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 <u>here</u>.

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.

Customize	Administrative Grant Selected	Options > Provider User Manager > Manage User (Groups > Central User Groups	Central Permissions > Permissions for Group: Central Permissi Print or Export		
Find Client Reports	Permise	Permissions for Group: Central Permissions				
Rapid Entry My Settings	Search: 2 Facto	d.				
System Information	Select	Permission	Status	Permission Catego		
System Messages		Reset User 2 Factor Key	Granted	Provider/User Mana		
Administrative Options Switch Providers Log Off		Turn 2 Factor On or Off	Granted	Advanced Security		

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

O Customize	Administrative Options > Advanced Security Options > 2Factor Auth > Edit
Add Client	Save Cancel
Find Client	
Reports	2Factor Auth
Rapid Entry	
My Settings	2 Factor Auth Setting: DN (using internal RFC 6238 TOTP key based authentication)
System Information	
System Messages	
Administrative Options	
Switch Providers	
Log Off	

- 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

O Customize	Administrative Options > Provider	User Manager > Manage Users > cwtemp				
Add Client	Back					
Find Client Reports Rapid Entry	®cwtemp					
My Settings System Information System Messages	User Info	CW TEMP (cwtemp)				
Administrative Options Switch Providers	Assign Providers	adap, Central Administration, Default, Default2, Marianas Trench Care Center, test, tester				
Log Off	Assign Provider Groups	all permissions, all permissions				
	Manage Permissions	252 / 252 permissions granted				
	Locked Providers	User locked out of 0 / 7 providers				
	Change Password	User password last updated on 9/24/2018 4:21 PM				
	Change Username	Change this user's Username				
	Change OIDC Alias	OpenID Connect Aliases are not enabled				
	Reset Security Challenges	Reset will force the user to set up security challenges upon next login				
	Undo Password Lockout	Not Locked Out				
	Reset Internal 2 Factor Key	Click button to reset this users 2 factor key				
	Manage Report Field Restrictions	Custom report field restrictions in effect: 0. Custom report restriction groups in effect: 0				
	User Notices	View acknowledged user notices				

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.

Login	
Submit Cancel	
Login	
	<u>Setup your authenticator then enter a valid code within its time window.</u>
Code from your device:	
Scan Code:	
Manual Code:	SEJK2LRWJC6GSXB4NHAATR7ABPK4GCSJ

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

CAREWare 2 Factor Deskto CAREWAREWAREWAREWAREWAREWAREWAREWAREWAREW	op Authenticator	_		×
Account:				
		▼ Del	Edit	Add
Code:				
Password Protected	Time used to calculate code:	12:17:37		

Add new 2 Factor Account	
Account Name:	
Secret Key:	
Secret Key:	< Show
Secret Key:	< Show

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

CAREWare 2 Factor Desi	top Authenticator		-		×
Account: CAREWare 6 HDP0		•	Del	Edit	Add
^{Code:} 005746	This code expires in 24 sect	onds.			
Password Protected	Time used to calculate code	e: 12:10:36	5		

- 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.

Login		
Submit	Cancel	
Logi	in	
		Submit a valid 6 digit code from your authentication device within the time window.
	User:	cwtemp
Code fr	om your device:	

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

🚸 CAREWare 2FA Get Password		_		×
Password:			< Show]
	Submit		Cancel	