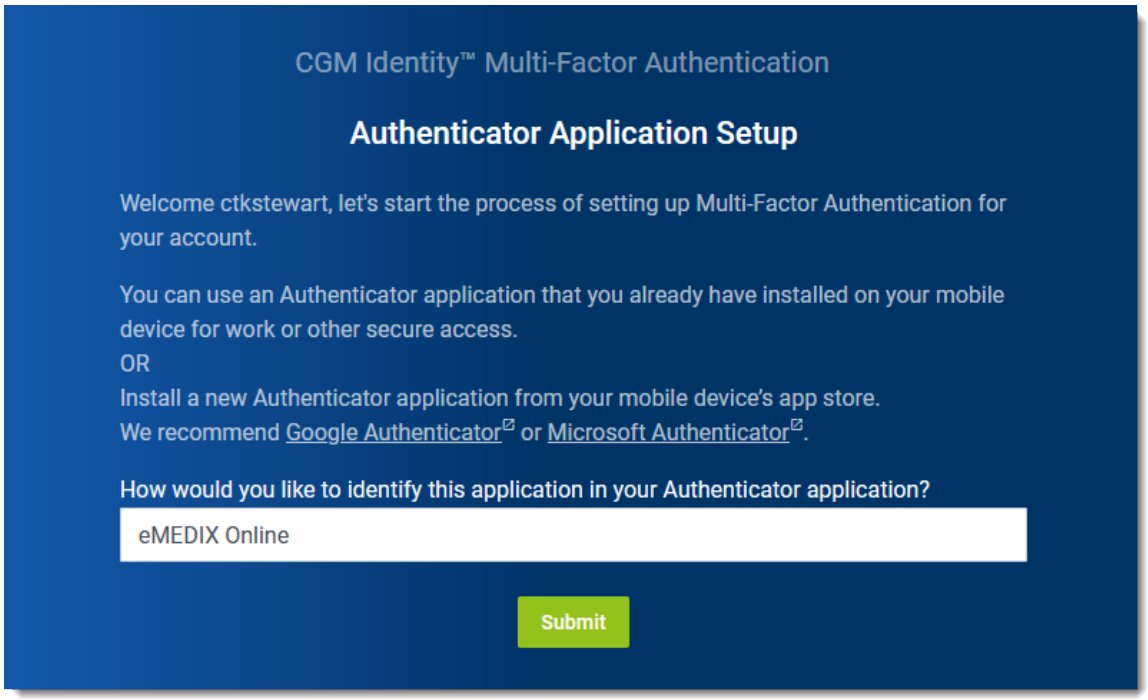
Multi-Factor Authentication

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.*

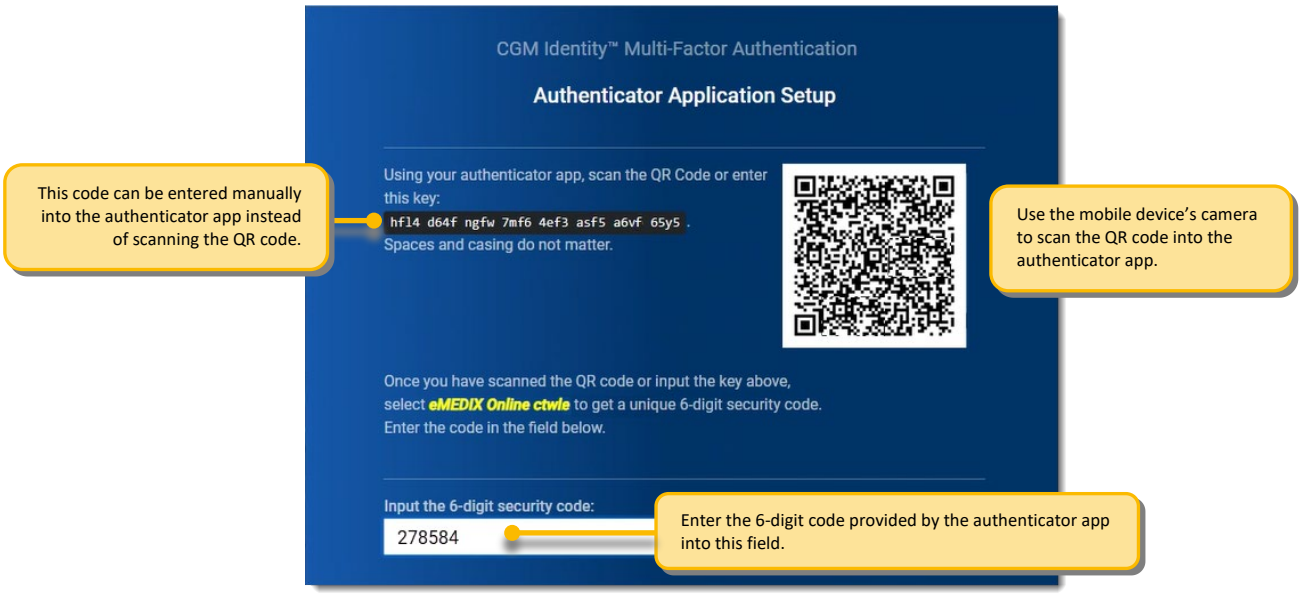
To set up Multi-Factor Authentication:

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. A prompt displays asking how to identify this application in the Authenticator app. Enter the desired name in the blank field and 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.

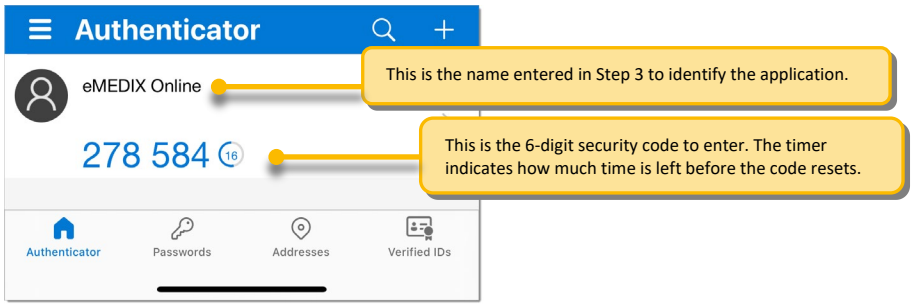


Note: *If a user attempts to login without using an authentication method, the system will continue to prompt for authentication. Exit completely out of the browser to escape.*

3. Using the authenticator app, scan the QR Code or enter the key indicated 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.

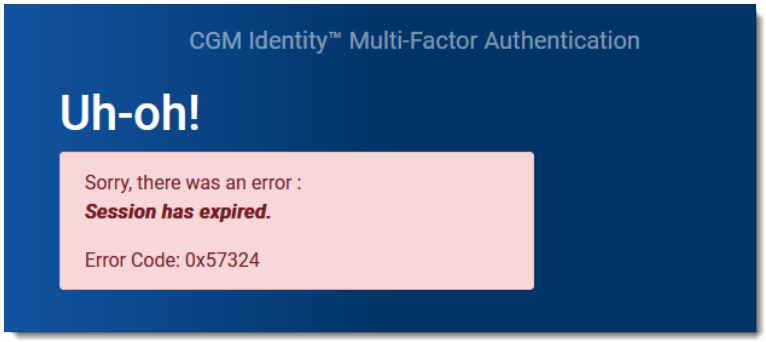


4. Once the QR Code is scanned, the authenticator provides a 6-digit verification code to enter on the eMEDIX Online authentication screen. The following example is from Microsoft Authenticator. The app gives the user 30 seconds to use the code before resetting to a new code. Enter the code on the eMEDIX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



5. 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.

6. If the following session expiration message displays, please attempt to set up the MFA again.



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