Microsoft Authenticator App, the fastest way to login.

Use Microsoft Authenticator to setup password-less sign-in. No more getting a phone call, or receiving a text code to sign-in!

Available on most major devices.

<table>
<thead>
<tr>
<th>Apple App Store</th>
<th>Google Play Store</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="App Store" /></td>
<td><img src="image" alt="Google Play" /></td>
</tr>
</tbody>
</table>

Do I Need a Working Phone Number to Use the Authenticator App?

No, once set up you can authenticate without the need for WIFI or mobile data. However, we recommend having a working phone number as backup.

Alternate Login Methods Using the App

1. **One-Time Password (OTP):**
   a. You can open the Authenticator app to receive a randomly generated 6 digit OTP code.
   i. These codes can be used when completely offline. No Wifi or mobile data connection needed.

2. **Push Authentications:**
   a. The apps receives a push notification via cell or Wi-Fi, when you are logging on. Simply hit approve or allow on the app.
   i. Note: if you are not expecting a push or not trying to log on at that time DO NOT approve.

   **Important Change Coming**
   To combat MFA fatigue, Millersville University will be switching from simple push notification to number matching.
   If you are using **phone sign-in** aka "password-less" then you are already using number matching, and this will not affect you. Scroll down to learn more about **phone sign-in**.
   Learn more here: [Defend your users from MFA fatigue attacks - Microsoft Community Hub](#)

3. **Password-less:**
   a. Passwords are not being eliminated anytime in the near future, but you can use them "less" often thus "password-less"
   b. This is still MFA
   i. The first authentication factor, is a two digit code you enter in the app.
      1. Random every time.
      2. This is called "number matching"
   ii. The second authentication factor is however you currently unlock your phone.
      1. PIN, FacetID, FingerID
      2. You must have your phone on you.
         a. Please watch video to see what to expect once properly set up.
         b. Your phone must have a PIN or lock on it to qualify.

How to Setup Password-less Sign-in on the App
Here is a video of how to setup the app.

Detailed instructions:

1. Get the Microsoft Authenticator App for your smartphone.
2. Set up the Microsoft Authenticator app to send notifications
   a. Be sure to set it to “Receive notifications for verification”
   b. Once set up “Enable phone sign-in”
   c. You will be asked to “register” your device. Please do so.
      i. This does not give Millersville nor Microsoft access to anything on your device.
3. Go Password-less (Phone Sign-In)
   a. This is easiest by using a computer or laptop to browse, rather than using the mobile device where the Authenticator App is installed.
4. Enter your Millersville’s email address and click “Next”.
5. On the password screen click “Use an app instead.”
8. In your browser you will receive your first factor.

9. Open the Microsoft Authenticator App on your phone. The App will display a keypad to enter the code. We highly recommend you allow notifications on your mobile device to make this easy.
10. Enter the same number that is displayed in your browser. (81 in our example)  
   a. Note: These will expire in about 30 seconds.
11. You will now be prompted for the second factor. You can use any of the following that you currently have setup for unlocking your mobile device.  
   i. FaceID (Biometric)  
   ii. FingerID (Biometric)  
   iii. PIN for that device  
12. Congratulations!! You are now logged into your account