Multi-Factor Authentication Setup

Before you start, please install the Microsoft Authenticator mobile app from the Apple or Android store. Also, this documentation will only work once IT has enabled your account for MFA. If there are any questions, please contact TechSupport at techsupport@westernu.edu or (909) 469-5432

1. Navigate to https://go.westernu.edu and login using your WesternU credentials.
2. Once authenticated you will be prompted to further verify your account.

![Western University of Health Sciences](https://example.com)

For added security, we need to further verify your account

mfa-test1@westernu.edu

Your admin has required that you set up this account for additional security verification.

Set it up now

3. Click the Set it up now button.

   NOTE: The recommended method for contact will be as follows. However, any combination of second factor authentication will be sufficient and it can always be modified later.

4. On the Additional security verification screen under step 1, change the first dropdown box to Mobile App, and select the first radio button for Receive notifications for verification.

![Additional security verification](https://example.com)

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

- Mobile app

   How do you want to use the mobile app?
   - Receive notifications for verification
   - Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up

5. Click the Set up button
6. Follow the instructions in the *Configure mobile app* dialog window, installing the **Microsoft Authenticator** from either the Apple or Android mobile store.

![Configure mobile app dialog window](image)

7. Once you have installed the app, and followed the on-screen instructions to add an account and scanned the QR code, you will see that the account has been added to your mobile app.

![Mobile app account](image)

8. On the *Configure mobile app* dialog window, click the **next** button.

9. Now that the mobile app has been configured, on your computer you can select **Next** on the *Additional security verification* window for Step 1.

   **NOTE:** There is a timeout involved with the setup and configuration of the mobile app. If time runs out you may see a message that the configuration has failed. If so, remove the account from the Microsoft Authenticator app and run through the setup again.

10. In Step 2, your mobile app will be tested to verify that the configuration is working. You will be sent a push notification to the Microsoft Authenticator app, in the dialog box click **Approve** on your mobile device.

   ![Approve sign-in?](image)

11. In Step 3, now that the mobile app has been configured and tested, you will be prompted for your mobile phone number in case you lose access to the mobile app. In the dropdown box, select **United States (+1)** and then **enter your mobile number** in the adjacent text field. Click the **Next** button.

12. In Step 4, you will be asked to save an “app password”. This is not required at this time and new app passwords can be generated later as needed for applications that do not support Multi-factor authentication. You can click the **Done** button.

13. You have successfully configured MFA! To review your settings, change your default options, or generate additional app passwords you can navigate here: [https://go.westernu.edu/MFASetup](https://go.westernu.edu/MFASetup)