Setting up Two Factor Authentication (2FA)

Last Modified on 08/05/2025 11:41 am ACST

Determine if a user has 2FA enabled:

Prerequisites

CareRight must on a version 6.87 or higher

System Administration > Users and Groups > Determine if a user has 2FA enabled

System administrators can review specific user accounts and determine if they have 2FA enabled.

Set up 2FA:

User Profile > Set up 2FA

Users wishing to enable 2FA, where the authentication mechanism is password, will see a new control available in their user profile:
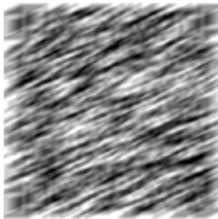

Simply scan the QR Code on screen with your preferred authenticator, then confirm your password(s).

Scan QR Code

Please scan the below QR code using an OTP compatible app (such as 1Password, Google Authenticator or Authy).

If you cannot scan, please enter the following code manually:

Confirm One Time Password

Please confirm that your authentication application is working by entering a generated code below.

* Code

* Enter your current password

[Confirm and Enable Two Factor]

You will be presented with your backup codes on a following screen.

Disable 2FA:

User profile -> Disable 2FA

User can disable 2FA from user profile under user Authentication.

test 3

[Edit] [View Staff Member Details]

⌂ Dashboard / Administration / Users and Groups

User Authentication

Username	test-three
Email	test3@clintel.com
	2FA Enabled
Disable 2FA	

Authorisation

Groups	• Healthsolve CMS Administration

Correspondence Settings

Correspondence View	All Correspondence
Correspondence Type Filter	Email
Default Patient Page	Accounts

Requiring 2FA

System Administrators can require password based users to enable 2FA via Global Settings

Security Options	
Force 2fa For Password User	false ▾
Location Restrict Patient Correspondence	true ▾
Location Restrict Patient Documents	false ▾
Same Site Cookie	Strict ▾
Session Time Out	60