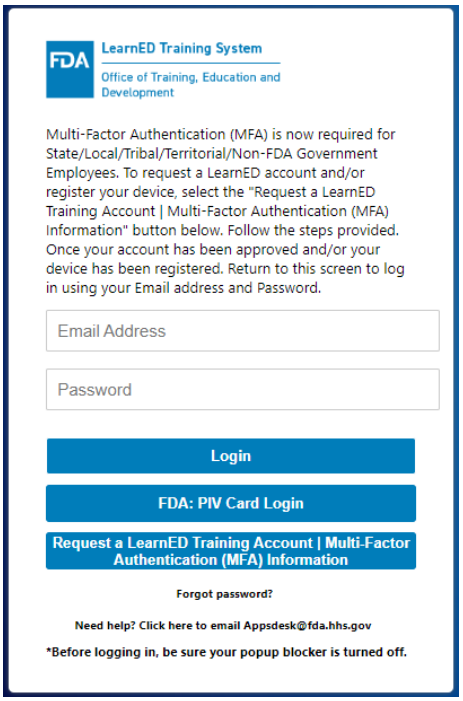
Multi-factor Authentication User Guide

Multi-factor Authentication (MFA) is a security mechanism to build stronger authentication into the LearnED LMS standard login process. Non-FDA Users who are required to log in with MFA must use a mobile device, such as a smartphone, with a virtual authenticator app. Examples of suggested Authenticator Apps are Google Authenticator and Microsoft Authenticator. Though Google and Microsoft Authenticators are suggested and supported by the HelpDesk Administrators, there are several available Authentication apps in app stores which can be found here: [Multi-Factor Authentication (MFA) Apps]

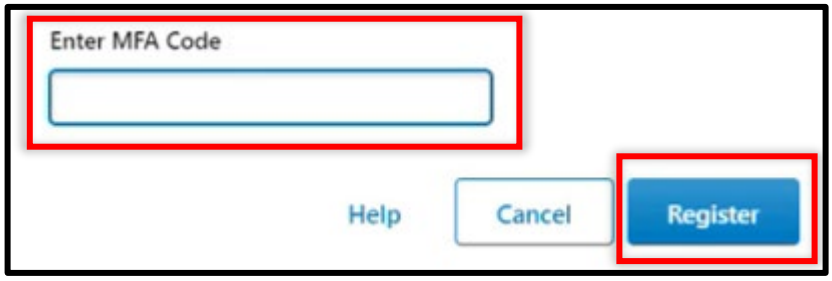
Upon your next log in, you will be required to register your device by following these steps.

1) Access the LearnED LMS as normal and enter your regular username and password.



2) On your smartphone, open your virtual authenticator app.
3) In the app, select the option to add an account or scan a QR code.
4) Use your smartphone's camera to scan the QR code on your computer screen. The app will automatically recognize the code and add the account.

5) After adding the account to your virtual authenticator app, the app will generate a one-time code. Enter this code into the Cornerstone MFA page and click Register.



6) Once verified, your MFA device is active. Now, each time you log in to your account, you must open your virtual authenticator app to generate a temporary code to complete the login process.