**UMass Boston Multi-Factor Authentication**

**Methods of Multi-Factor Authentication**

**Duo Push via mobile device (recommended)**
1. Select “Send Me a Push”
2. You can press and approve the notification from device’s locked screen or proceed to step 3
3. Open the Duo Mobile application on your enrolled device
4. Tap on the “1 Request waiting. Tap to Respond…” notification, tap “Approve”
5. Then return to the screen that you had open in step 1, and you should be logged in

**NOTE:** If you receive a login request that you have not initiated, select “Deny”

**Call Me via mobile phone or landline**
1. Select “Call Me.”
2. You will receive a phone call on your enrolled phone
3. You will hear an automated message starting with “Welcome to UMass Boston Duo Security”, press 9 to login
4. Then return to the web browser you opened in step 1, and you should be logged in

**NOTE:** If you receive a login request that you have not initiated, press 7 to report fraud

**Passcode via mobile device - using Duo Mobile app**
1. Select “Enter a Passcode”
2. Open the Duo Mobile application on your mobile device
3. Tap the key icon to get a 6-digit passcode
4. Return to the web browser and enter the passcode at the Duo prompt
5. Click login, and you should be logged in

**NOTE:** Duo Mobile Passcodes can be used even if you do not have internet or cellular network

**Passcode via mobile device - using text message (SMS)**
1. Select “Enter a Passcode”
2. Then select “Text me new codes” at the bottom of the Duo prompt
3. You will receive a 7-digit passcode via a free text on your enrolled MFA device
4. Return to the screen you had open in step 1
5. Input the passcode you received as text, click login and you should be logged in

**NOTE:** Open the text to reveal the 7-digit code. Text passcodes expire in 2 minutes.