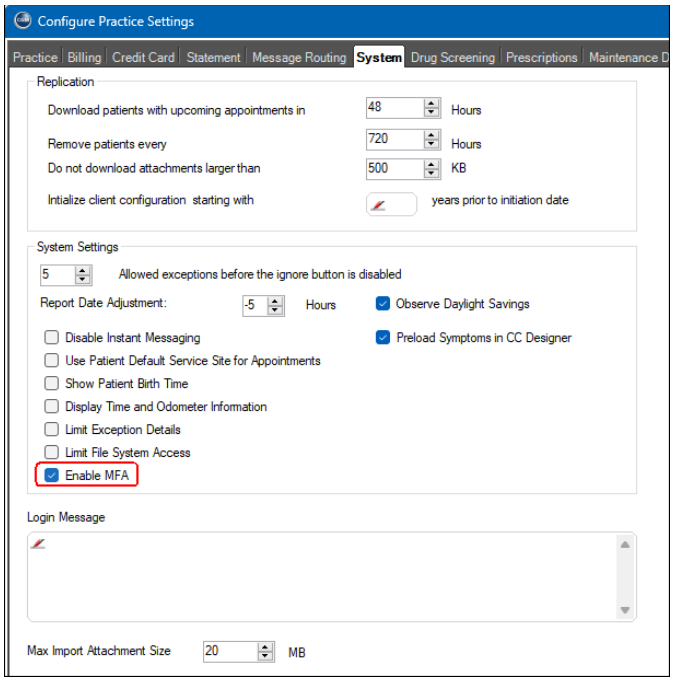
Multifactor Authentication

Multifactor Authentication (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. CGM APRIMA will have MFA disabled by default, and you can enable it by completing the following steps. If your system is hosted, MFA settings will be enabled once you are upgraded to hotfix 1517 and you will not be able to disable those settings.

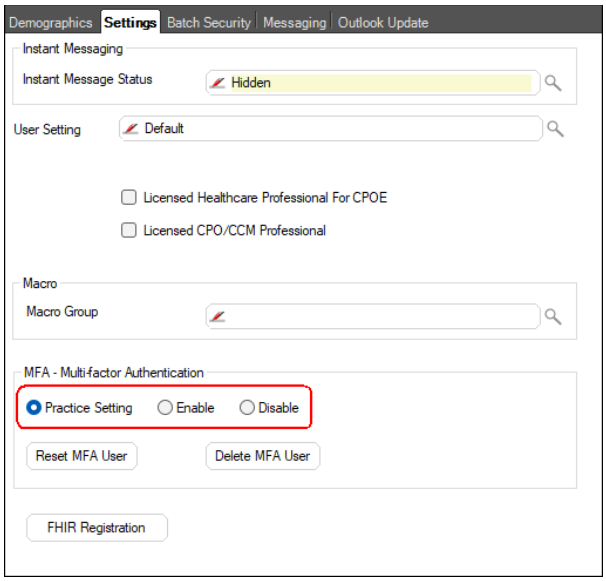
To enable MFA:

1. On the CGM APRIMA homepage navigation bar, select Configure > System Configuration > **Practice Settings**. The Configure Practice Settings window appears.
2. Select the **System** tab.
3. Select the **Enable MFA** check box to turn on MFA for all users at the practice.



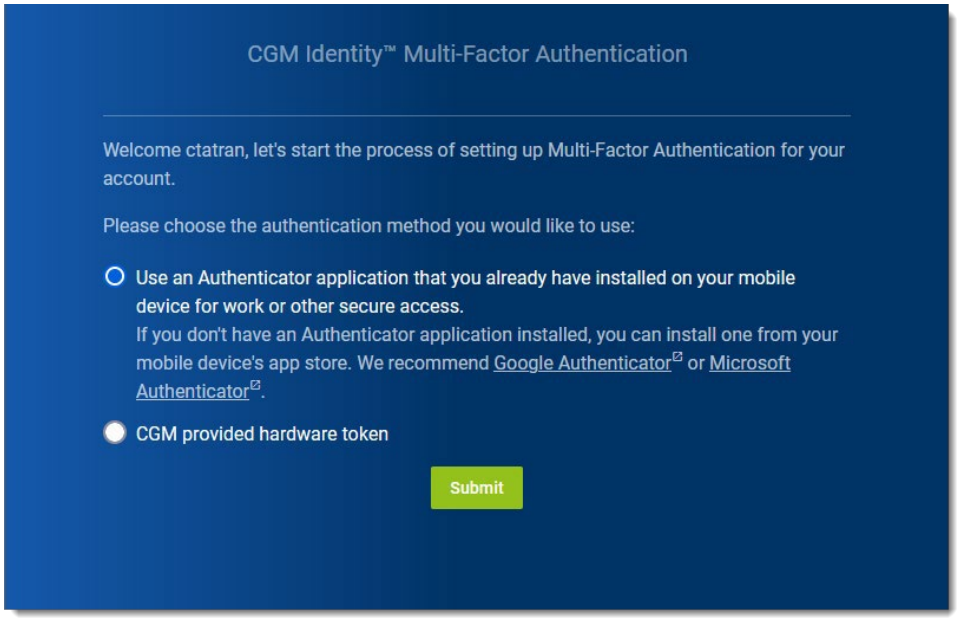
To change a single user's MFA setting:

1. On the CGM APRIMA homepage navigation bar, select Configure > System Configuration > List Editor > System > **User**. Search for and select the desired user. The Modify User window appears.
2. Select the **Settings** tab. In the **MFA – Multifactor Authentication** section, select the appropriate option.
   Practice Setting: The user's MFA will be enabled/disabled based on Practice Settings. This is the default setting for all users.
   Enable: The user's MFA will be enabled. This option overrides Practice Settings.
   Disable: The user's MFA will be disabled. This option overrides Practice Settings.

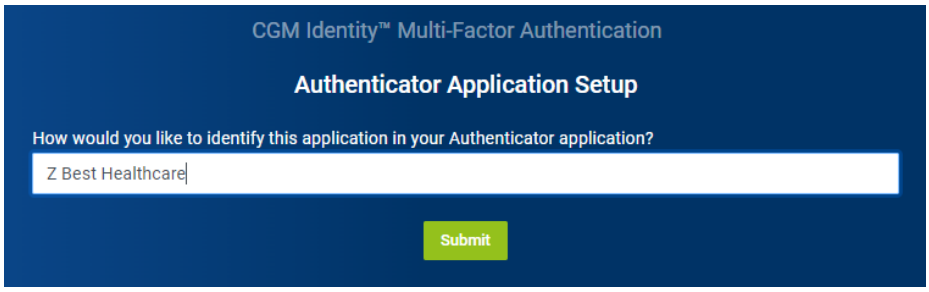


To set up MFA:

1. Enter your username and password for your CGM APRIMA account and click **Login**.
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**. If you are using a hardware token, skip to step 7. To purchase a hardware token if needed, contact your sales team member.



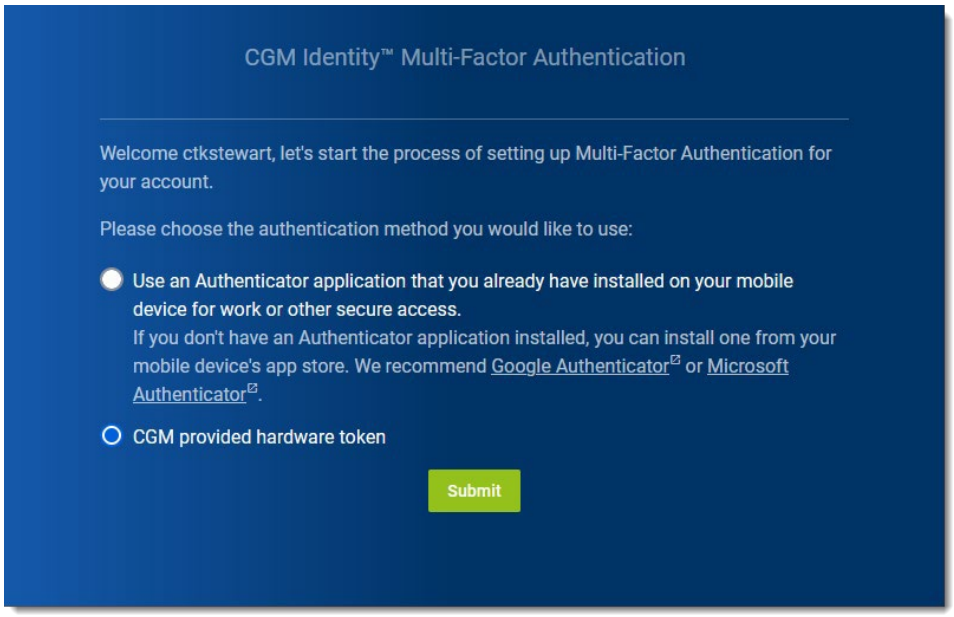
4. Enter a name to be used to identify this application in the Authenticator app. Click **Submit**. The authenticator app login is valid for a 12-hour duration. Once logged in, the MFA will not prompt again for 12 hours.



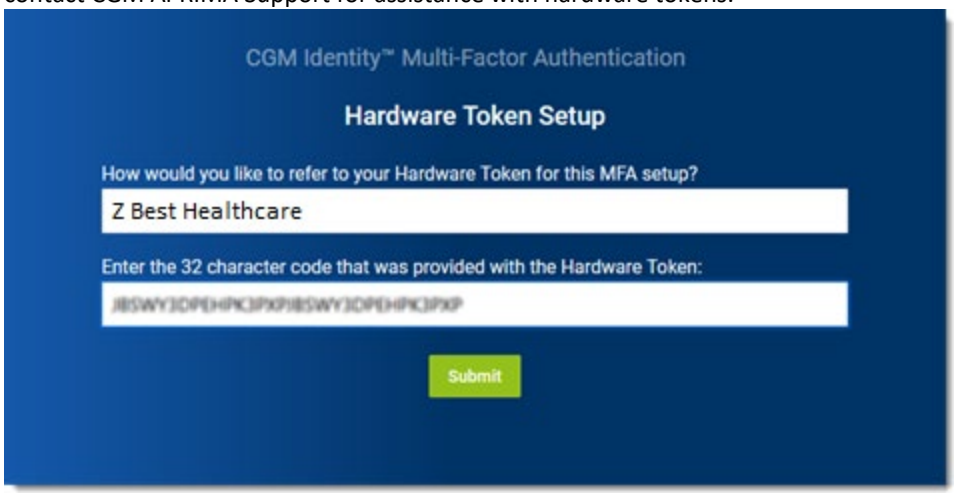
5. Using the authenticator app, scan the QR Code or enter the key shown on the screen. To scan the QR Code, use your mobile device's camera with the QR Code scanner in the authenticator app. This process varies depending on the app in use. Users can also enter the key provided instead of scanning the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

6. Once the QR Code is scanned, the authenticator provides a 6-digit verification code to enter on the Authenticator Application Setup 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.

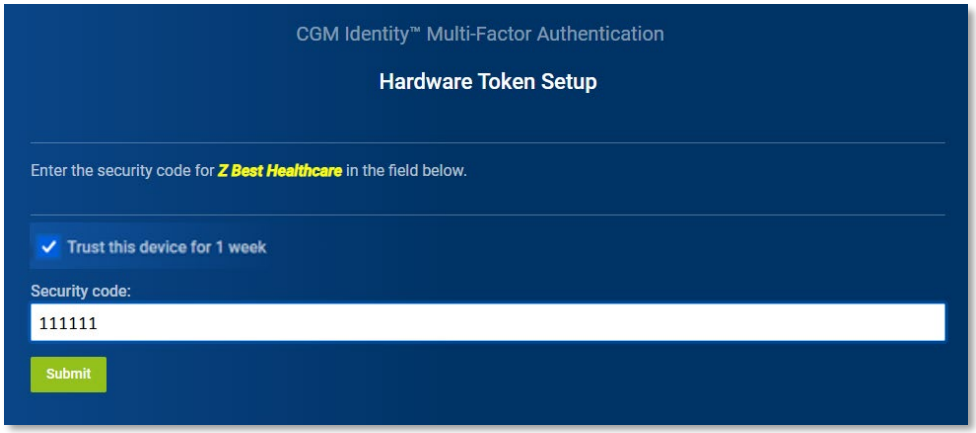
7. If using a CGM hardware token for MFA, select the second radio button and click **Submit**. (If you are interested in purchasing a CGM hardware token, please contact your sales team member.)



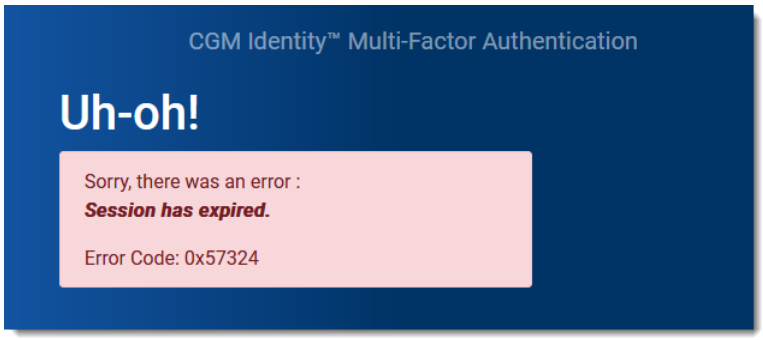
8. Enter a name to identify the Hardware Token for this setup and then enter the 32-character code for the hardware token. Please contact CGM APRIMA Support for assistance with hardware tokens.



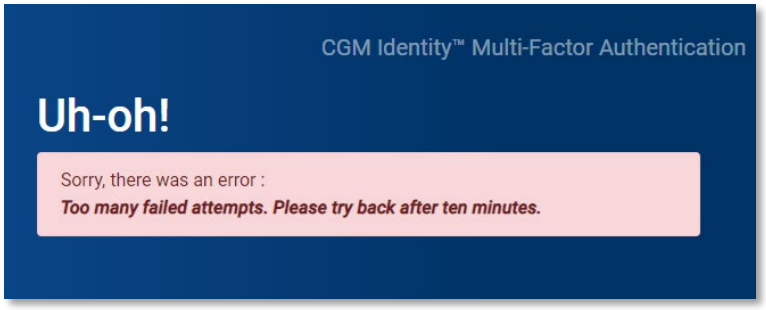
9. Select **Trust this device for 1 week** to avoid entering the 6-digit code for one week after initial MFA setup. Enter the 6-digit code provided by the hardware token and click **Submit**.



10. If the following session expiration message displays, please try to login to CGM APRIMA again.



11. If there are too many failed attempts to authenticate, then an error will display. The account will be locked for 10 minutes before the user can attempt again.



12. After the MFA setup is successful, if the **Trust this device for 1 week** box was left unchecked, the user has 12 hours before being prompted again to enter their 6-digit code.

13. The user's MFA setup can be reset User Settings. In the **Settings** tab, click the **Reset MFA User** button to reset the user's MFA settings in Identity. The user then will have to set up their MFA Authenticator next time they log in to CGM APRIMA.
***Note**: If a user gets locked out of their account by entering too many incorrect MFA 6-digit codes, do not use the **Reset MFA User** option because it will force the user to re-create their entire MFA account. Instead, the user should wait 10 minutes and try again.*
You also can remove the user from Identity completely by clicking the **Delete MFA User** button.