

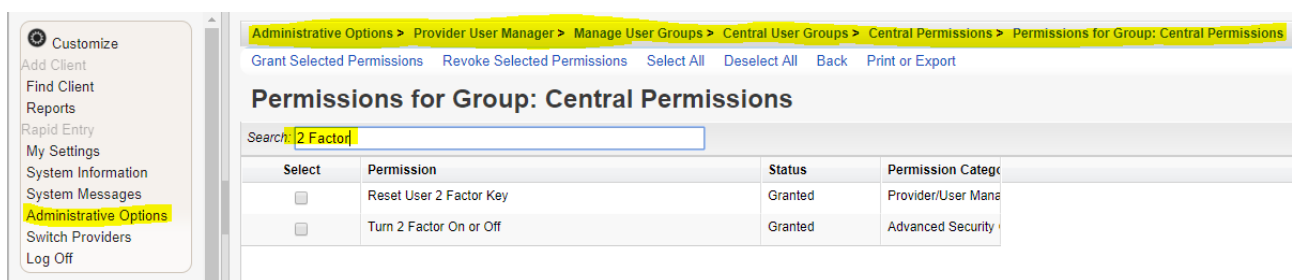
Two-Factor Authentication Setup for CAREWare 6

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. CAREWare works with most 2FA applications and has its own 2FA application that can be downloaded [here](#).

Configure central administrator permissions related to the 2FA feature

- *Turn 2 Factor On or Off.* Granting this permission enables a user to choose whether or not the server will enforce 2FA.
- *Reset User 2 Factor Key.* Granting this permission enables 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:

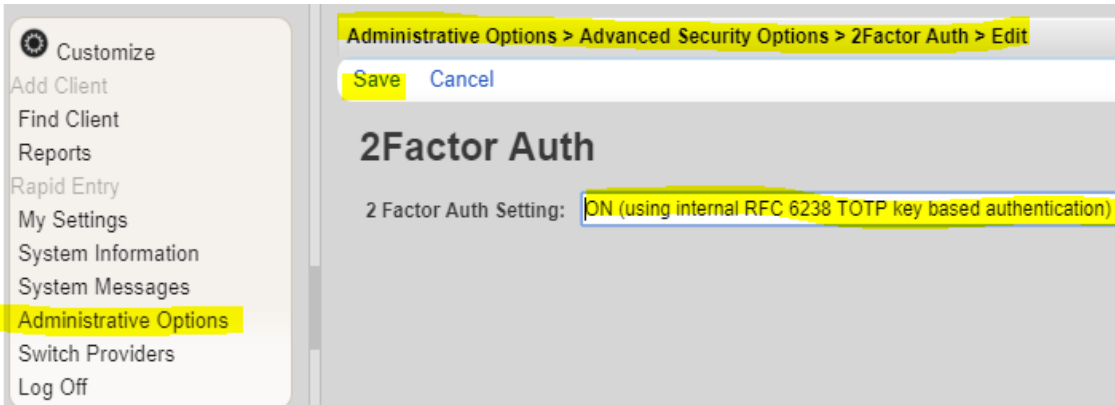
1. Log into *Central Administration*.
2. Click *Administrative Options*.
3. Click *Provider User Manager*.
4. Click *Manage User Groups*.
5. Click *Central User Groups*.
6. Select the *User Group Name*.
7. Click *Manage*.
8. Click *Change Permissions*.
9. Type *2 Factor* in the Search field.
10. Check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

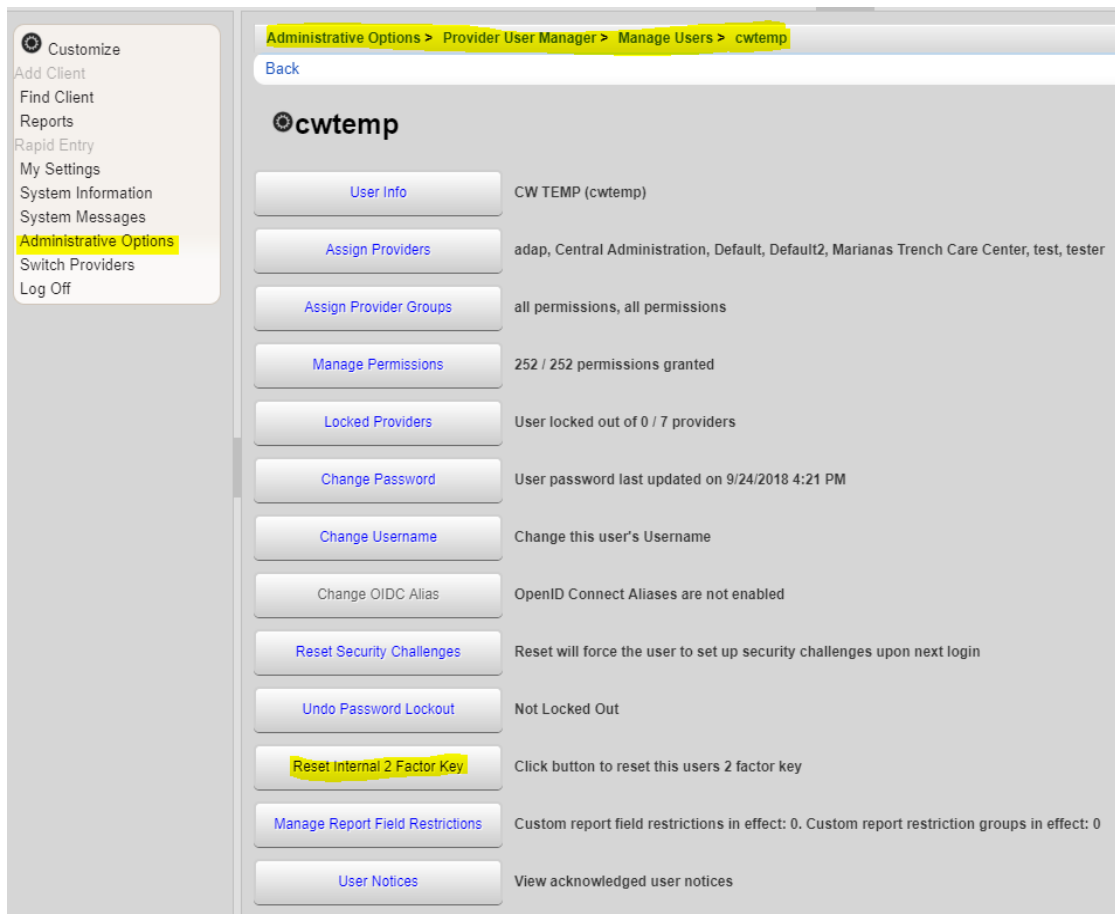
10. Check each permission to be granted.
11. Click *Grant Selected Permissions*.

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
5. Click *Manage*.
6. Click *Reset Internal 2 Factor Key*.

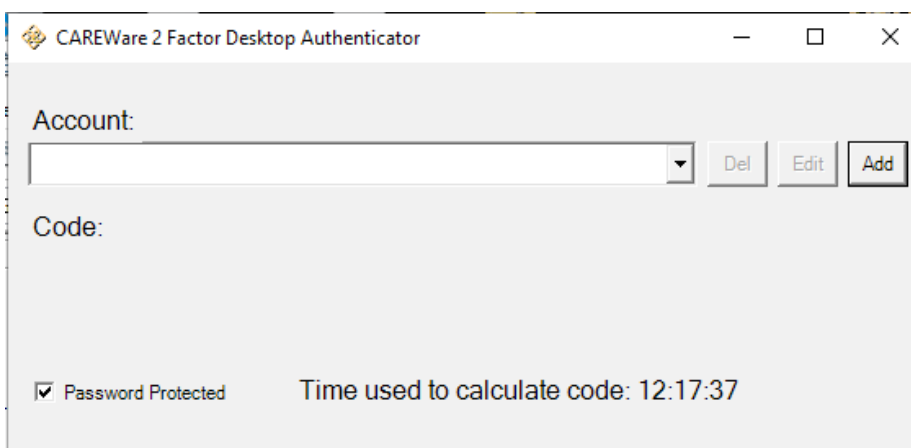
Once two-factor authentication (2FA) is set up in CAREWare, two-factor authentication (2FA) can be set up for the device by completing the following instructions:

1. Reset *Internal 2 Factor Key*.
2. Log into CAREWare.

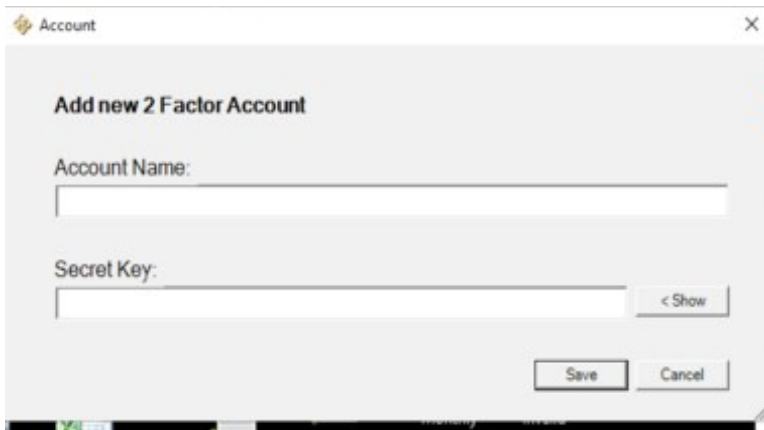


The screenshot shows a web browser window titled "Login". At the top, there are "Submit" and "Cancel" buttons. Below the title, there is a heading "Login" and a sub-heading "Setup your authenticator then enter a valid code within its time window." There are two input fields: "Code from your device:" which is empty, and "Manual Code:" which contains the text "SEJK2LRWJC6GSXB4NHAATR7ABPK4GCSJ" highlighted in yellow. A QR code is displayed in the center of the page, labeled "Scan Code:".

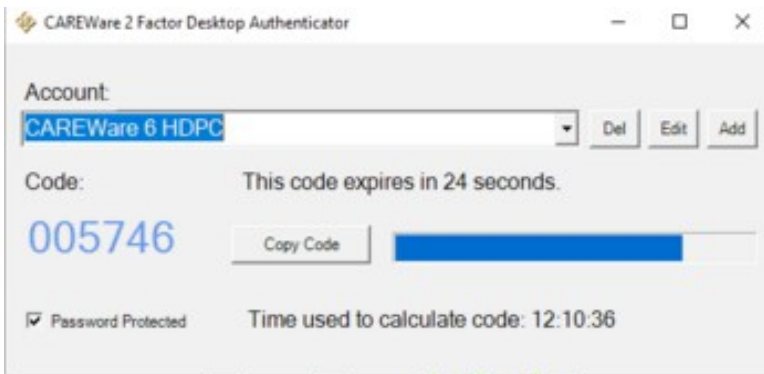
3. Copy the *Manual Code*.
4. Start the CAREWare 2FA Desktop Client.



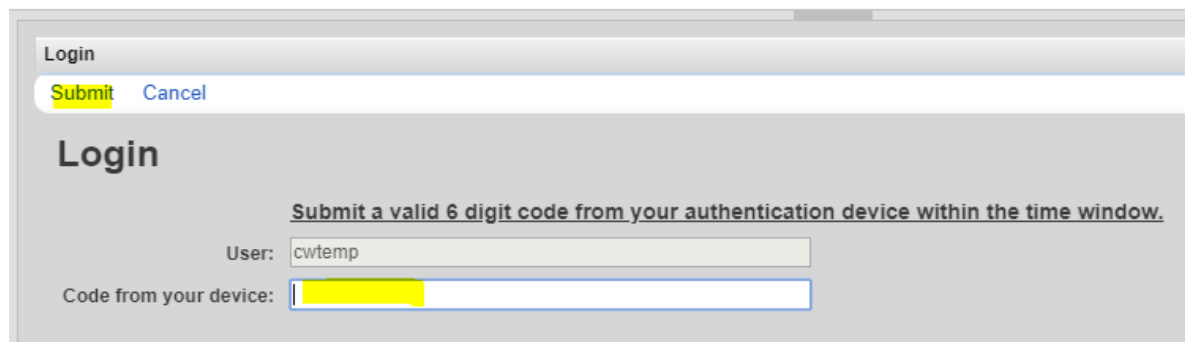
The screenshot shows a desktop application window titled "CAREWare 2 Factor Desktop Authenticator". It has a standard Windows window title bar with minimize, maximize, and close buttons. The main content area includes an "Account:" label above a dropdown menu. To the right of the dropdown are three buttons: "Del", "Edit", and "Add". Below the dropdown is a "Code:" label. At the bottom left, there is a checked checkbox labeled "Password Protected". At the bottom right, it displays "Time used to calculate code: 12:17:37".



5. Click *Add*.
6. Enter the *Account Name*.
7. Paste the manual code in the *Secret Key* line.
8. Click *Save*.



9. Enter the code in the code from device line in the log in screen.
10. Click *Submit*.
11. Log into CAREWare.
12. Enter the code again.
13. Click *Submit*.



The 2FA application can be password protected by checking *Password Protected*.

