Multi-Factor Authentication

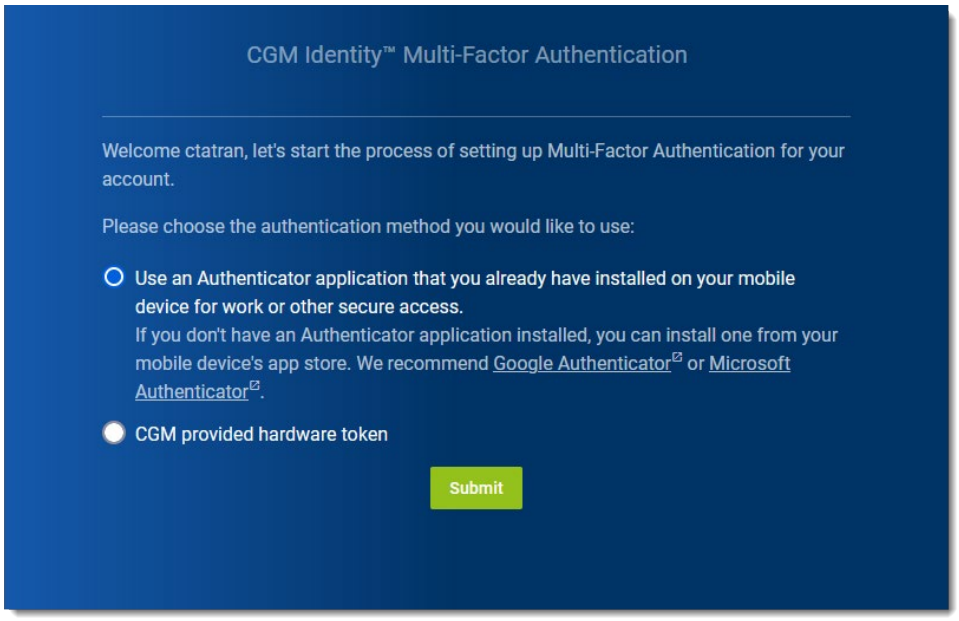
Multi-Factor Authentication (MFA) will be required for eMEDIX Online. MFA is a multi-step account login process that requires users to authenticate their account with more than just a password. Users can use an Authenticator application such as Google Authenticator or Microsoft Authenticator.

Note: *Please verify that all pop-up blockers are turned off or you allow pop-ups from https://online.emedixus.com. If neither are true, a warning message displays indicating pop-ups are blocked and the login/MFA cannot proceed until corrected.*

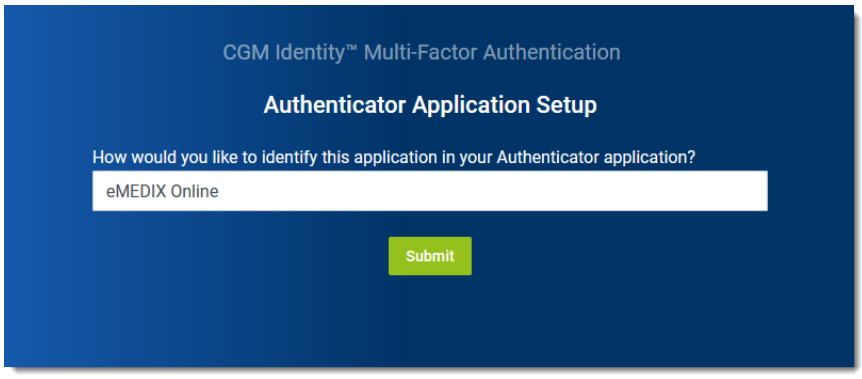
To set up Multi-Factor Authentication:

1. Enter your username and password associated with the eMEDIX Online account and click **Sign In**.
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.

   Note: *If a user attempts to login without using an authentication method, the system will continue to prompt for authentication. Exit completely out of the browser to escape.*
3. If using the Authenticator app for MFA, select the first radio button and click **Submit**.

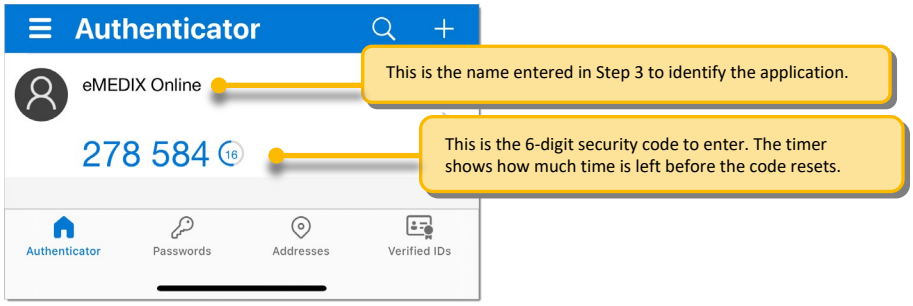


4. Enter a name to be used to identify this application in the Authenticator app. Click **Submit**.

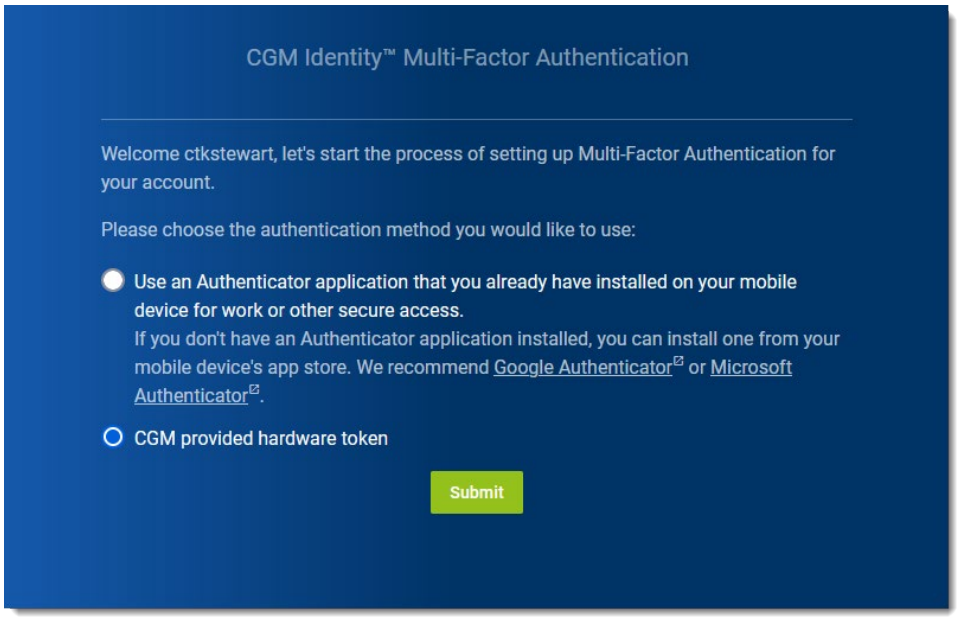


5. Using the authenticator app, scan the QR Code or enter the key shown on the screen. To scan the QR Code, use your mobile device's camera with the QR Code scanner in the authenticator app. This process varies depending on the app in use. Users can also enter the key provided instead of scanning the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

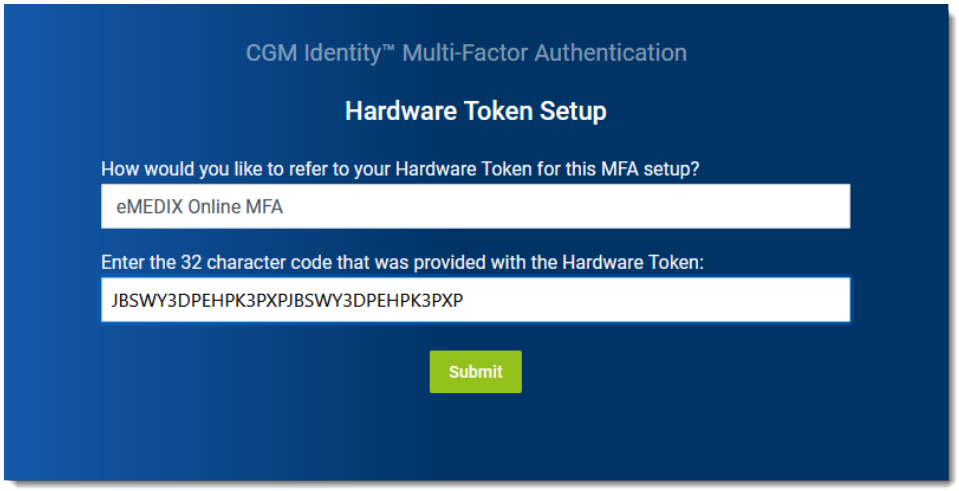
6. Once the QR Code is scanned, the authenticator provides a 6-digit verification code to enter on the eMEDIX Online authentication screen. The following example is from Microsoft Authenticator. The app gives the user 30 seconds to use the code before resetting to a new code. Enter the code on the eMEDIX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



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.)

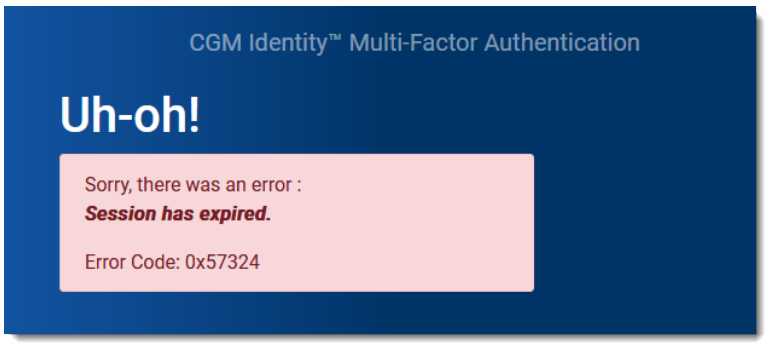


8. Enter a name to identify the Hardware Token for this setup and then enter the 32-character code for the hardware token. Please contact eMEDIX Support for assistance with hardware tokens.

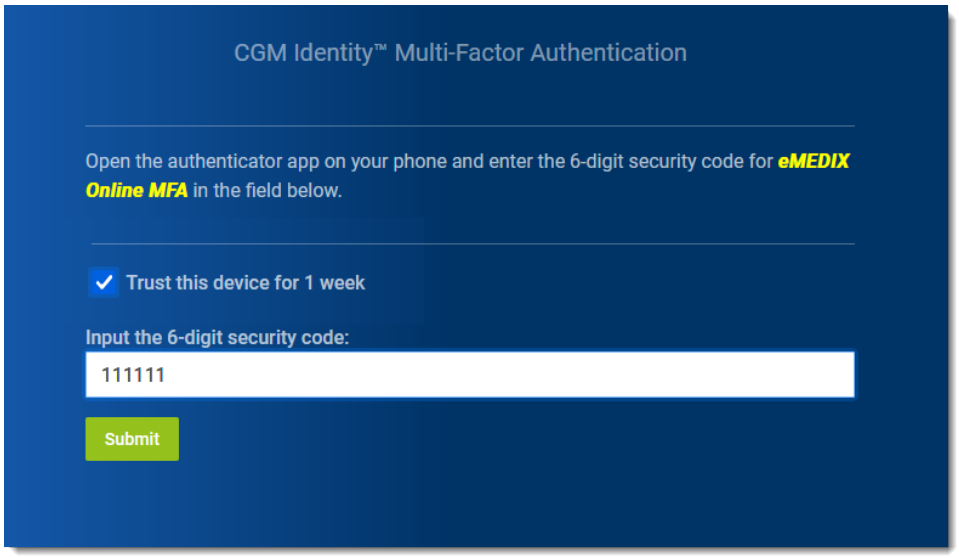


9. If the verification code is correct, the user will be logged into the account. If a user attempts to login without using an authentication method, the system will continue to prompt for authentication. Exit completely out of the browser to escape.

10. If the following session expiration message displays, please try to set up the MFA again.



11. After initial setup, when the user attempts to log into eMEDIX Online, 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.



Note: *The Trust this Device option stores a cookie on the user's browser for the last login session. The session stores details about the device/browser and the originating IP address. If either of these things change, the user will be prompted for MFA again. (For example, the user logs in from a home IP address and marks the Trust this Device check mark. The following day, the user logs in from their office IP address. Because the IP address changed, the user is prompted for MFA again.)*

12. The MFA can be reset in User Admin. Users must have the appropriate permissions to view this screen. Please see the User Admin section in Online help for more information.