**Two-Factor Authentication Setup for CAREWare 6**

Overview

Setting up two-factor authentication (2FA) in CAREWare 6 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

- *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.
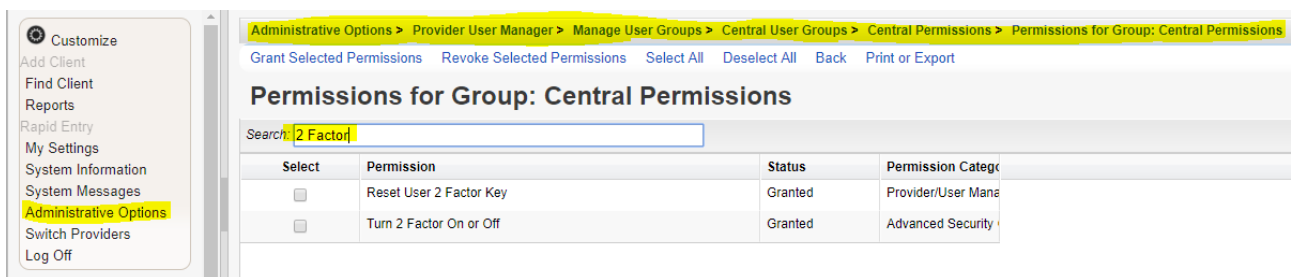
To grant permissions for 2 Factor Authentication for Central Administration Groups:

1. Log into *Central Administration*.
2. Click *Administrative Options*.
3. Click *Provider User Manager*.
4. Click *Manage User Groups*.
5. Click *Central User Groups*.
6. Select the *User Group Name*.
7. Click *Manage*.
8. Click *Change Permissions*.
9. Type *2 Factor* in the Search field.
10. Check each permission to be granted.
11. Click *Grant Selected Permissions*.

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.

1. Log into *Central Administration*.
2. Click *Administrative Options*.
3. Click *Provider User Manager*.
4. Click *Manage User Groups*.
5. Click Provider*User Groups*.
6. Select the *User Group Name*.
7. Click *Manage*.
8. Click *Change Permissions*.
9. Type *2 Factor* in the Search field.
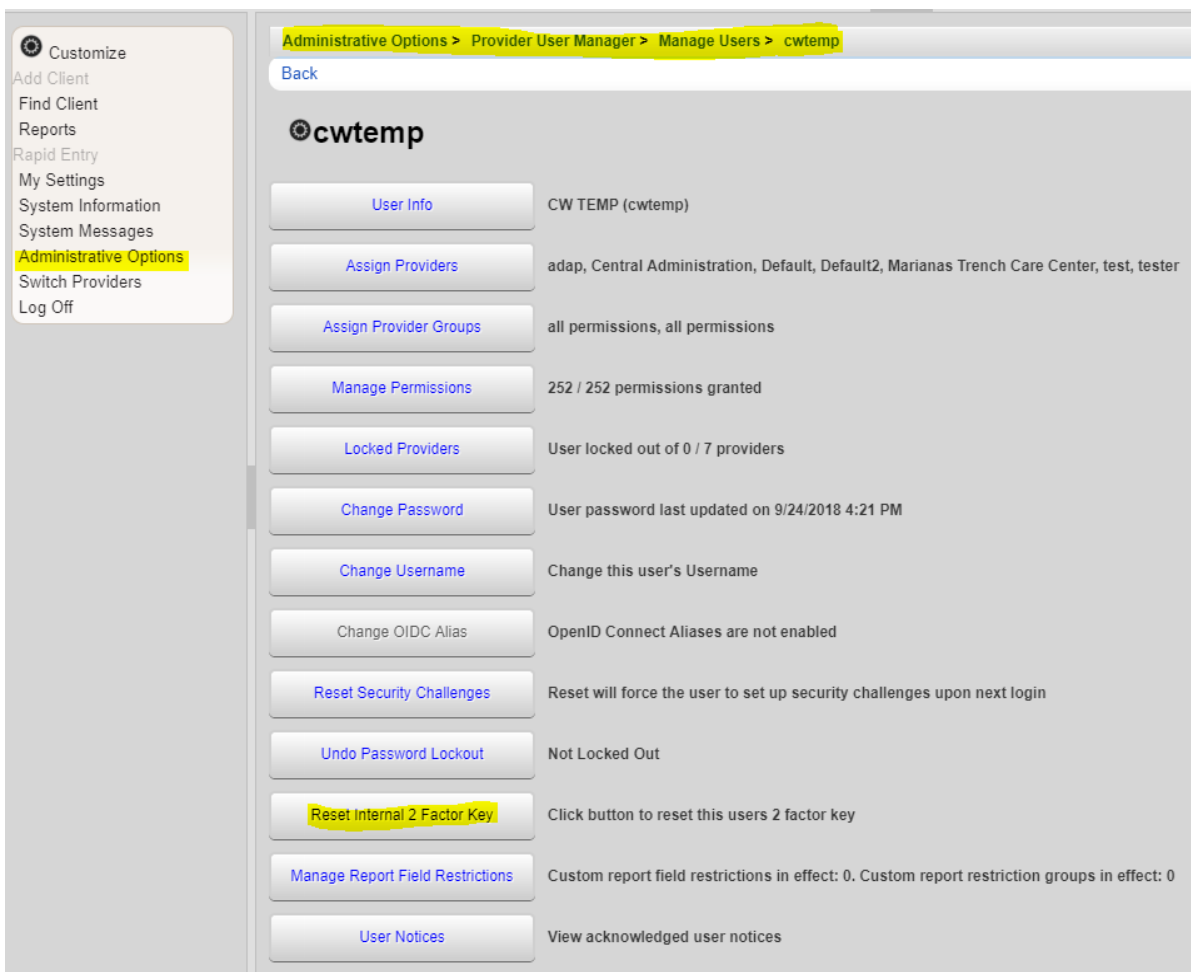10. Check each permission to be granted.

11. Click *Grant Selected Permissions*.

Turn on 2FA from Central Administration
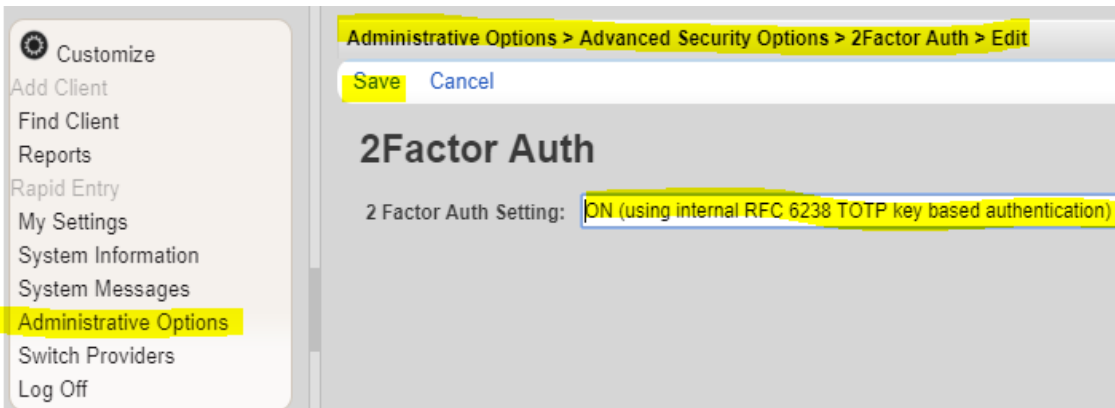
1. Click *Administrative Options*.
2. Click *Advanced Security Setup*.
3. Click *Turn 2 factor authentication On or Off*.
4. Click *Edit*.
5. Choose *ON (using internal RFC 6238 TOTP key based authentication)*.
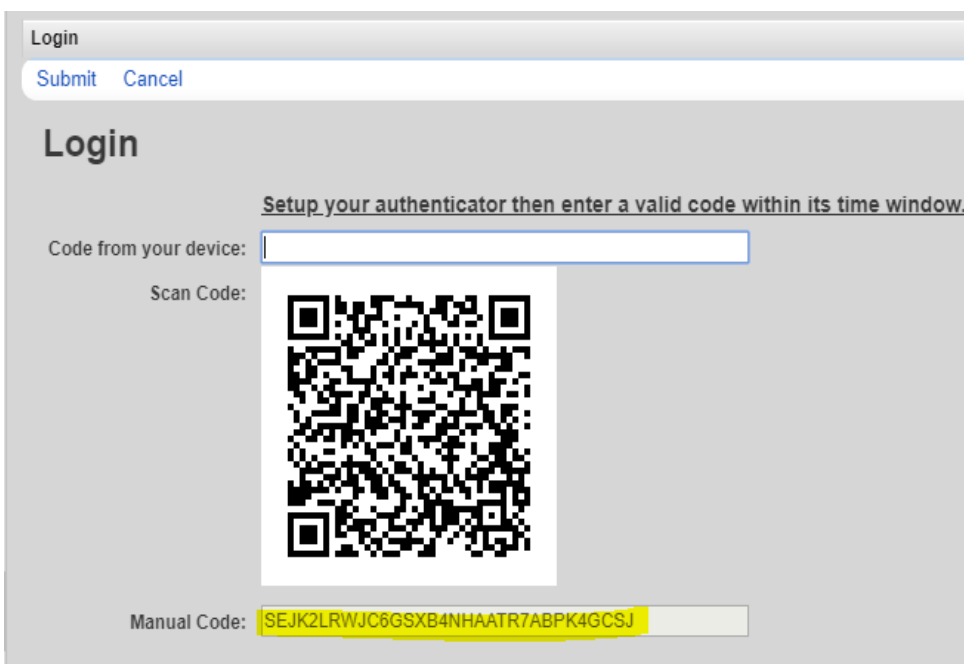6. Click *Save*.

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. Click *Manage Users*.
4. Select the user and click *Manage*.
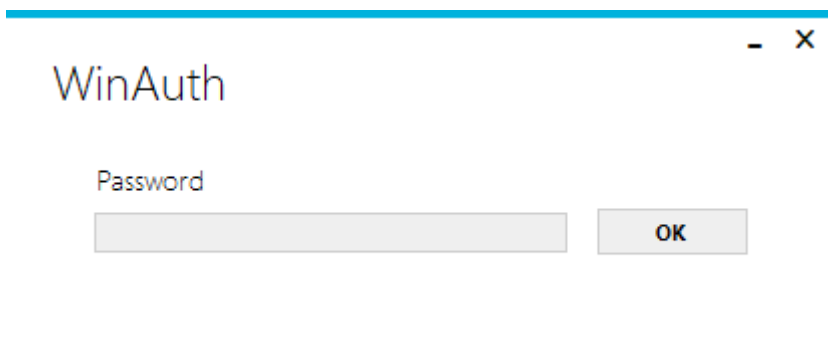5. Click *Reset Internal 2 Factor Key*.

Once two-factor authentication (2FA) is set up in CAREWare, two-factor authentication (2FA) can be set up for the device by completing the following instructions:

1. Reset Internal 2 Facotr Key.

2. Log into CAREWare.

3. Copy the Manual Code.

4. Start the 2 Factor application.

5. Enter the password.

6. Click OK.

7. Click Add.

8. Select the 2 Factor application from the list.

9. Paste the manual code in the Decode line.

10. Click Verify Authentication.

11. Enter the code in the code from device line in the log in screen.

12. Click Submit.

13. Log into CAREWare.

14. Enter the code again.

15. Click Submit.