MCCMH Multi-Factor Authentication
Updated 2026-11-02

MCCMH has implemented changes to Multi-Factor Authentication (MFA) in anticipation of the release of the new HIPAA final rule which strengthens the requirements for MFA in environments that handle Protected Health Information (PHI).

Additionally, CareConnect 360 (CC360) API access has been integrated directly into FOCUS, and MFA is a requirement for accounts accessing this integration. Previously, CareConnect 360 access required creating a login in the MILOGIN system and requesting access.

MFA will be required every 24 hours if the box to "Trust this device for the next 24 hours is checked". Otherwise, you will be required to enter your authentication code at every login.

MFA Setup Instructions (FOCUS):

How to Setup Two-Factor Authentication Device

Users who login to the system from outside of an approved network may be prompted to enter both their system password and a token ID as a second layer of authentication.

To Setup the Authenticator App on your Mobile Phone

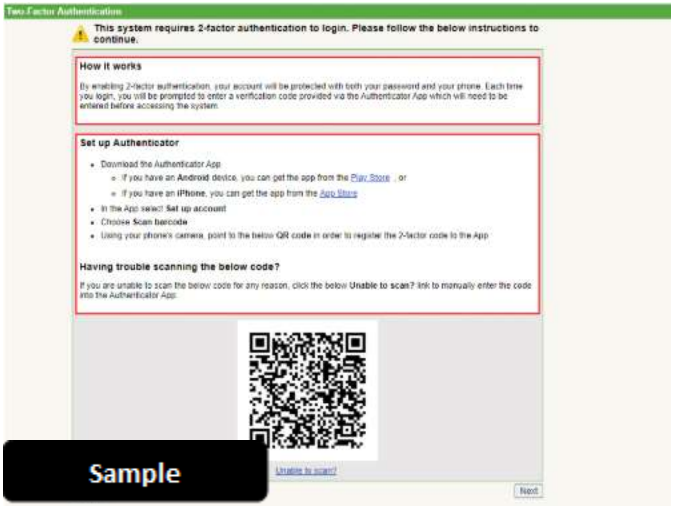
1. Install the *Microsoft Authenticator* application from your mobile phone's app store. The app is free to use.



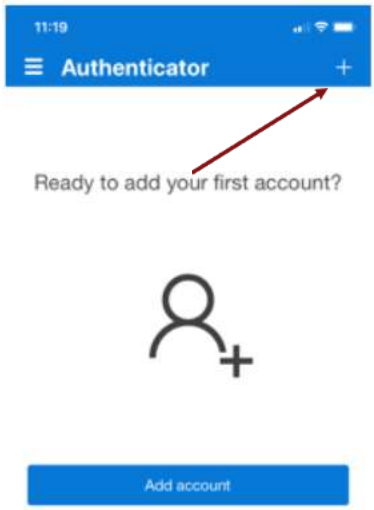
2. Go to the system login screen and enter your user ID and password.



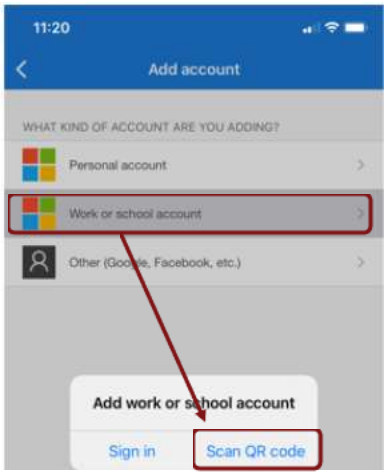
3. If you are outside of the approved networks and/or are logging into the system for the first time, you may receive the following screen after entering your password.



4. **Open the Microsoft Authenticator app on your mobile phone** and click “Scan QR Code” or click the “+ Plus” sign to Add Account.



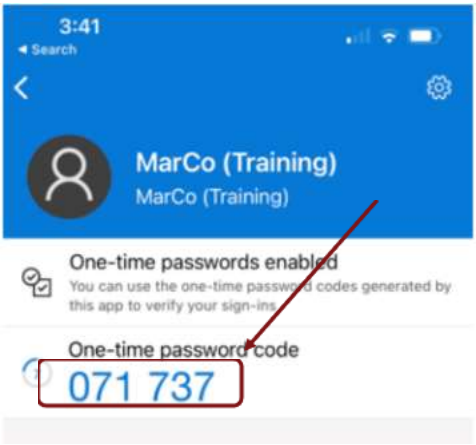
5. If prompted to select account type, select “Work or school account” and then “Scan QR Code”.

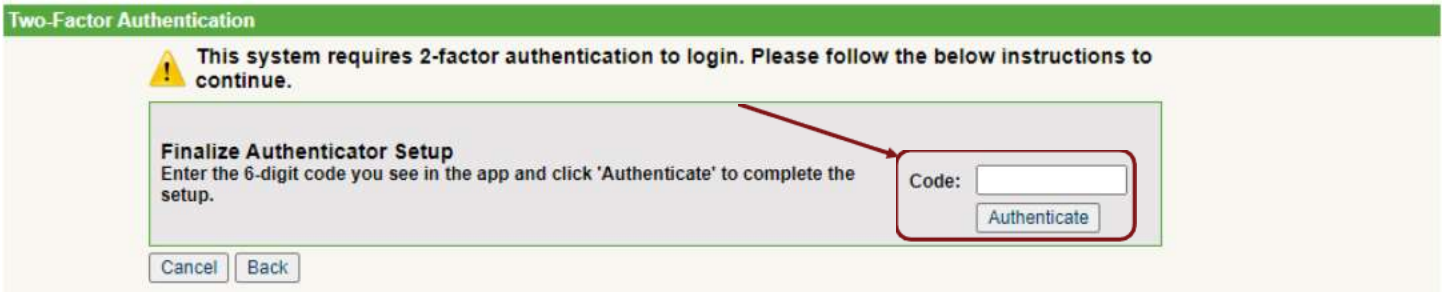


6. If prompted to allow access to the camera, click “OK”.
7. Hold the camera up to take a picture of the QR code that appears on the screen.
8. After scanning the QR code, click “Next” in the system.



9. Enter the 6-digit code that appears on the app into the “Code” field in PCE and click “Authenticate”.





10. You will receive the following confirmation screen. Click “Continue”.



11. You will now be logged into the system.
12. When you login to the system in the future, you’ll be asked to enter the 6-digit code from the Authenticator app after you enter your system password. Type the code when prompted to complete your login.
13. Authentication will be required only every 24 hours if the box to “Trust this device for the next 24 hours is checked”. Otherwise, you will be required to enter your authentication code at every login.

