".

For Account Admins - Managing MFA for a single user

1. Log in to your Beonic account.
2. Navigate to the Users settings under the Accounts Settings menu.
3. Select the user that requires MFA management.
4. The enabled MFA method(s) for that user will be displayed on the bottom of the page under Multi-Factor Authentication. To disable a method, toggle it off and click Submit.

4



Date Format: 19/04/2017

Time Format: 3:48 pm - h:mm a

System of Units: Metric

Roles: User ×

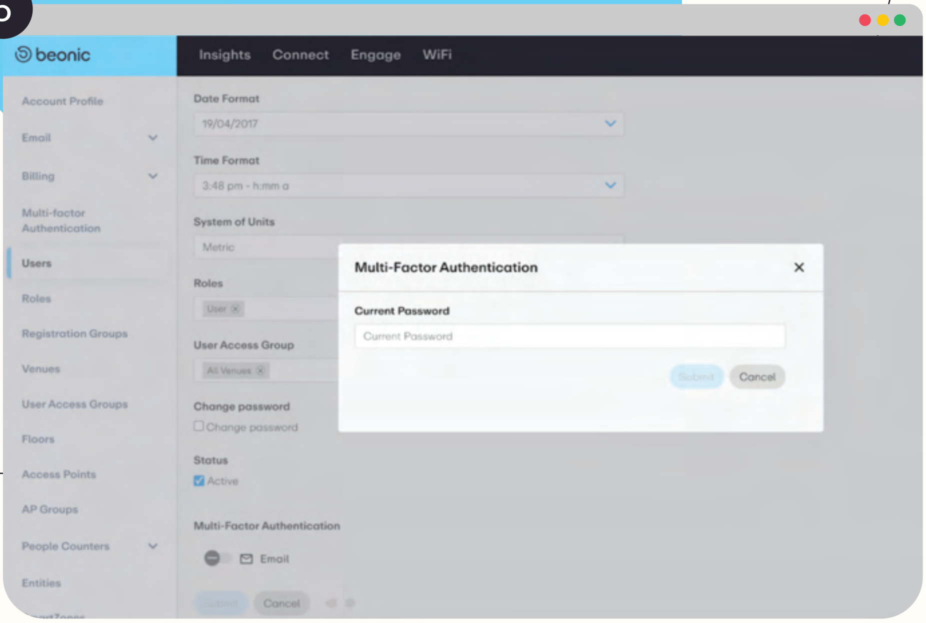
User Access Group: All Venues ×

Change password: □ Change password

Status: ☑ Active

Multi-Factor Authentication: ● Email

5



Date Format: 19/04/2017

Time Format: 3:48 pm - h:mm a

System of Units: Metric

Roles: User ×

User Access Group: All Venues ×

Change password: □ Change password

Status: ☑ Active

Multi-Factor Authentication: ○ Email

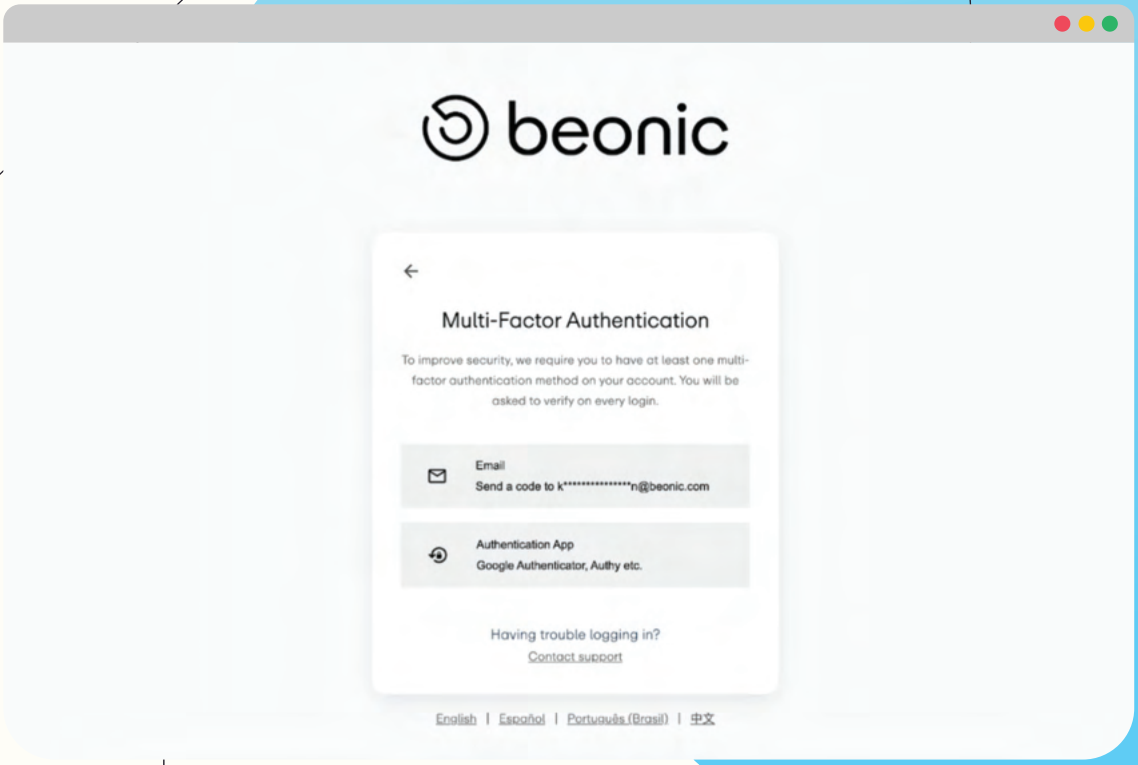
Multi-Factor Authentication

Current Password: Current Password

5. Follow the on-screen instructions to complete the process. You will be required to provide your password (and OTP if MFA is enabled).

For Users - Logging in for the first time after MFA enforcement on account

1. Enter your username and password as usual on the log in screen.
2. If your Account Admin enabled both authentication methods, you will be prompted to choose your preferred authentication method.



Multi-Factor Authentication

To improve security, we require you to have at least one multi-factor authentication method on your account. You will be asked to verify on every login.

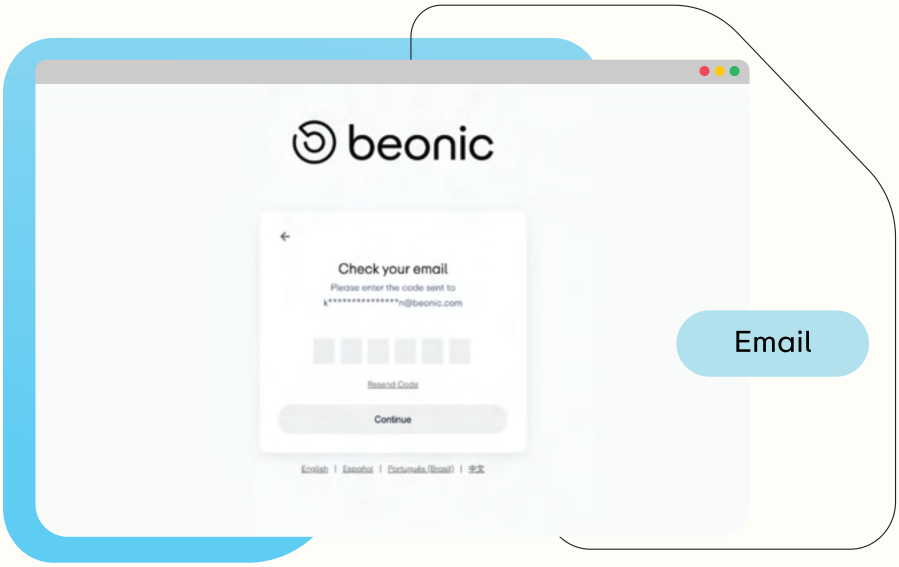
Email
Send a code to k***************n@beonic.com

Authentication App
Google Authenticator, Authy etc.

Having trouble logging in?
Contact support

English | Español | Português (Brasil) | 中文

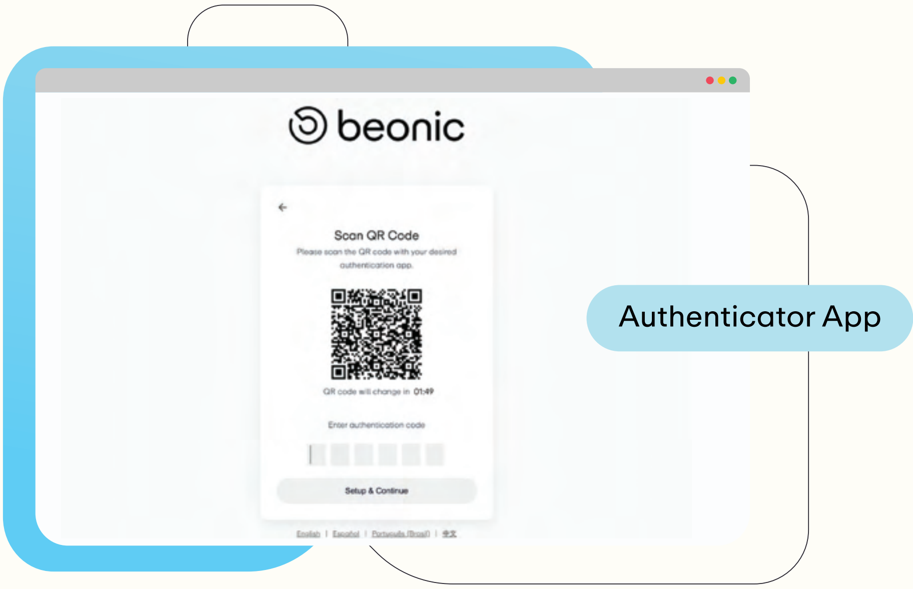
3. Follow the on-screen instructions to complete the set up for your chosen MFA method.



Email

Check your email

Please enter the code sent to k****************n@beonic.com



Authenticator App

Scan QR Code

Please scan the QR code with your desired authentication app.

QR code will change in 01:49

Enter authentication code

4. Verify your identity using your chosen MFA method:

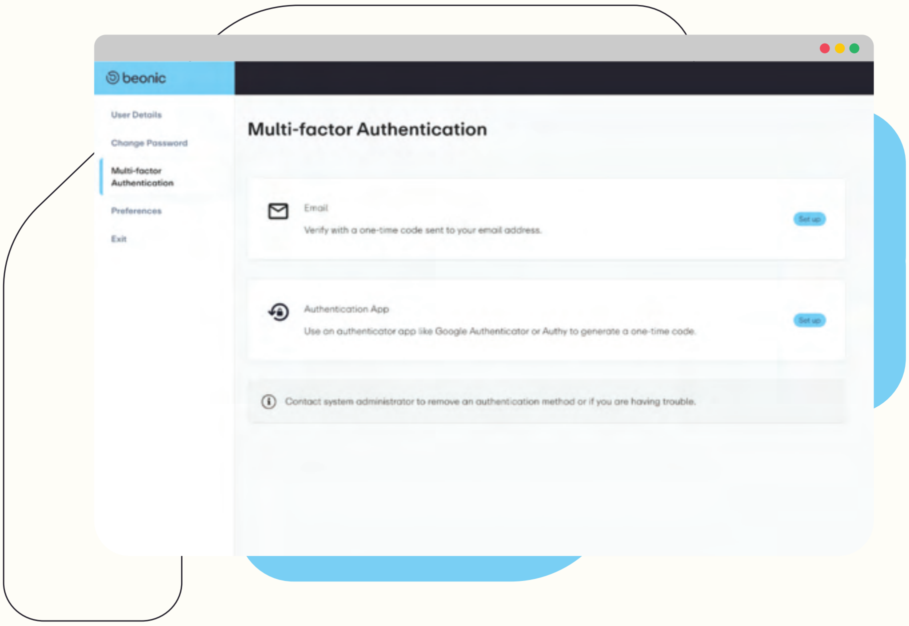
- If using email, enter the OTP sent to your email address
- If using an authenticator app, enter the time-based OTP displayed in the app.

5. Complete the log in process and gain access to your account.

For Users - Managing MFA on a user account (Opt-in)

If MFA is not enforced by your account admin, you can still choose to opt-in to MFA for added security on your personal account.

1. Log in to your Beonic account.
2. Navigate to the Multi-Factor Authentication settings under your User Profile.



Multi-factor Authentication

Email

Verify with a one-time code sent to your email address.

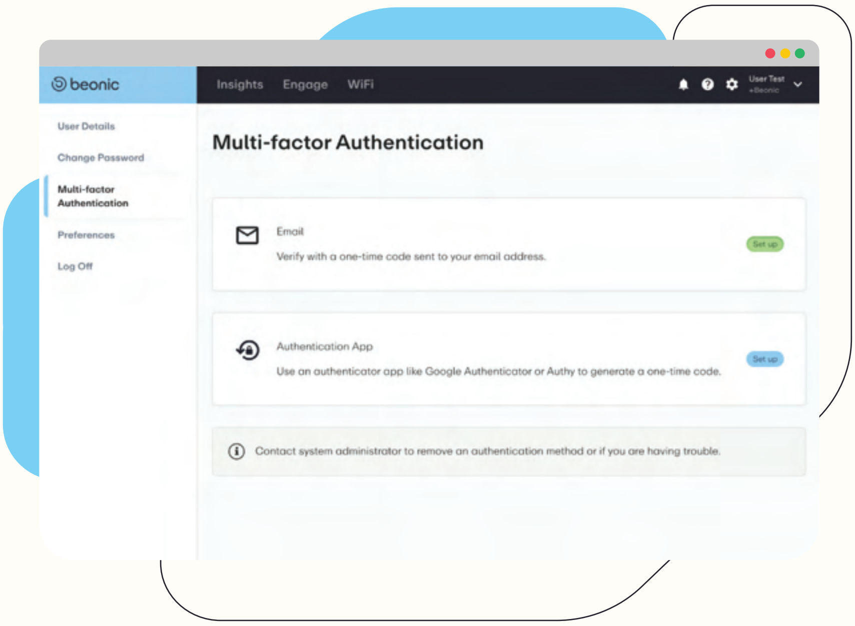
Authentication App

Use an authenticator app like Google Authenticator or Authy to generate a one-time code.

Contact system administrator to remove an authentication method or if you are having trouble.

3. Choose your preferred authentication method by selecting “Set up”. You can choose one or both of the following:

- Email-based OTP
- Authenticator app (e.g. Google Authenticator, Authy, Microsoft Authenticator, etc)



Multi-factor Authentication

Email

Verify with a one-time code sent to your email address.

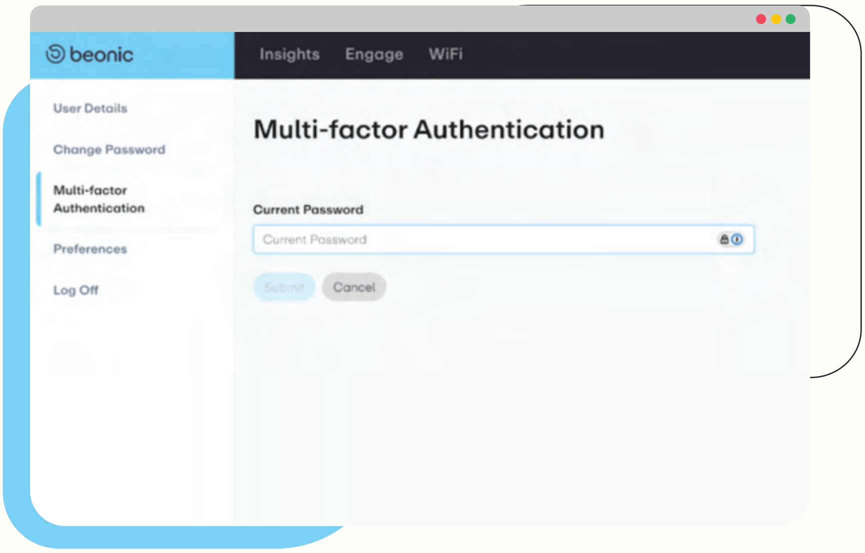
Authentication App

Use an authenticator app like Google Authenticator or Authy to generate a one-time code.

Contact system administrator to remove an authentication method or if you are having trouble.

4. Follow the on-screen instructions to complete the set up.

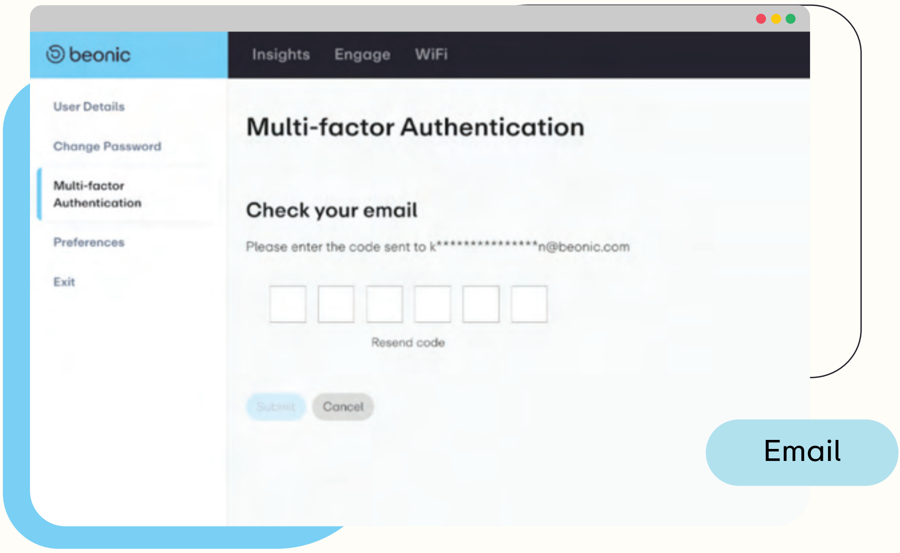
Enter your password when prompted:



Multi-factor Authentication

Current Password: Current Password

If setting up Email-based MFA:



Multi-factor Authentication

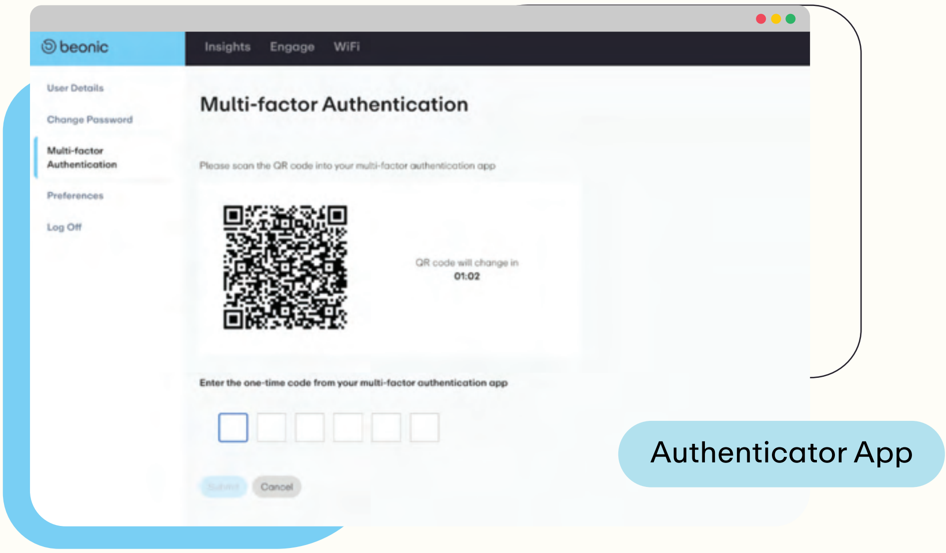
Check your email

Please enter the code sent to k***************n@beonic.com

□ □ □ □ □ □

Email

If setting up Authenticator App:



Multi-factor Authentication

Please scan the QR code into your multi-factor authentication app

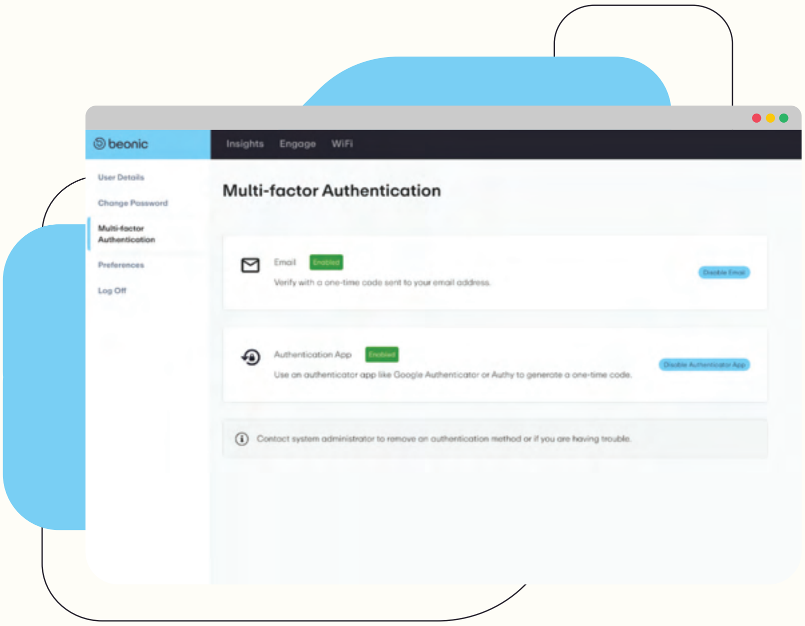
QR code will change in
01:02

Enter the one-time code from your multi-factor authentication app

□ □ □ □ □ □

Authenticator App

5. If you have both MFA methods enabled and only want to keep one, or if you want to change your MFA method from email to authenticator app or vice versa, disable the unwanted method by selecting the "Disable..." button next to that method.



Multi-factor Authentication

Verify with a one-time code sent to your email address.

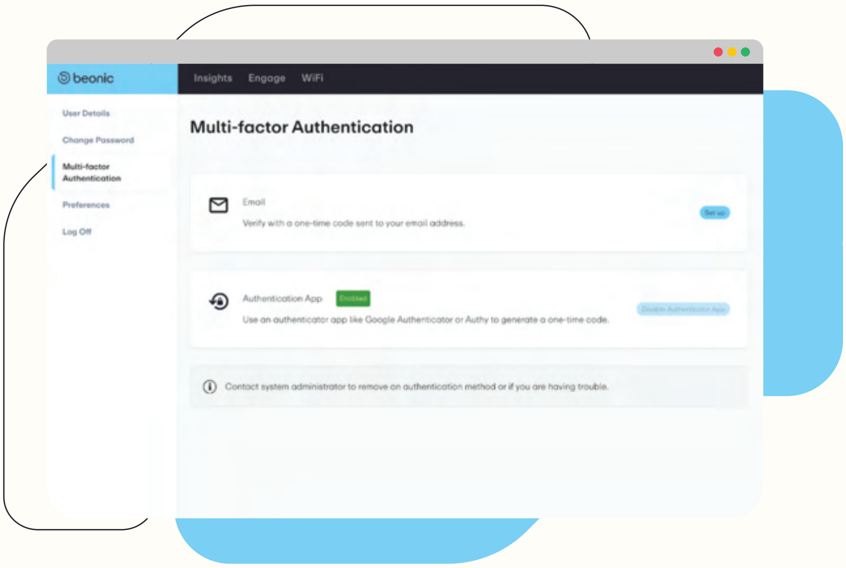
Use an authenticator app like Google Authenticator or Authy to generate a one-time code.

Contact system administrator to remove an authentication method or if you are having trouble.

Please note:

- *If you opted in to MFA (i.e. it's not enforced by your account admin), you will be able to disable both methods, at which point your account will no longer have MFA for added security.*
- *If MFA is enforced by your account admin, and both methods are allowed, you will need to have at least one method enabled.*
- *If a particular MFA method is required by your account admin, you will not be able to disable it.*

6. Follow the on-screen instructions to disable the selected method.



Multi-factor Authentication

Verify with a one-time code sent to your email address.

Use an authenticator app like Google Authenticator or Authy to generate a one-time code.

Contact system administrator to remove an authentication method or if you are having trouble.