Microsoft Authenticator App

Use Microsoft Authenticator for easy, secure sign-ins for all your online accounts using multi-factor authentication, passwordless, or password autofill. You also have additional account management options for your Microsoft personal, work or school accounts.

Available on most major devices.

<table>
<thead>
<tr>
<th>Apple App Store</th>
<th>Google Play Store</th>
<th>Microsoft Store (For Windows Phone)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://via.placeholder.com/150" alt="App Store" /></td>
<td><img src="https://via.placeholder.com/150" alt="Google Play" /></td>
<td><img src="https://via.placeholder.com/150" alt="Microsoft Store" /></td>
</tr>
</tbody>
</table>

What is multifactor authentication (MFA)?

Multifactor authentication (MFA) adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.

It’s more secure than passwords?

In most identity attacks, it doesn’t matter how long or complex your passwords are.

Watch the webinar

How to go Passwordless.

Going passwordless is the next generation of account security. **Simple, fast, secure.**

- Get the Microsoft Authenticator App for your smartphone.
- Set up the Microsoft Authenticator app to send notifications
  - Be sure to set it to "Receive notifications for verification"
  - Once set up “Enable phone sign-in”
• Go Passwordless
  • This is easiest by using a computer or laptop to browse, rather than using the mobile device where the Authenticator App is installed.
  • In an in-private or incognito windows browse to office.com
  • Enter your Millersville’s email address and click "Next":
    • This is your official User Principal Name (UPN) and not any simpler email alias you may have.

• On the password screen click "Use an app instead."

• In your browser you will receive your first challenge or factor.
At the same time the Microsoft Authenticator App will display three choices. We highly recommend you allow notifications on your mobile device to make this easy.

- Select the same number that is displayed in your browser. (81 in our example)
- Note: These will expire in about 30 seconds.
  - One of the reasons it's so secure.

Congratulations! You just completed the first challenge.

The second challenge or factor is one of the following on your mobile device.
- FaceID (Biometric) something you are.
- FingerID (Biometric) something you are.
- PIN for that device
  - While something you know, device must be in hand so something you have.

Congratulations!! You just completed the second factor (2FA) or multi-factor (MFA)

- You never entered a password!
Simple, fast, secure.

Change is hard

I do not like **Simple, fast, & secure** logons and wish to return to a texted based password; that is stored on a server I have no control over and hope it is never compromised; I prefer to transmit my password over the Internet every time I logon.

I really should [watch the webinar](#) and learn why passwords are no longer secure.

To do this simply select "Use your password instead."

---

[Image: Millersville University sign in page]

[Image: Use your password instead]