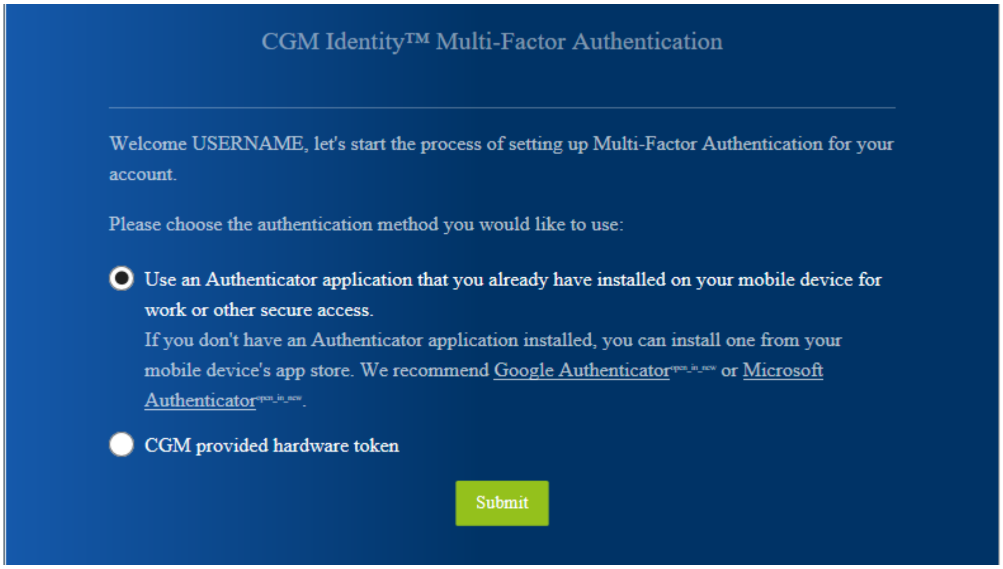
Multi-Factor Authentication

Multi-Factor Authentication (MFA) will be required for DAQbilling. MFA is a multi-step account login process that requires users to authenticate their account with more than just a password. Users can use an Authenticator application such as Google Authenticator or Microsoft Authenticator.

To set up Multi-Factor Authentication:

1. Enter your client name, username, and password associated with your DAQbilling account and click **OK**.
2. The MFA is triggered by the sign in process. Please choose the authentication method to use. Options are an Authenticator app or a CGM provided hardware token.
3. If using the Authenticator app for MFA, select the first radio button and click **Submit**.



CGM Identity™ Multi-Factor Authentication

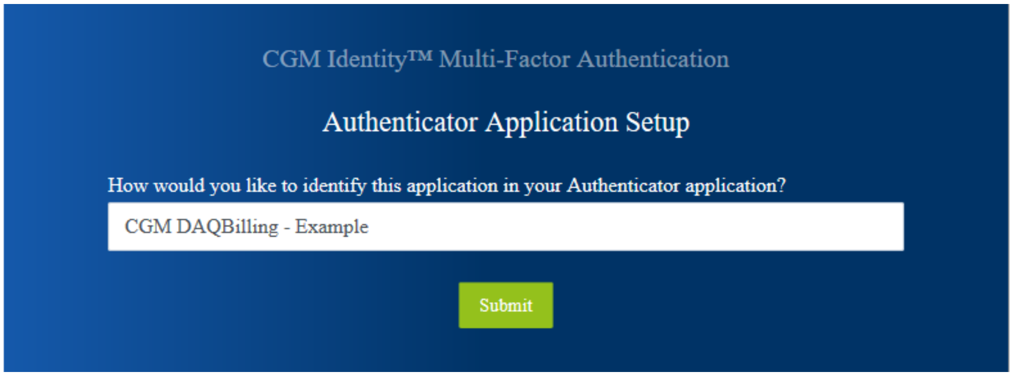
Welcome USERNAME, let's start the process of setting up Multi-Factor Authentication for your account.

Please choose the authentication method you would like to use:

● Use an Authenticator application that you already have installed on your mobile device for work or other secure access.
If you don't have an Authenticator application installed, you can install one from your mobile device's app store. We recommend Google Authenticator$^{open\_in\_new}$ or Microsoft Authenticator$^{open\_in\_new}$.

○ CGM provided hardware token

4. Enter a name to be used to identify this application in the Authenticator app. Click **Submit**. The authenticator app login is valid for a 12-hour duration. Once logged in, the MFA will not prompt again for 12 hours.



CGM Identity™ Multi-Factor Authentication

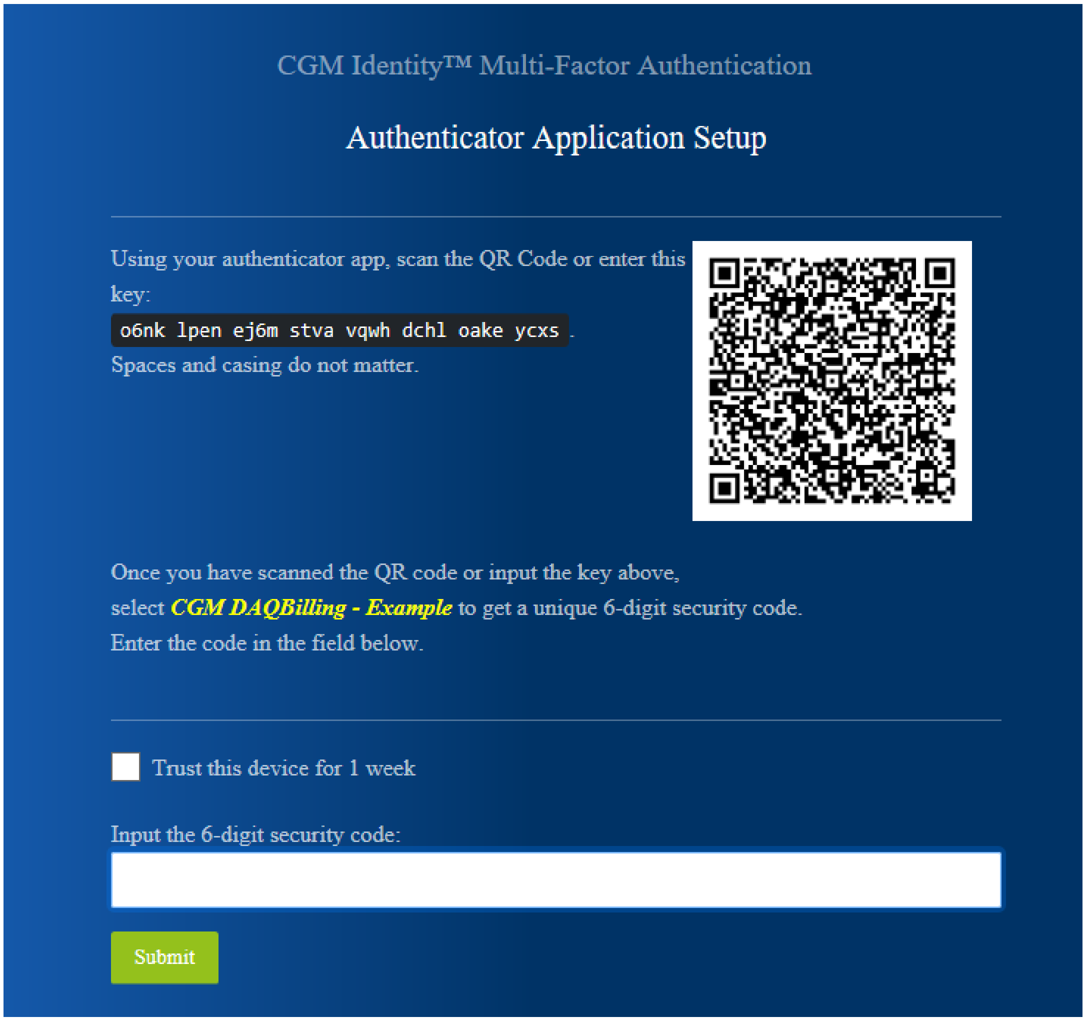
Authenticator Application Setup

How would you like to identify this application in your Authenticator application?

CGM DAQBilling - Example

Note: If a user attempts to login without using an authentication method, the system will continue to prompt for authentication.

5. Using the authenticator app, scan the QR Code or enter the key shown on the screen. To scan the QR Code, use your mobile device's camera with the QR Code scanner in the authenticator app. This process varies depending on the app in use. Users can also enter the key provided instead of scanning the QR Code, if preferred.



CGM Identity™ Multi-Factor Authentication

Authenticator Application Setup

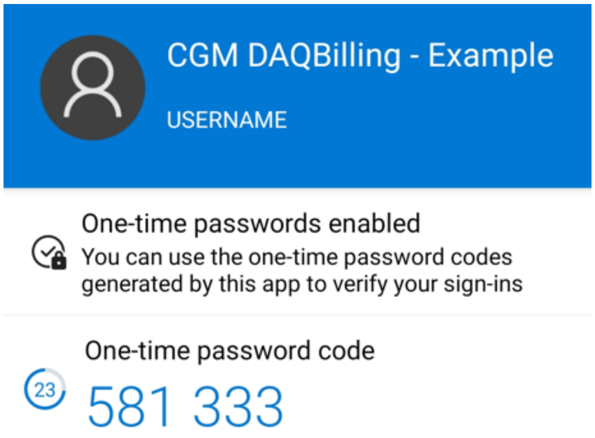
Using your authenticator app, scan the QR Code or enter this key:
`o6nk lpen ej6m stva vqwh dchl oake ycxs` .
Spaces and casing do not matter.

Once you have scanned the QR code or input the key above,
select ***CGM DAQBilling - Example*** to get a unique 6-digit security code.
Enter the code in the field below.

□ Trust this device for 1 week

Input the 6-digit security code:

6. Once the QR Code is scanned, the authenticator provides a 6-digit verification code to enter on the DAQbilling authentication screen. The following example is from Microsoft Authenticator. The app gives the user 30 seconds to use the code before resetting to a new code. Enter the code on the DAQbilling Authentication screen. An error displays if the code is entered incorrectly.



CGM DAQBilling - Example

USERNAME

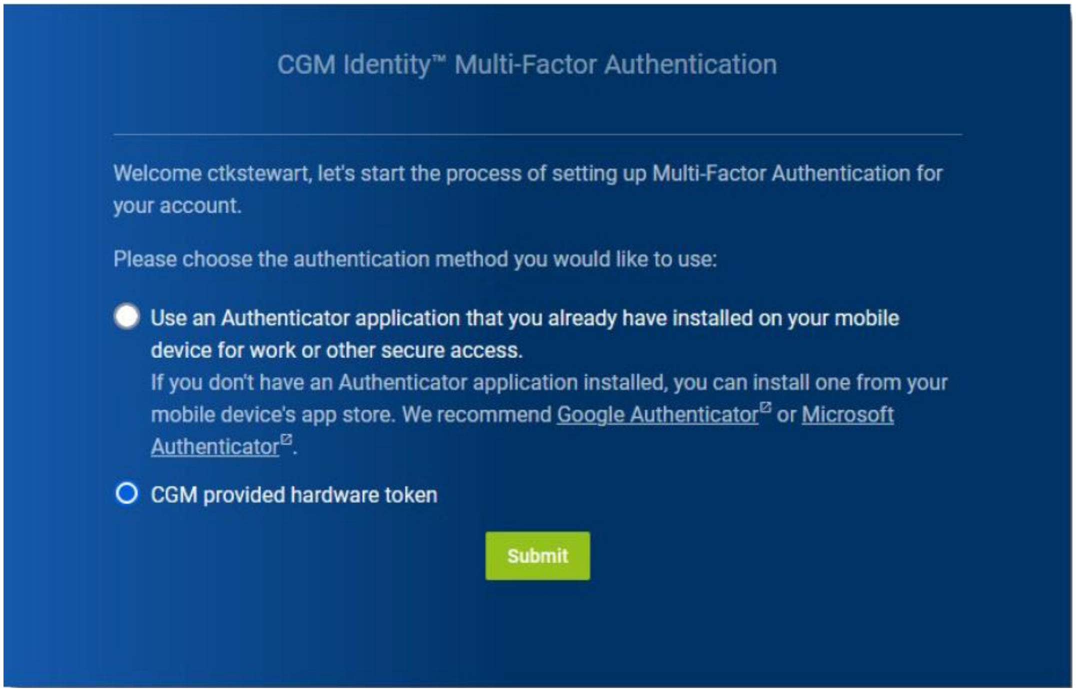
One-time passwords enabled

You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code

581 333

7. If using a CGM hardware token for MFA, select the second radio button and click Submit. (If you are interested in purchasing a CGM hardware token, please contact your sales team member.)



CGM Identity™ Multi-Factor Authentication

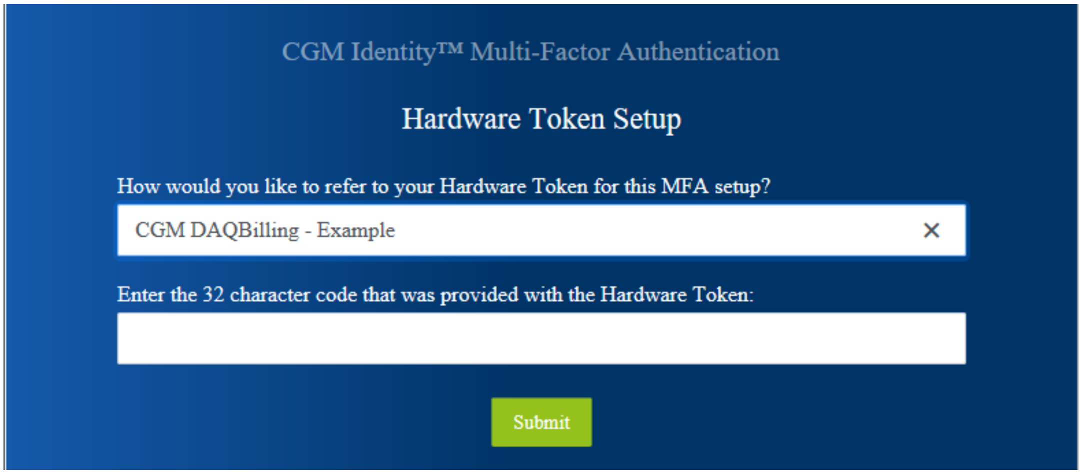
Welcome ctkstewart, let's start the process of setting up Multi-Factor Authentication for your account.

Please choose the authentication method you would like to use:

○ Use an Authenticator application that you already have installed on your mobile device for work or other secure access.
If you don't have an Authenticator application installed, you can install one from your mobile device's app store. We recommend Google Authenticator or Microsoft Authenticator.

● CGM provided hardware token

8. Enter a name to identify the Hardware Token for this setup and then enter the 32-character code for the hardware token. Please contact DAQbilling Support for assistance with hardware tokens.



CGM Identity™ Multi-Factor Authentication

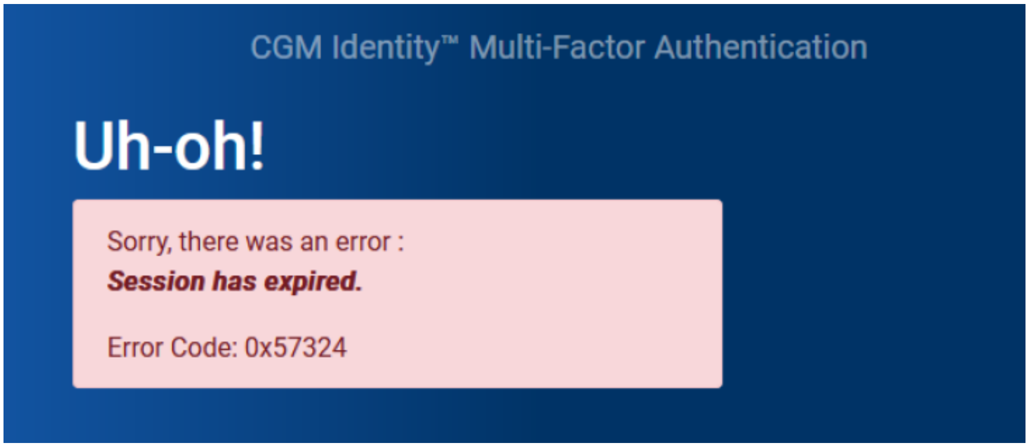
Hardware Token Setup

How would you like to refer to your Hardware Token for this MFA setup?

CGM DAQBilling - Example

Enter the 32 character code that was provided with the Hardware Token:

9. If the verification code is correct, the user will be logged into the account. If a user attempts to login without using an authentication method, the system will continue to prompt for authentication.
10. If the following session expiration message displays, please try to set up the MFA again.



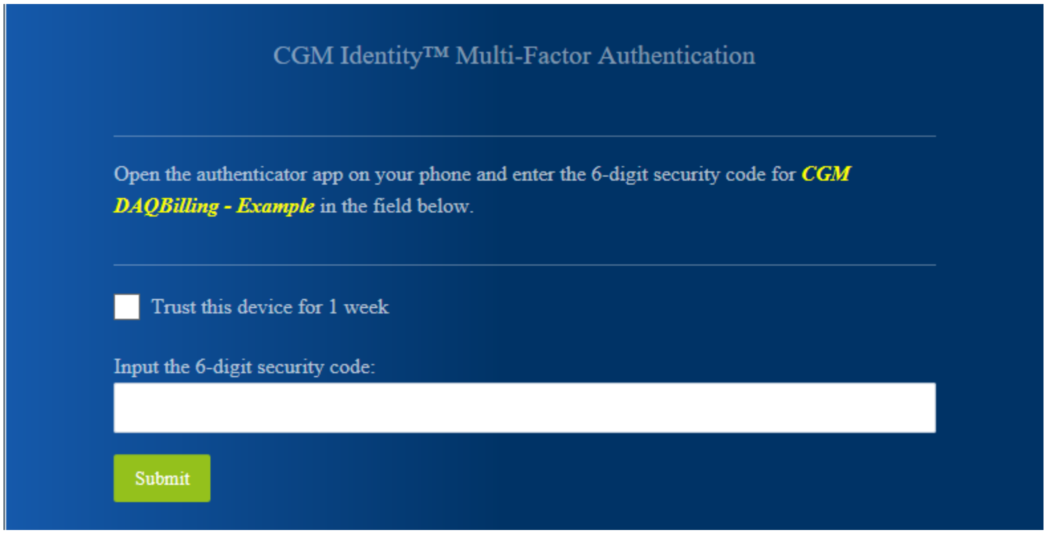
CGM Identity™ Multi-Factor Authentication

Uh-oh!

Sorry, there was an error :
Session has expired.

Error Code: 0x57324

11. After initial setup, when the user attempts to log into DAQbilling, the MFA prompts the user to open the authenticator app on their phone and enter the 6-digit security code. If the user marks the check box **Trust this device for 1 week**, the MFA will not prompt the user again for a week. If the check box is left unmarked, the user has 12 hours before being prompted again.



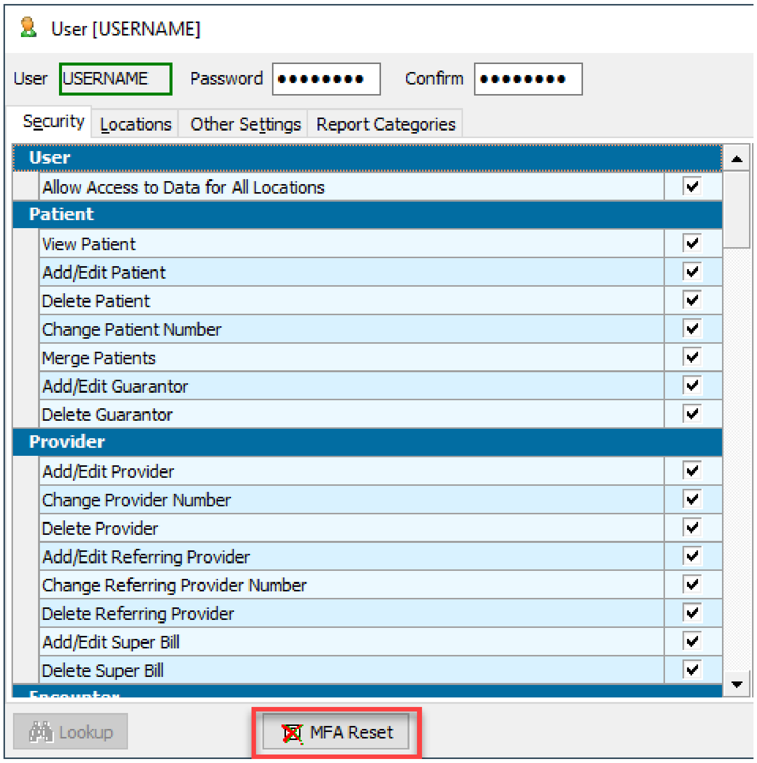
CGM Identity™ Multi-Factor Authentication

Open the authenticator app on your phone and enter the 6-digit security code for ***CGM DAQBilling - Example*** in the field below.

□ Trust this device for 1 week

Input the 6-digit security code:

12. The MFA can be reset in User Settings. Users must have the appropriate permissions to view this screen. Clicking **MFA Reset** will reset MFA for that user.



User [USERNAME]

User USERNAME Password •••••••• Confirm ••••••••

User	
Allow Access to Data for All Locations	☑
Patient	
View Patient	☑
Add/Edit Patient	☑
Delete Patient	☑
Change Patient Number	☑
Merge Patients	☑
Add/Edit Guarantor	☑
Delete Guarantor	☑
Provider	
Add/Edit Provider	☑
Change Provider Number	☑
Delete Provider	☑
Add/Edit Referring Provider	☑
Change Referring Provider Number	☑
Delete Referring Provider	☑
Add/Edit Super Bill	☑
Delete Super Bill	☑
Encounter	