Two-factor authentication (2FA)

Two-factor authentication (2FA) is a security method that requires users to provide two distinct forms of verification, typically a password and a unique code sent to a device, enhancing protection by adding an extra layer of defense against unauthorized access to accounts and systems.

2FA is supported by Coro to reduce the risk of unauthorized access to your Coro console.

> **Note**
>
> To learn more about the User Profile page, see **User Profile settings**.

Setting up 2FA with Coro

The first factor is your user credentials (username and password) and the second factor is provided through a mobile app.

There are two methods for enforcing 2FA:

- **An admin user chooses to enable 2FA from their profile**.
- **2FA is enforced for all Admin users**.

Enabling 2FA from an admin user's profile

To enable 2FA from an admin user profile:

1. Install an authenticator app on your mobile device (such as Google Authenticator).
2. **Log into the Coro console** and select the **User Profile** icon in the toolbar (an avatar, typically set to your initials):

3. Select **My Account** from the menu: