Set Up Microsoft Authenticator

Use this guide to install Microsoft Authenticator and register it as a sign-in method for your Penn Medicine account. Before you begin, have your mobile device, Penn Medicine email address, and current multi-factor authentication method available.

1. Install Microsoft Authenticator

If you already have the Microsoft Authenticator app installed, proceed to Step 2: Register Microsoft Authenticator.

1.1. **Company-issued devices:** Microsoft Authenticator is pre-installed. Proceed to Step 2.
1.2. **Personal devices with Company Portal**: Download Microsoft Authenticator from Company Portal.
1.3. **Personal devices without Company Portal:** Download Microsoft Authenticator from your device's app store:

iPhone/iPad: Apple App Store

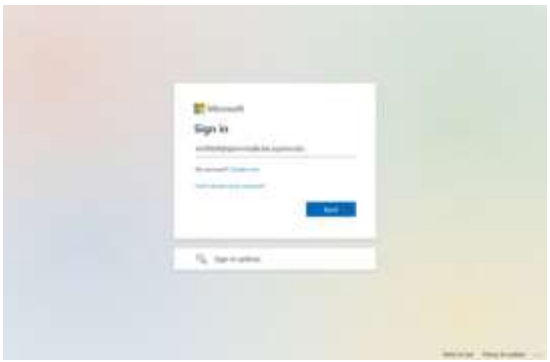
Android: Google Play Store

1.4. Follow the onscreen directions to download and install the Authenticator app.

Important: If you are replacing or upgrading your phone, set up Microsoft Authenticator on your new device before erasing your old device. If you erase your old device first, you may lose access to your account.

2. Register Microsoft Authenticator for your Penn Medicine account

2.1. On a computer, open a browser and go to https://aka.ms/mysecurityinfo. Sign in when prompted. If you see a prompt to keep your account secure, follow the prompts to continue setting up Microsoft Authenticator.
2.2. Sign in with your Penn Medicine email address, such as **my.email@pennmedicine.upenn.edu**.
Select **Next**, enter your password, and then select **Sign in**.





2.3. You may be prompted to approve the sign-in using Duo. If you no longer have Duo, or if Authenticator was only installed on an old device that has been erased, submit a support ticket to request a Temporary Access Pass (TAP). A TAP is a short-term code that allows you to sign in and add a new authentication method.
- If you see the **"Let's keep your account secure"** screen, select **Next**.
- If you are already on the **Security Info** page, select **Add sign-in method**.
- From the drop-down menu, select **Microsoft Authenticator**, then select **Add**.
- Select **Next** until a QR code is displayed on your computer screen.

2.4. Open the **Microsoft Authenticator** app on your mobile device.

2.5. If prompted, accept the privacy notice and continue through any app setup or improvement prompts.

2.6. If prompted to add a personal Microsoft account, select **Skip** or continue until you reach the main Authenticator screen.

2.7. Tap the **+ (plus)** icon to add an account. **Note: If this is your first time opening the app, the account-add workflow may start automatically.**

2.8. Select **Work or School Account**.

2.9. Select **Scan QR Code**.

2.10. When prompted, allow Authenticator to access your device's camera.

2.11. Point your phone's camera at the QR code displayed on your computer screen.

2.12. After the QR code is scanned, Microsoft Authenticator will ask you to complete number matching to verify the setup.

2.13. On your computer screen, a unique number will be displayed.

2.13.1. Enter the number displayed on your computer screen into your phone.

2.13.2. Select **Yes** or Approve to complete the verification.

2.13.3. Return to your computer and select **Next**.

2.14. A "**Success**!" message should appear. Select Done to complete the setup.

3. Troubleshooting

- If the QR code times out, select **Back** and then **Next** to generate a new QR code.
- If you receive a message indicating that the QR code has already been used, select **Cancel** and start the process again.

- If issues persist, close the browser, reopen https://aka.ms/mysecurityinfo, and restart the registration process. If you still cannot complete setup, contact the Service Desk for assistance.

If you do not receive the notification

- Open the Microsoft Authenticator app manually and check for the approval request.
- If no request appears, wait for the challenge to time out and request a new notification.
- Verify that notifications are enabled for Microsoft Authenticator.
- If your device uses **Do Not Disturb**, **Focus**, or **Work Profile** settings, add Microsoft Authenticator as an allowed application to ensure notifications are delivered.

4. Setup complete

Microsoft Authenticator is now registered as a sign-in method for your Penn Medicine account and can be used for future multi-factor authentication requests. **Do not uninstall Duo until you are notified that your apps no longer require it.**

---------- *[End of Document]* ----------