



Multi-Factor Authentication Instructions

06 August 2026 - Microsoft Authenticator app required to verify user identity through MFA when signing in to the CMMI website and CMMI Model Viewer.

To protect your CMMI account and the security of our platforms, we are introducing mandatory multi-factor authentication (MFA).

These instructions show the basic steps to install Microsoft Authenticator and register your CMMI account for MFA. If your account portal prompts you, follow the portal's on-screen guidance to begin enrollment.

1. Install Microsoft Authenticator

- iPhone/iPad: [Download from the App store](#)
- Android device: [Download from Google Play store](#)

2. Begin enrollment from the CMMI sign-in portal

- Sign in to the [CMMI Website](#) as you normally do.
- You will be prompted to set up MFA or add a security method.
- The portal will display a QR code (or a code to enter manually).

3. Add your account to Microsoft Authenticator

- Open the Microsoft Authenticator app on your device.
- If prompted, allow notifications.
- Tap **Add account** (or the + icon) and select the relevant account.
- Use the app to scan the QR code shown. If you cannot scan, choose the manual entry option and enter the code provided.

4. Complete verification

- After scanning the QR code, the portal may prompt a test notification or request a one-time code from the app.
- Approve the notification in the app or enter the one-time code displayed by the app to confirm the enrollment.

5. Test your sign in.

- Sign out, and sign back in to confirm that MFA is working.
- When prompted, approve the sign-in request in the Microsoft Authenticator app or enter a one-time code from the app.



Microsoft resources

- [How Microsoft MFA works](#)
- [Authenticator how-to and troubleshooting](#)



Need assistance?

If you have questions, need help, lose your authentication device or are unable to sign in. **Please contact our Support Desk immediately.**

Call: +1-847-660-5505 or
+1-855-549-2047 (toll free)

Web: [ISACA Support](#)



Account safety

Do not share authentication codes or device details with anyone other than authorized support personnel.

Sharing of CMMI login credentials is prohibited and may result in termination of any user licenses or agreements as per [CMMI Institute's Corrective Action Policy](#).

We appreciate your cooperation as we implement this important security improvement.