Two-Factor Authentication Setup for CAREWare 5

Overview

Setting up two-factor authentication (2FA) in CAREWare 5 is a quick and powerful way to increase the security of the CAREWare user login process.

Configure central administrator permissions related to the 2FA feature

Here are instructions for granting permissions in CAREWare.

•*Turn 2 Factor On and Off*. Granting this permission will enable a user to choose whether or not the server will enforce 2FA.
•*Reset User 2 Factor Key*. Granting this permission will enable a user to reset other users' 2FA keys. When a user's 2FA key is reset, that user will be prompted to set up his or her device at the next login.

Configure provider domain permissions related to the 2FA feature (if desired)

•*Reset User 2 Factor Key*. Granting this permission will enable a user to reset 2FA keys for user accounts assigned to the provider they administer. When a user's 2FA key is reset, that user will be prompted to set up his or her device at the next login.

Turn on 2FA from Central Administration

1.Click *Administrative Options*.
2.Click *Advanced Security Options*.
3.Click *Server 2 Factor Setup*.
4.Choose : *ON* (using internal RFC 6238 TOTP key based authentication).
5.Click *Submit*.

Resetting Users' 2 Factor Keys

If a user gets a new smartphone or for other reasons needs to start over with a new authenticator, you will need to reset his or her key.

1.Click *Administrative Options*.
2.Click *Provider/User Manager*.
3.Expand *Users*.
4.Right-click on the user.
5.Click *Reset 2 Factor Key*.