



2 Factor Authentication (2FA)

Increase security and reduce fault risk

8 2FA



Contents

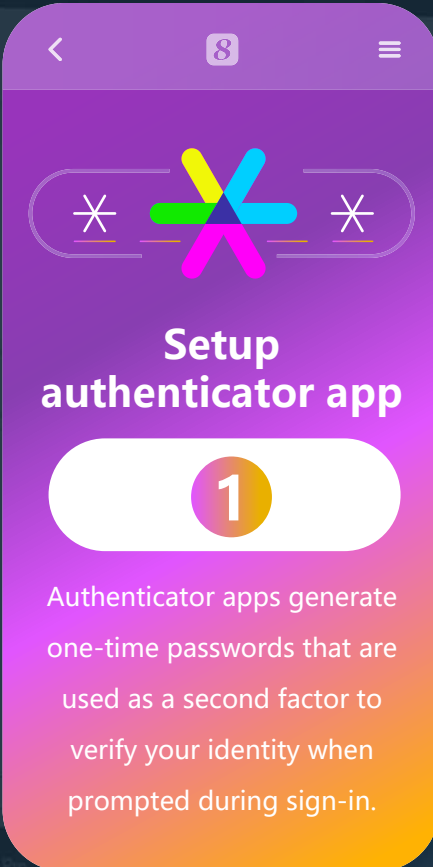
How it works

Setup the Authenticator app

Steps to start



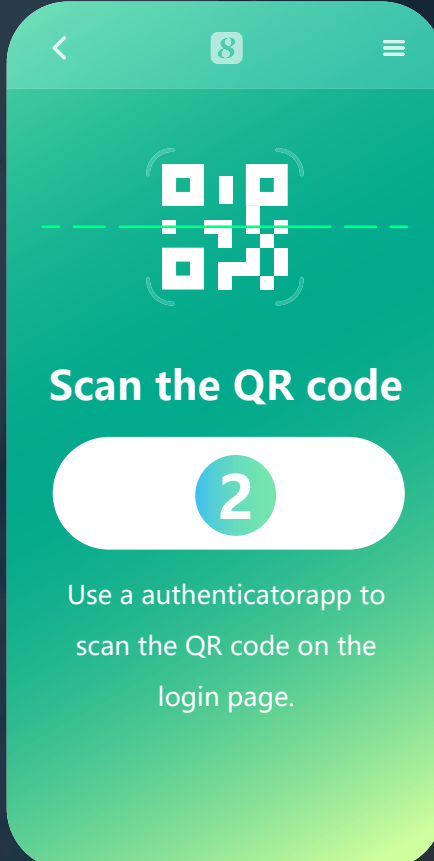
How it works



Setup authenticator app

1

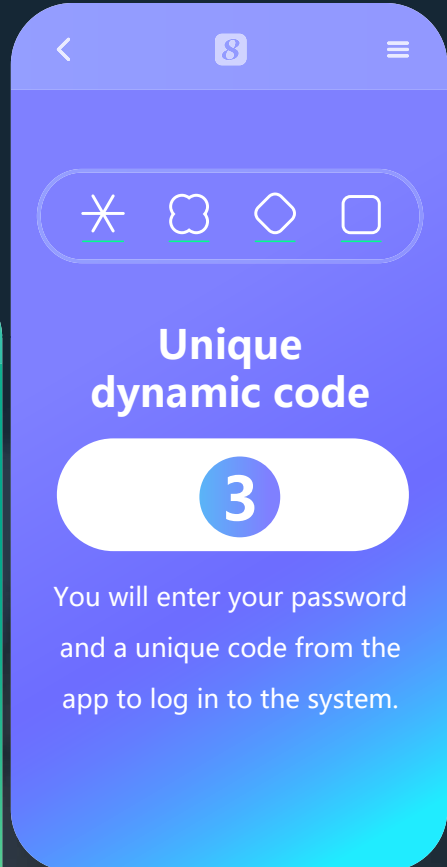
Authenticator apps generate one-time passwords that are used as a second factor to verify your identity when prompted during sign-in.



Scan the QR code

2

Use a authenticatorapp to scan the QR code on the login page.



Unique dynamic code

3

You will enter your password and a unique code from the app to log in to the system.

Setup the Authenticator app

The following are commonly used authenticator apps.



Google Authenticator

Dynamic



Microsoft Authenticator
Microsoft Corporation



Twilio Authy Authenticator
Authy

Security



1Password: Password Manager
AgileBits
In-app purchases



Dynamic passwords will be updated regularly, such as Google Authenticator, which is valid for 30 seconds.

Steps to start

- 1 Install a 2FA app (e.g., Google Authenticator) on your phone.
- 2 Login 8 via a PC browser for the first time and it will generate a QR code.



- 3 Scan the QR code via the 2FA app and it will bind 8 to the 2FA app.
- 4 Enter the one-time password generated by 2FA app on the 8 login page and login the 8.

8 can provide best combination of standard products & redevelopment services for enterprise management and over 500 corporations in Asia are using our following modules on-premises or SaaS:

8 CRM : Corporate Client CRM and Consumer CRM

8 Service : Service Management

8 SRM : Supplier Management, e-Procurement and e-Tender

8 PPM : Project and Portfolio Management

8 New Way : Visual Agile and Lean

8 Timesheet : Resource Time and Cost Management

8 EDMS : Electronic Document Management System

8 OA : Office Automation

8 HCM : Human Capital Management

8 All-in-one : Enterprise Full Automation