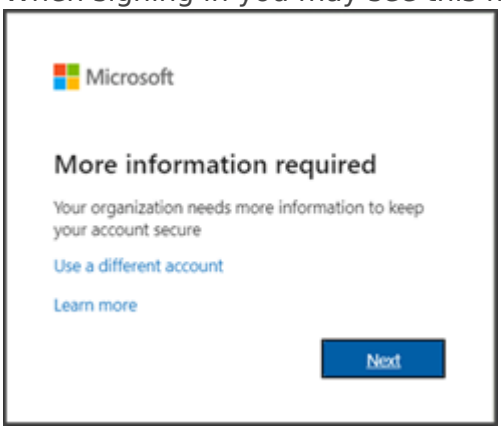
Multi-Factor Authentication (MFA)

This guide provides step-by-step instructions for users on how to reset their multi-factor authentication (MFA) using the Microsoft Authenticator app. It offers a user-friendly walkthrough, ensuring a seamless and secure process to regain access to their accounts while maintaining the highest level of security.

Setting Up MFA

When signing in you may see this message.



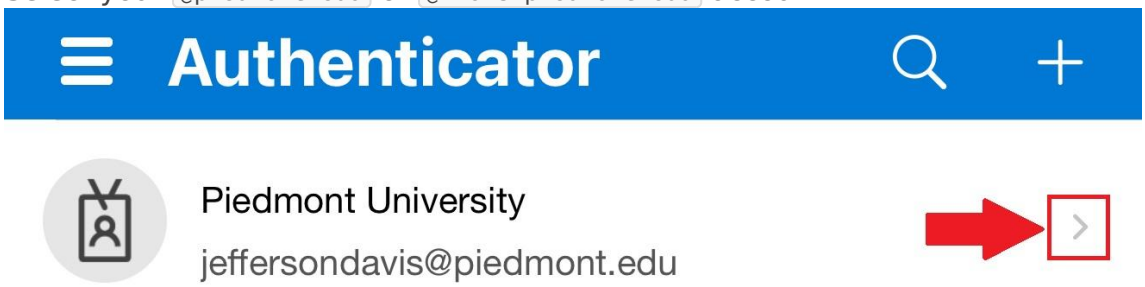
This message indicates that you must reconfigure your Multi-Factor Authentication. Follow through the on-screen prompts until you reach a page with a QR Code

Once you reach this page, please proceed to the next steps on your **mobile device**.

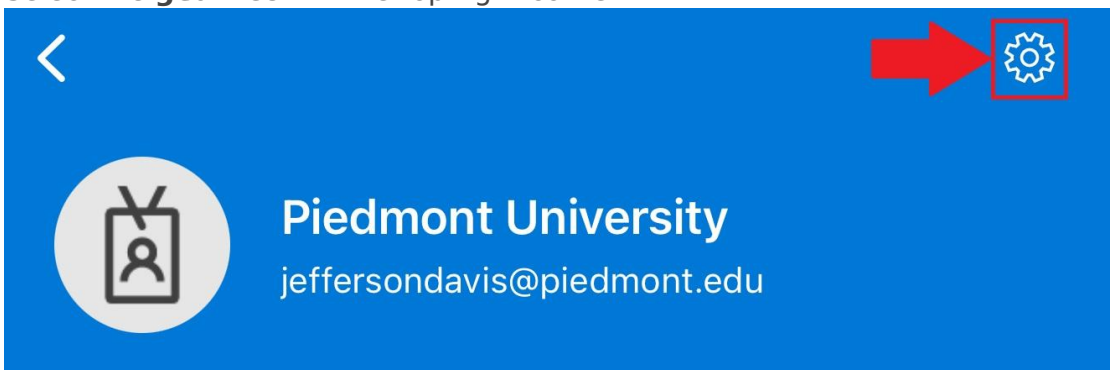
Delete previous sign-in method

> This section is only necessary if you have **previously set up Microsoft Authenticator**.

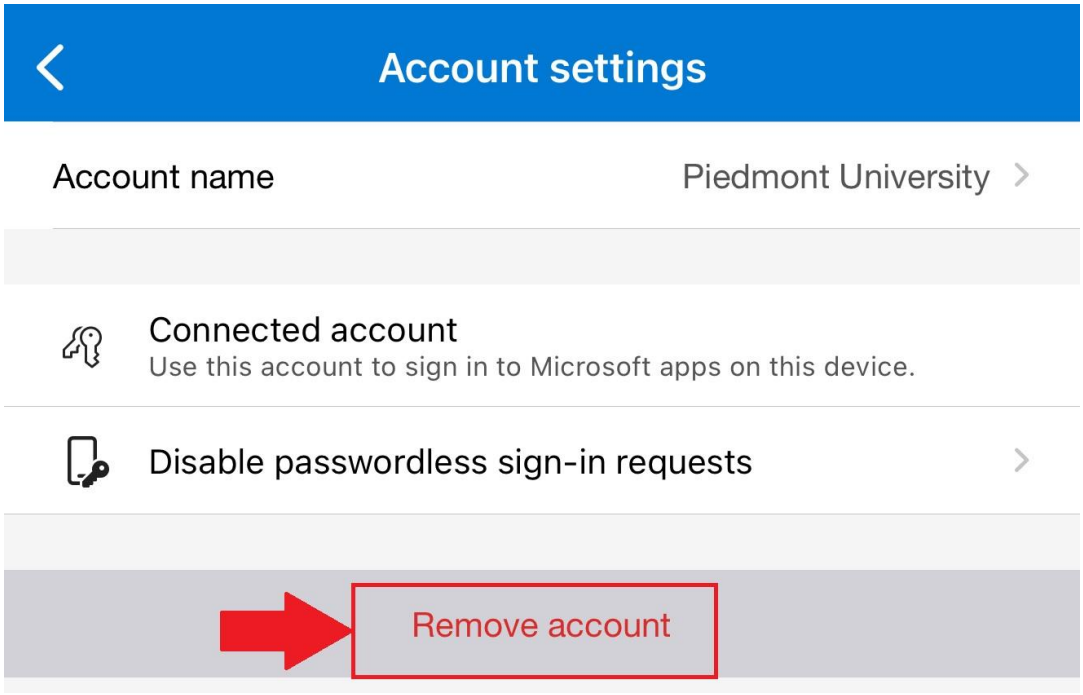
1. To set up MFA again you must **delete the previous account** to receive MFA notifications.
2. Open **Microsoft Authenticator**
3. Select your `@piedmont.edu` or `@lions.piedmont.edu` account



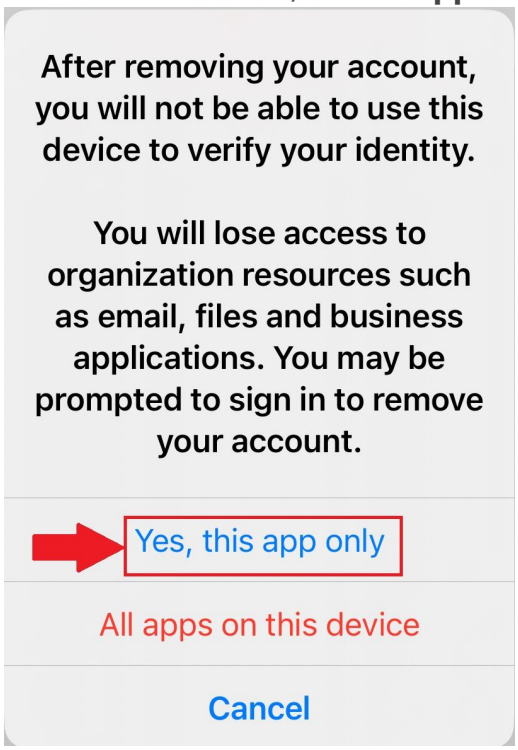
4. Select the **gear icon** in the top right corner



5. Select **Remove Account**



6. Press **Continue** and/or **This app only** to finish removing the account

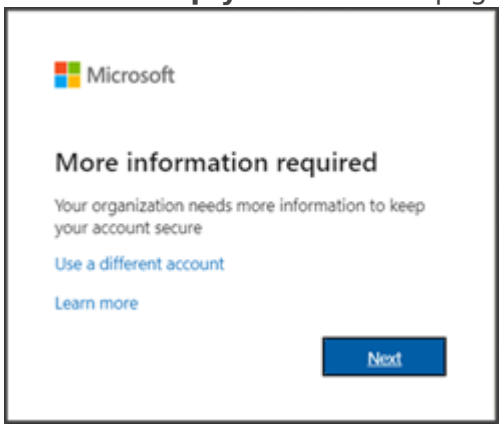


Set up Microsoft Authenticator

1. Open the **Microsoft Authenticator** app on your iOS or Android device
   - If you do not have Microsoft Authenticator installed, please download it from the **iOS App Store** or **Google Play Store**
2. Open the app, **allow notifications** (if prompted)
3. Select **Add account** from the '+' icon in the upper-right
4. Then select **Work or school account**

> On your Computer:

5. On the **Set up your account** page, select **Next**



6. The **Scan the QR code** page appears

7. Use your mobile device to scan the **provided QR code** with the Microsoft Authenticator app
8. Select **Next** on your computer
9. A 2 digit number is displayed on the computer

> On your Mobile Device:

9. A notification is sent to your mobile device prompting for a 2 digit number
10. On your mobile device, **enter the 2 digit number, show on the computer,** in the Microsoft Authenticator app
11. Select **Done** on your computer
12. Your security info is now updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.

Login methods using MFA

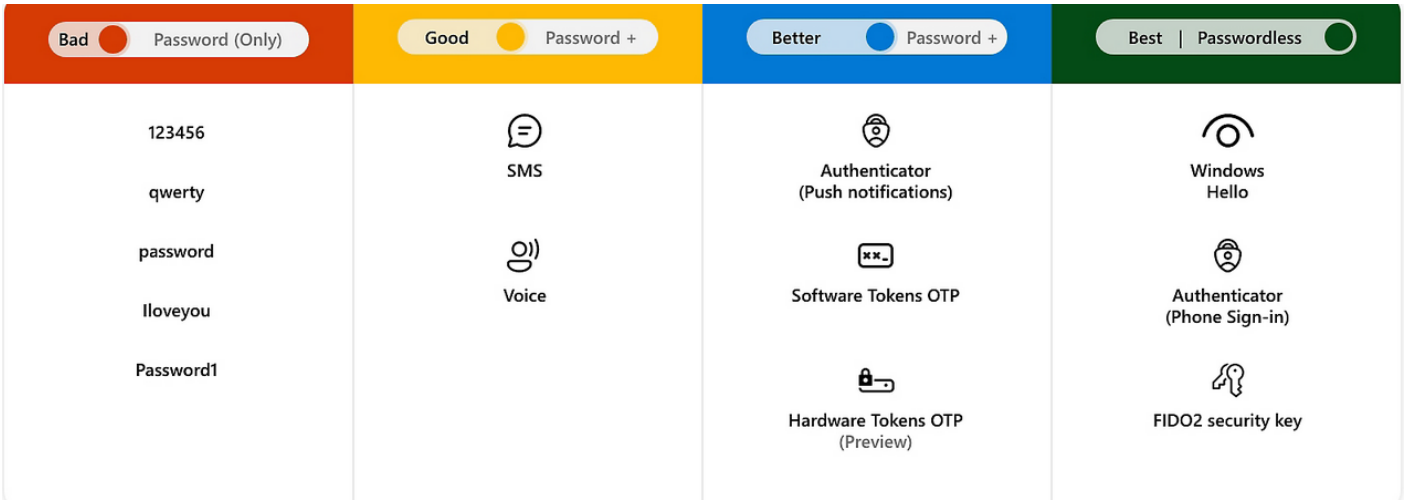
> Our Helpdesk Team is happy to provide assistance with this process! Just give us a call at 706-894-4205!

MFA Passkeys

1. What is a Passkey?

> A passkey is a modern, phishing-resistant way to sign in without using a password!

- Instead of something *you know* (like a password), a **passkey** uses something *you have* (your phone or device) and something *you are* (Face ID, Fingerprint, or device PIN)
- The credential is stored securely on your device and is never shared with the website or service that you're signing into. Because of this, passkeys can't be reused, stolen by fake websites, or guessed.
- Passkeys are based on industry security standards (FIDO2). Your device proves to Microsoft that it's really you, without ever sending a password across the internet.
  - If the site is not legitimate, the passkey simply won't work, and there's nothing for the attacker to steal.
- Your device becomes your key, and your identity stays locked inside it!



- Did you know that passwords are the weakest link in modern security? They are often:
  - Reused
  - Phished
  - Leaked in breaches
  - Guessed
- Microsoft's goal with passwordless sign-in is to:
  - **Eliminate passwords as an attack target** - No passwords means nothing to phish, reuse, or brute-force.
  - **Reduce account takeovers and phishing** - Passkeys only work on the real Microsoft sign-in and approved services. Fake sites can't trick your device into handing over a credential.

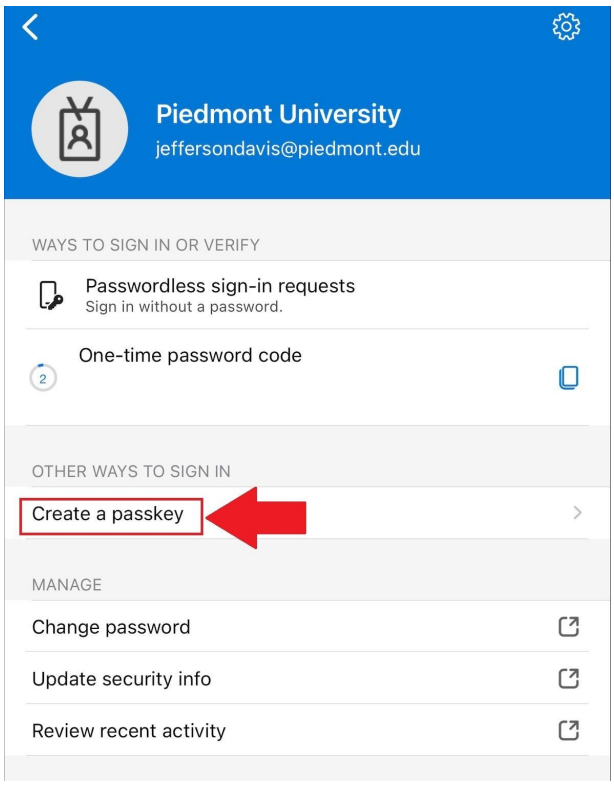
- **Make sign-ins faster and simpler** - Approving with Face ID, fingerprint, or a device PIN is quicker than typing passwords and codes.
- **Improve both security and user experience** - Stronger security without extra steps, fewer account lockouts.

> Passkeys are part of Microsoft's move to a passwordless future where accounts are protected by your device and biometrics instead of passwords that can be stolen, guessed, or phished

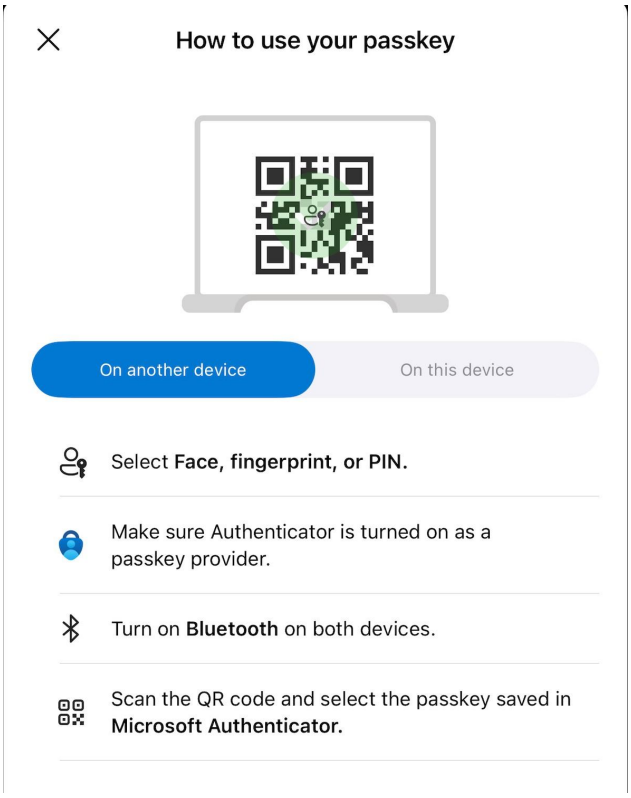
---

2. Create a Passkey

1. Open the Microsoft Authenticator app on your mobile device.
2. Select your @Piedmont.edu or @lions.piedmont.edu account.
3. Under **Other ways to Sign in,** select **Create a Passkey**

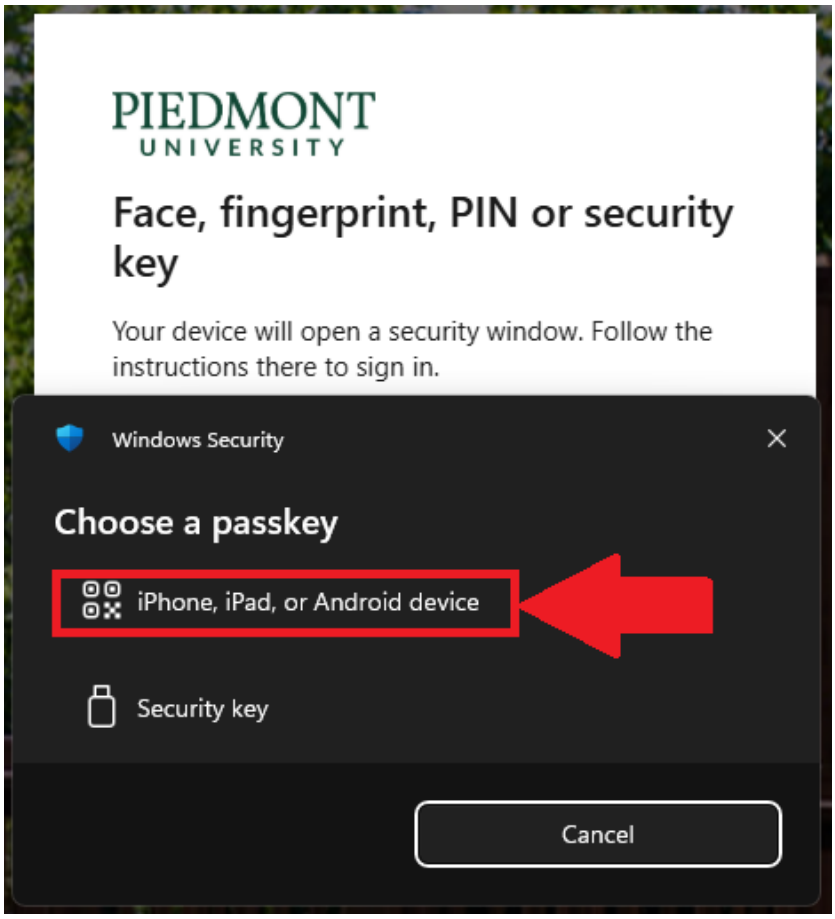


4. Select **Sign in** on the next page.
5. Login using your Piedmont credentials.
6. You will be prompted to complete MFA.
7. Once logged in, your Passkey is created.



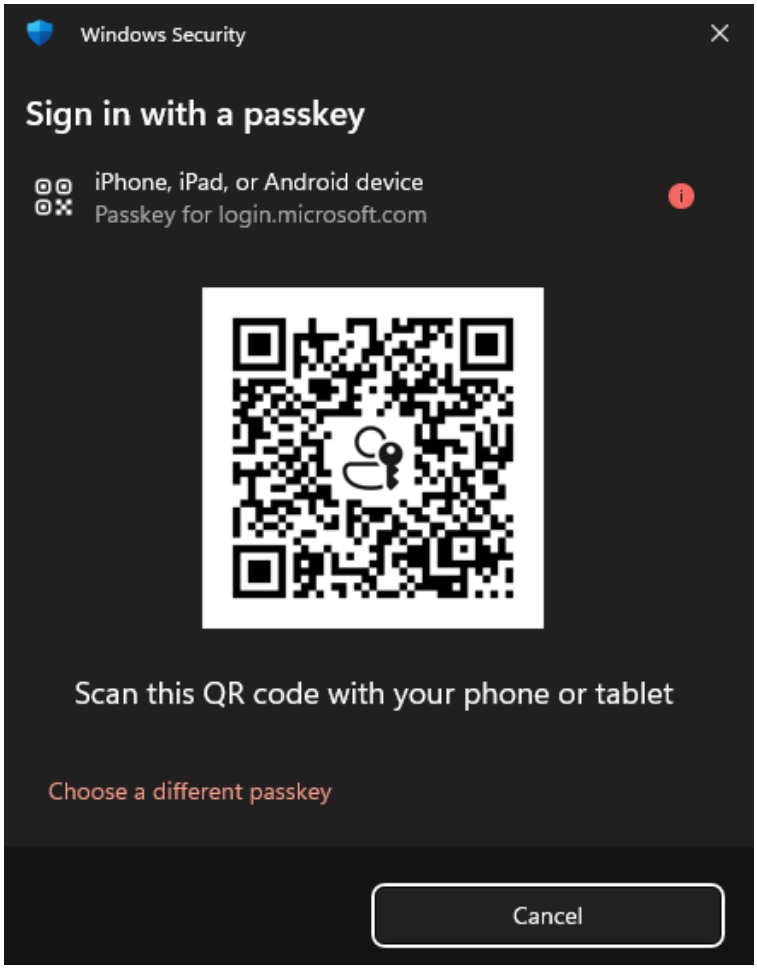
3. Sign in with Passkey

1. When you login using your Piedmont credentials, you will receive a new popup window in place of Microsoft Authenticator



2. Select **iPhone, iPad, or Android device.**

3. Use your mobile device to scan the QR Code on your computer, select **Sign in with Passkey**

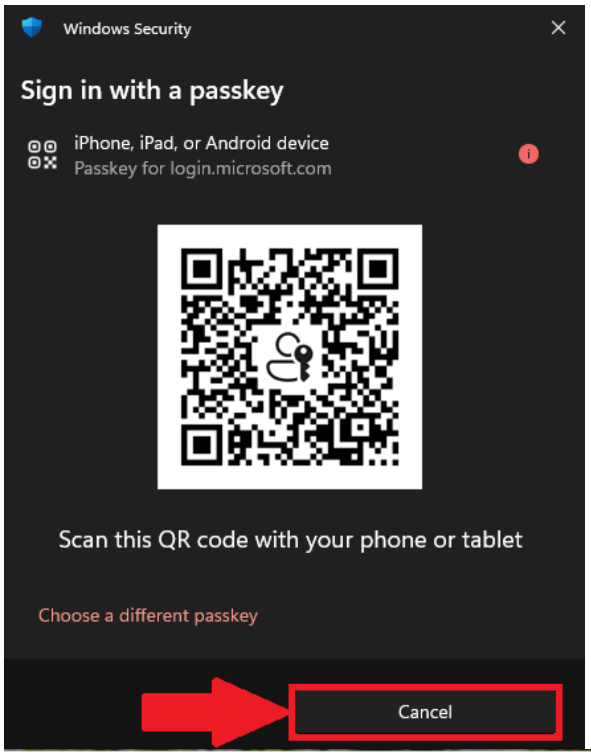


4. On your mobile device, a message will appear "**Sign in to login.microsoft.com" on the other device with your passkey for "@piedmont.edu" saved in "Authenticator" ?**
   - Choose **Use Passkey**
5. Your mobile device will prompt for Face ID or biometrics.

---

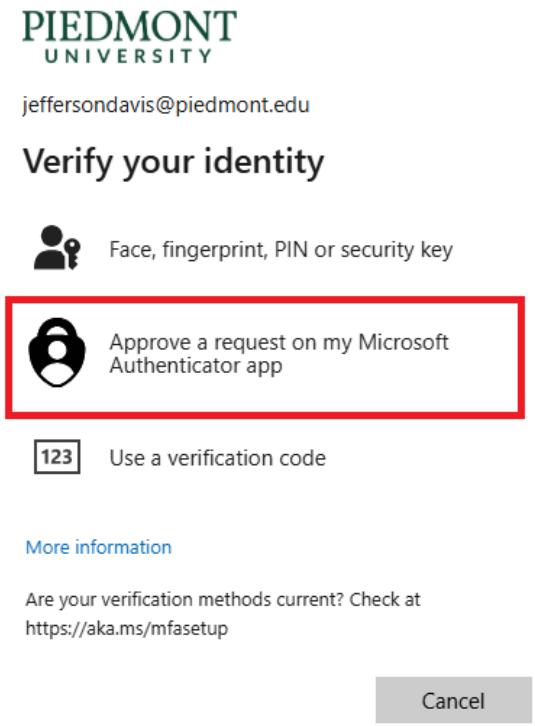
4. Use Original Authentication method

1. In some cases you may need to use the original MFA through the Authenticator app, to do so, select the 'X' or 'Cancel' button and select **Sign in Another way**


Windows Security
Sign in with a passkey
iPhone, iPad, or Android device
Passkey for login.microsoft.com
Scan this QR code with your phone or tablet
Choose a different passkey
Cancel


PIEDMONT
UNIVERSITY
We couldn't sign you in
Something went wrong when trying to sign in with a passkey. Please try again.
Learn more about passkeys
Sign in another way
Back
Try again

2. Select **Approve a request on my Microsoft Authenticator app** to complete original MFA steps.



3. Follow the on-screen instructions to approve the Authenticator request.

Department Contact Info
For any issues or questions regarding MFA, please contact IT Helpdesk support

(706) 894-4205

ITSupport@piedmont.edu

https://itsupport.piedmont.edu/