Disclaimer: *This document has been translated using Lilly Translate. While we strive for accuracy, please be aware that there may be errors or inaccuracies in the translation. Please contact IdentityManagementServices@lilly.com if you have any suggested corrections.*

Introduction

What are Passkeys? Passkeys are a modern, secure alternative to traditional passwords. They use cryptographic keys to authenticate users without requiring a username or password. Passkeys provide stronger verification because they are securely stored on your device and require biometric authentication (such as a fingerprint or facial recognition) or a device PIN, making them more secure than traditional usernames and passwords.

Follow these instructions to set up your passkey in Microsoft Authenticator as a passwordless sign-in method, sign in with a passkey, or delete a passkey.

Jump to section (use Ctrl + click):

1. Confirm your mobile device is ready for passkeys
2. Register Passkey on a Lilly mobile device
3. Register Passkey on a non-Lilly mobile device
4. Sign in with Passkeys in Authenticator for Android and iOS devices (preview)
5. Delete your Passkey in Authenticator for Android or iOS
6. Additional Help

Confirm your mobile device is ready for passkeys

To register a passkey on your mobile device, your mobile device must have:

- iOS version 17, or Android version 14, or later
- Microsoft Authenticator app installed and enabled for passkeys

1. Check your version of iOS or Android
   - **For IOS Devices:** On your device, open the **Settings** app, tap **General**, tap **About**
   - **For Android Devices:** On your device, open the **Settings** app, tap **About Phone**
2. Check that Microsoft Authenticator is installed

   FOR LILLY iOS DEVICES: Microsoft Authenticator should be installed on your Lilly iOS device. If not, ensure you have completed the Mobility@Lilly: Setup and enroll your Lilly iPhone/iPad guide, including the Microsoft iOS Registration procedure.

   FOR PERSONAL MOBILE DEVICES: Download the Microsoft Authenticator application from the Apple App Store (iPhone/iPad) or Google Play Store (Android). Be sure to keep the Microsoft Authenticator app updated on your mobile device via the appropriate app store.

3. Enable Authenticator as a passkey provider in **Settings** of your mobile device:

For iOS Devices:

- On your iOS device, open **Settings**.
- Open **General** and select **Autofill & Passwords**
- Under **Autofill From** enable **Authenticator**

For Android Devices:

Note: The exact wording of settings and screen layout may vary depending on the device's OS version and customizations.

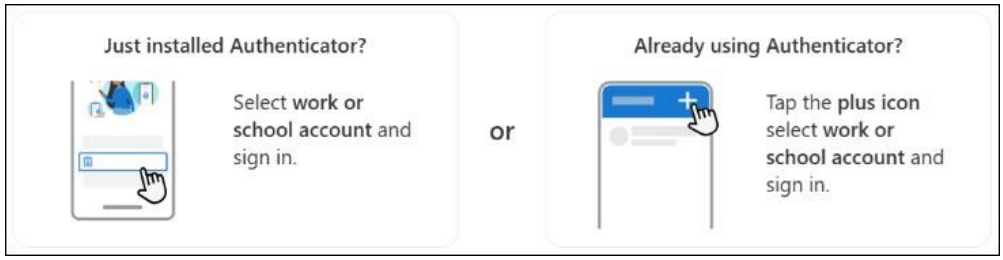
- On your Android device, open **Settings**.
- Open **Passwords & Accounts**.

- Under **Additional providers** enable **Authenticator**.

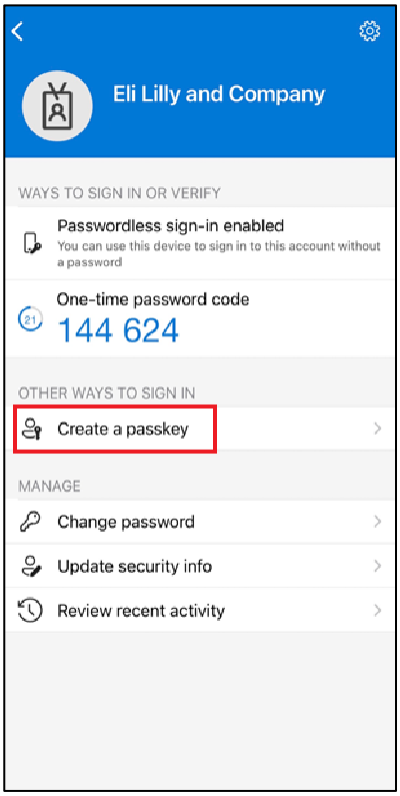
Register Passkey on a Lilly Mobile Device

Follow these instructions to set up a passkey in Microsoft Authenticator on a Lilly-provided mobile device. If you are using a non-Lilly device, use Register Passkey on a non-Lilly Mobile Device to complete your registration.

1. Open Microsoft Authenticator on your mobile device
2. In Microsoft Authenticator, **select your Lilly account**. If you do not see your Lilly account, follow the steps below.



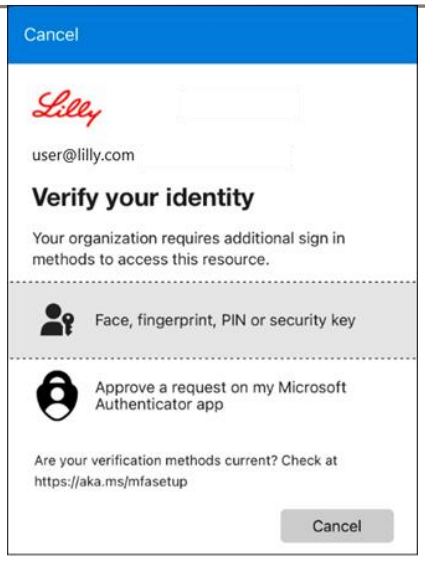
3. Tap **Create a passkey** or tap settings and select **Create a passkey**



4. On the **Let's create your** passkey screen, select Sign-in to complete multifactor authentication (MFA).

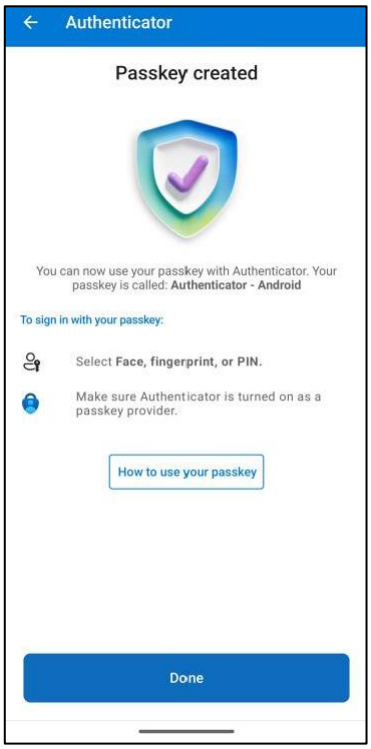
   On the **Verify your identity** screen, select one of your available authentication methods.

   If you see the **Something went wrong** screen, select **Other ways to sign in,** then select one of your available authentication methods.

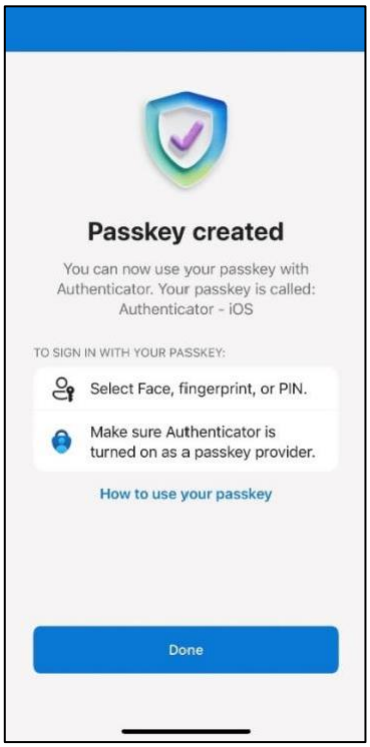


5. Your passkey is successfully added as a sign-in method for your account.
   Select **Done**.

For Android mobile devices:



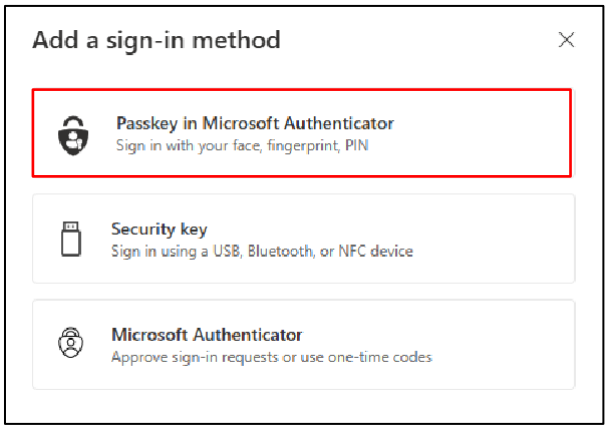
For iOS mobile devices:



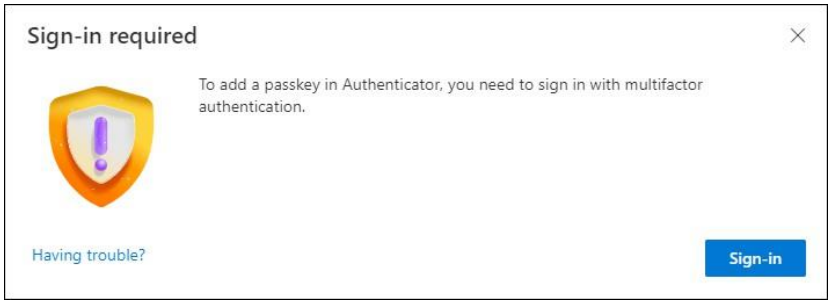
Register Passkey on a non-Lilly Mobile Device

If you are using a non-Lilly mobile device, follow these instructions to set up a passkey using the mobile device browser or using a separate computer. This registration requires Bluetooth to be enabled and an internet connection for both devices.

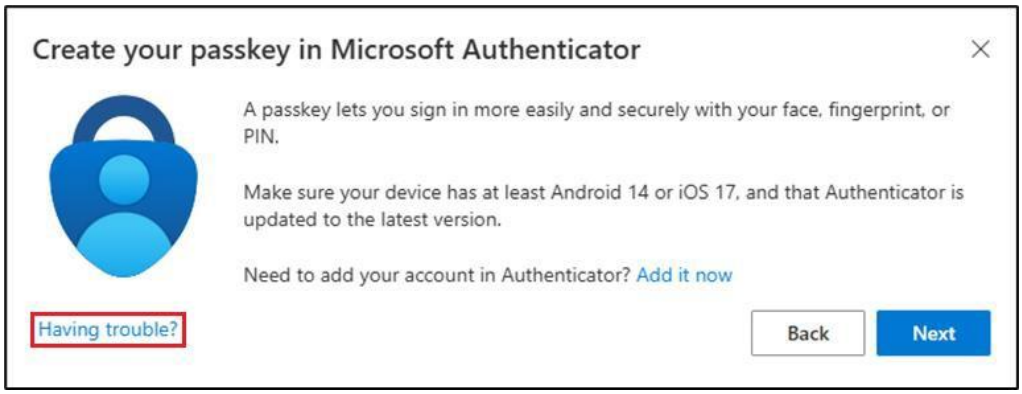
1) Open Microsoft Edge and access My Sign-Ins.
2) In the top right corner, click your picture and ensure you are signed in with the account you plan to use with your passkey (e.g., standard account, -CA, or -DS).
3) Select **+ Add sign-in method.**
4) Select the **Passkey in Microsoft Authenticator** method and select **Add**.



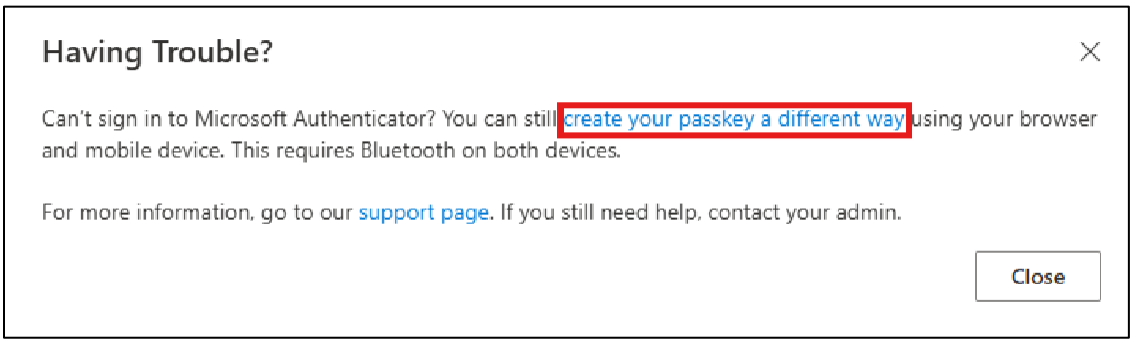
5) Select **Sign-in** to verify your identity by authenticating using your preferred authentication method (Windows Hello for Business, mobile phone notification, or security key).



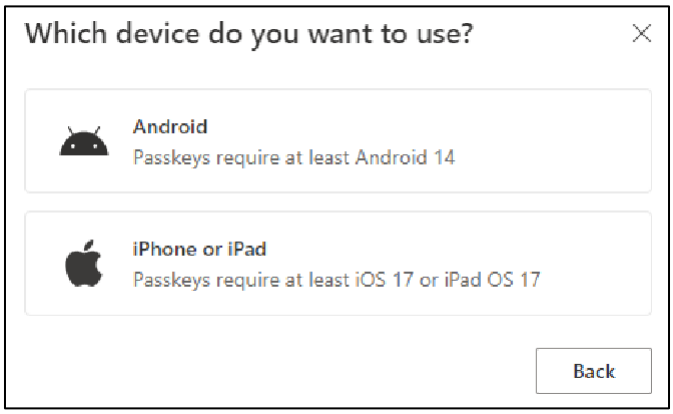
6) On the **Create your passkey in Microsoft Authenticator screen**, select the '**Having Trouble?**' link.



7) On the **Having Trouble?** screen, select the '<u>create your passkey a different way</u>' link to register a passkey for PPA.

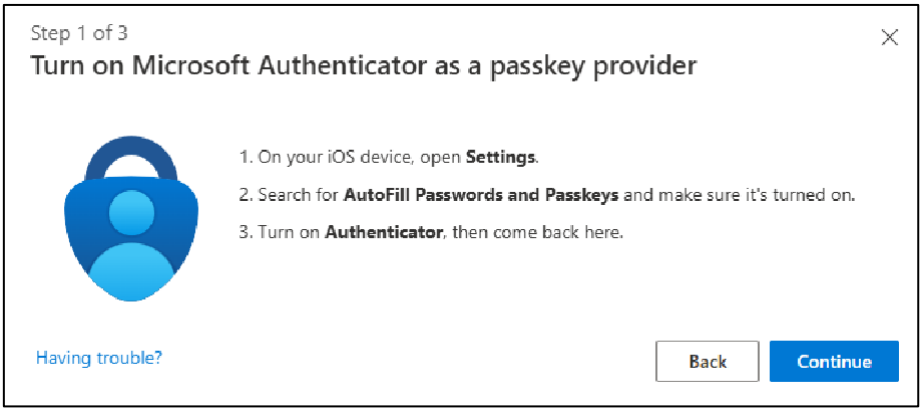


8) Select your device type:

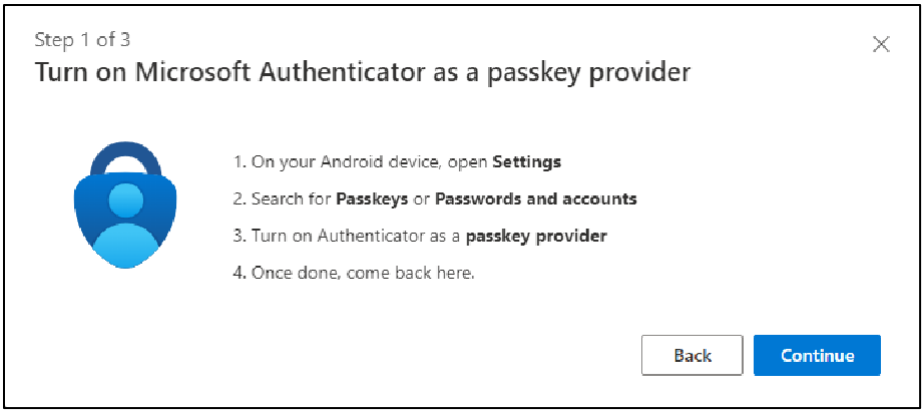


9) On the **Turn on Microsoft Authenticator as a passkey provider** screen, select **Continue**.

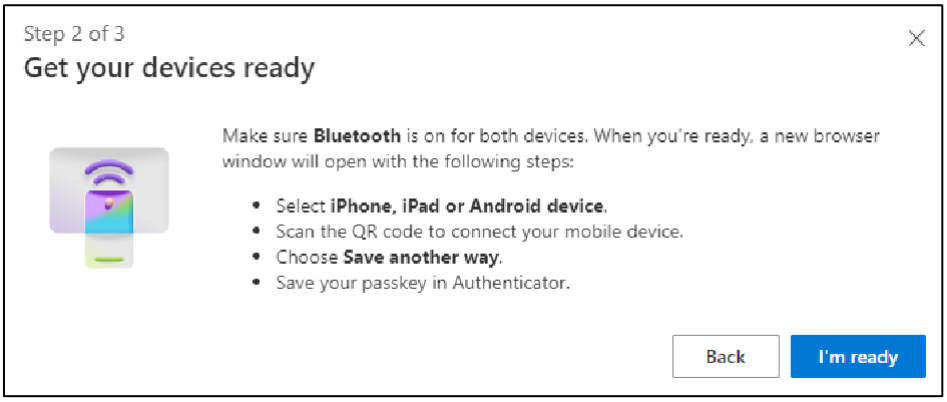
For iOS Devices:



For Android Devices:

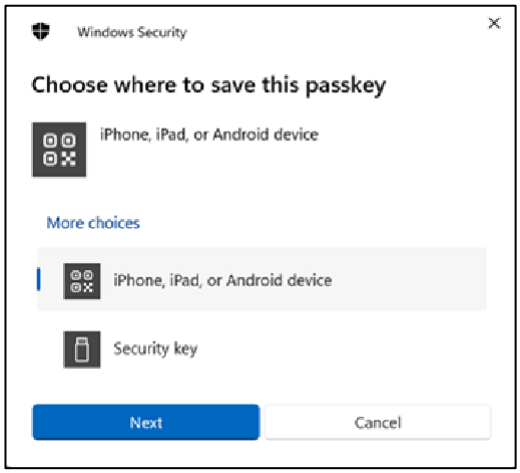


10) Make sure Bluetooth is enabled for both devices and select **I'm ready**.

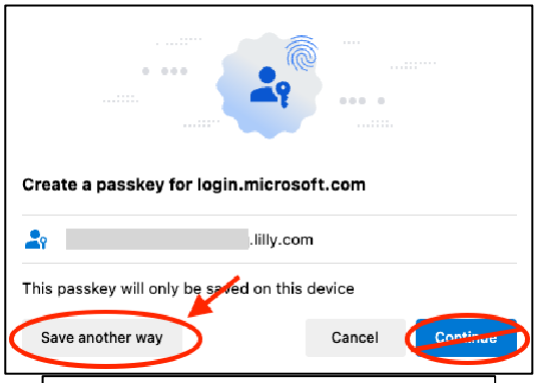


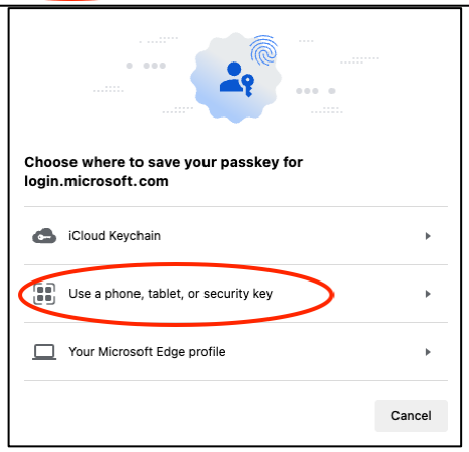
11) Select where to save your passkey.

For Windows devices:
In the security dialog that opens on your browser, select **iPhone, iPad, or Android device**, and tap **Next**.



For Mac devices:
In the security dialog that opens on your browser, select **Save another way** and on the next dialog select **Use a phone, tablet, or security key.**

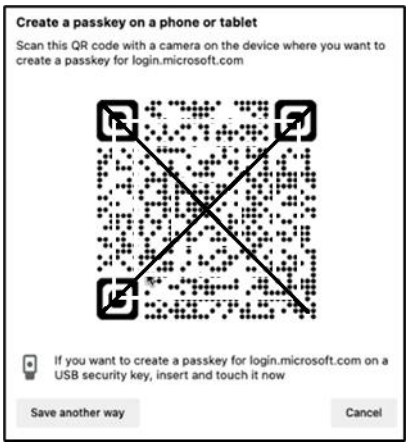




12) Use your mobile device camera to scan the QR code on your screen, and then tap **Save a passkey**.

For Windows devices:

For Mac devices:



13) Your device should now connect over Bluetooth to the device you started registration with.

For Windows devices:

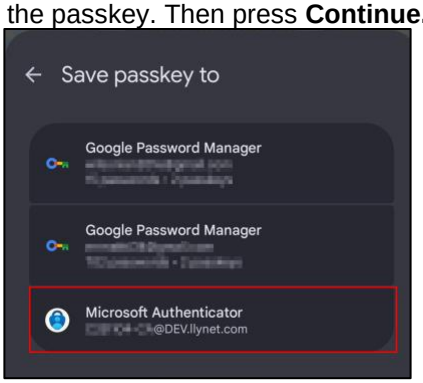
For Mac devices:

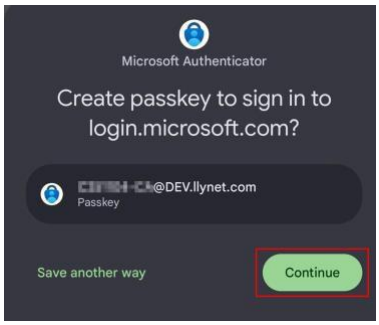
Note: Bluetooth and an internet connection are required for this step and must be enabled on your mobile and computer device.

14) Your device will prompt to save or create a passkey. Select **Continue** to save the passkey to Authenticator.

For Android mobile devices:

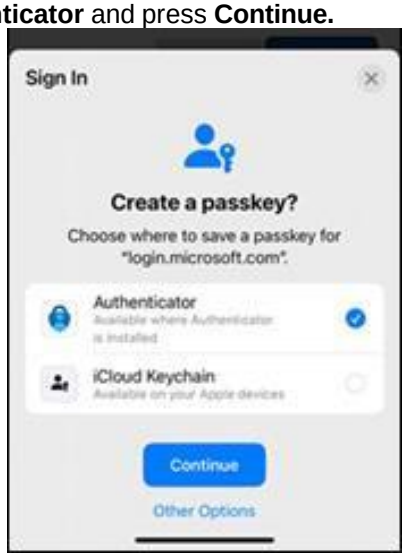
Select **Microsoft Authenticator** as the location to save the passkey. Then press **Continue.**



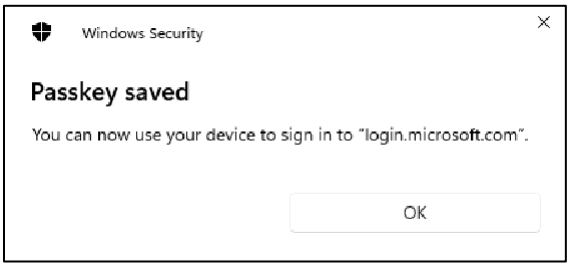


For iOS mobile devices:

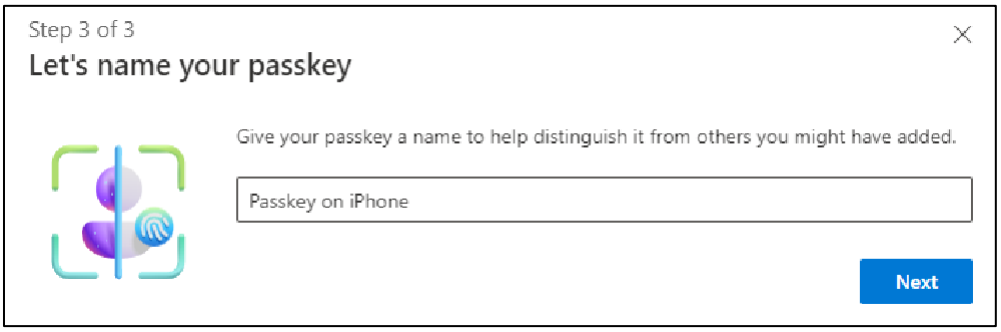
Ensure the checkbox is selected for **Authenticator** and press **Continue.**



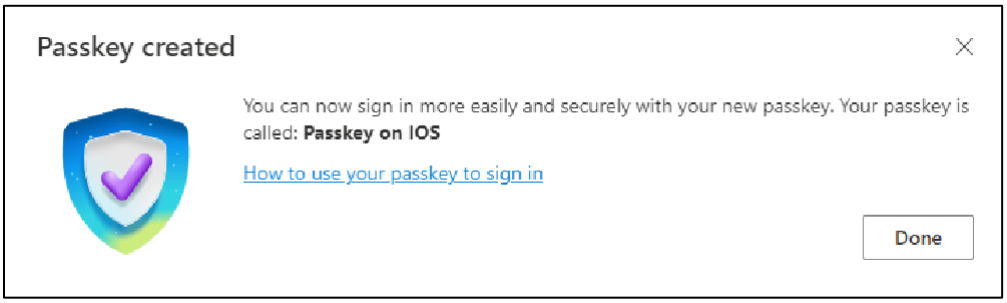
15) Once the passkey is successfully created on your device, you're directed back to My Security info. If prompted, select **OK**.



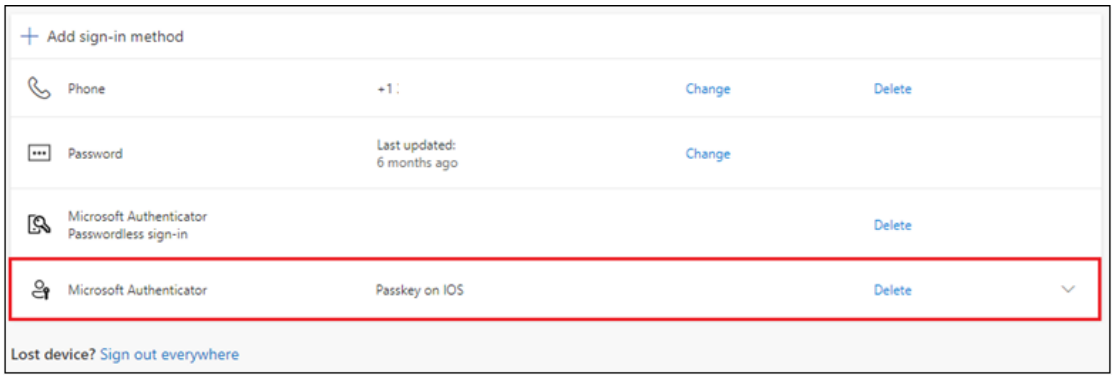
16) Enter a passkey name to help distinguish it from other keys and select **Next**.



17) Your passkey is created successfully. Select **Done.**



18) In Security info, you can see the new passkey added.

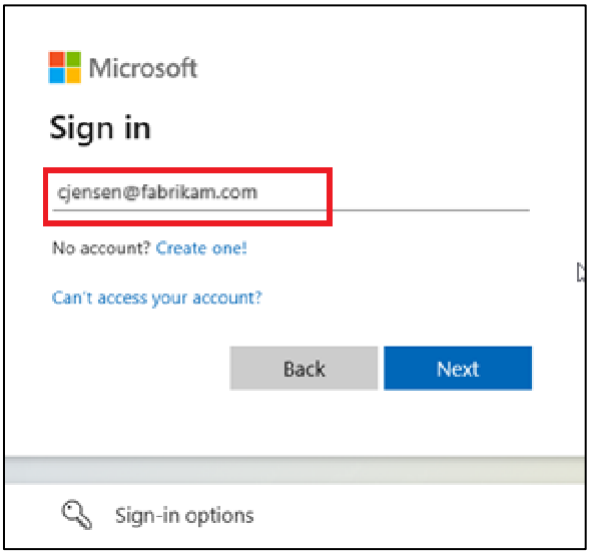


Sign in with passkeys in Authenticator for Android and iOS devices

Note: To sign in with a passkey in Microsoft Authenticator, your mobile device needs to run iOS version 17, or Android version 14, or later.

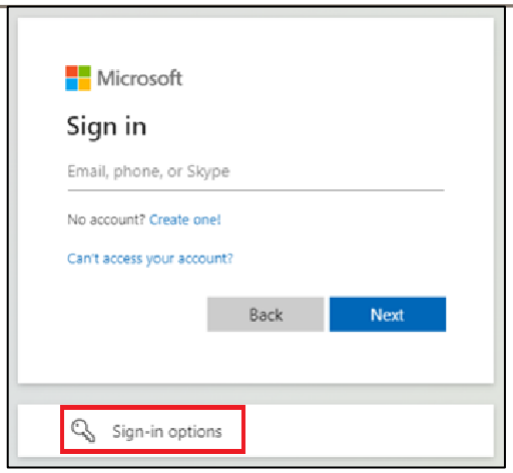
Follow these steps to sign-in to Microsoft Entra ID with a passkey in Authenticator on your iOS device. On the computer browser, navigate to the web URL you're trying to access such as My Sign-Ins.

1. If prompted, enter your sign-in address:



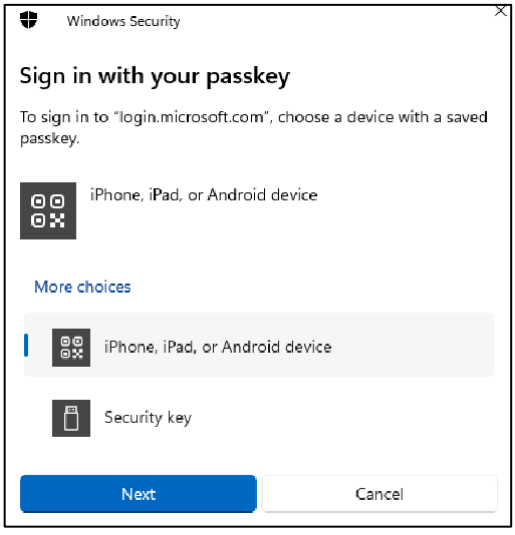
If you last used a passkey to authenticate, you will be automatically prompted to authenticate with a passkey. Otherwise, you may click on **other ways to sign in** and then select **Face, fingerprint, PIN, or security key**.

Alternatively, click **Sign-in options** to sign in more conveniently without having to enter a username.



If you chose **Sign-in options**, select **Face, fingerprint, PIN, or security key**. Otherwise, skip to next step.

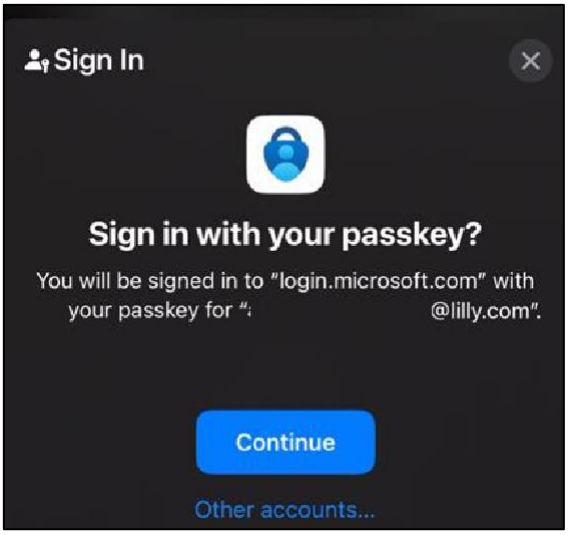
2. Select **iPhone, iPad, or Android device**.



3. A QR code should appear on screen. On your mobile device, **open the Camera app** and **scan the QR code**.

Note: Bluetooth and an internet connection are required for this step, and both must be enabled on your mobile and computer device.

4. To select your passkey, follow the steps in the Android operating system dialog. Verify that it's you by scanning your face, fingerprint, or enter your device PIN or unlock gesture.



5. You're now signed into My Sign-Ins on your computer browser.

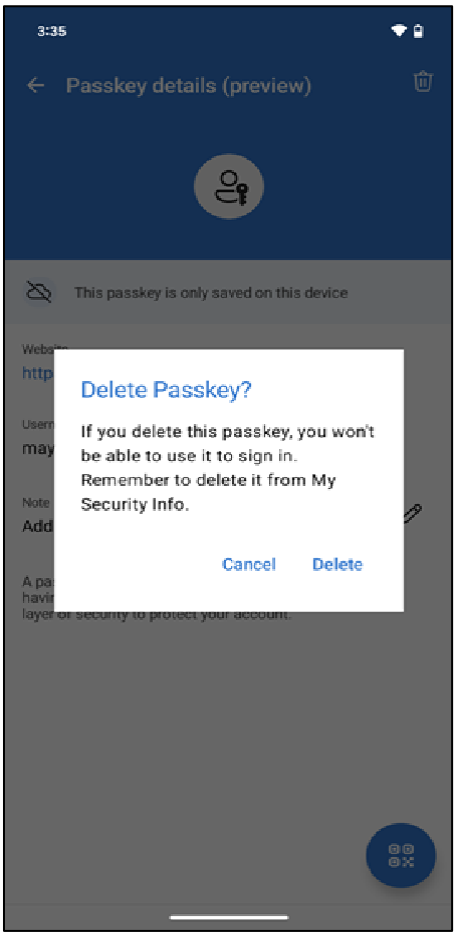
Delete your Passkey in Authenticator for Android or iOS

Note: To completely remove Passkey method, you need to delete the passkey from **both** Microsoft Authenticator App on your device and My Security info page on your computer browser.

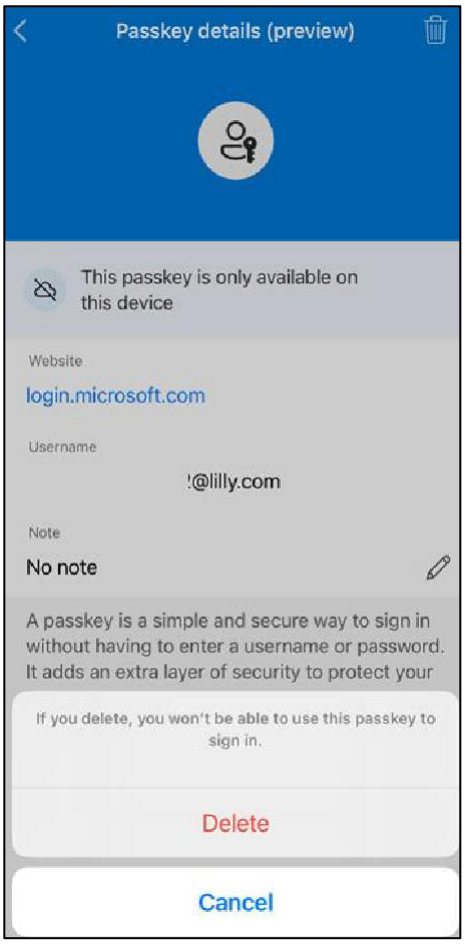
Follow these steps to delete the passkey from Microsoft Authenticator App on your device.

1. **Open Authenticator App** on your device and select the account from which you want to remove the Passkey.
2. Select Passkey under your account and click the **Trash Can** icon on top right corner of the screen, then tap **Delete** to confirm.
3. You have successfully deleted the passkey from Microsoft Authenticator App**.** Follow the next steps to remove passkey from My Security info page on your computer.

For Android mobile devices:

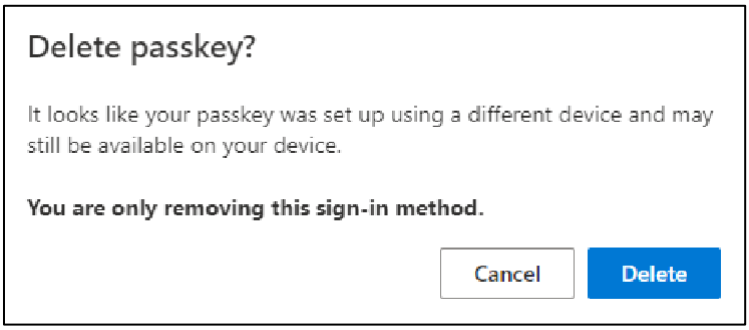


For iOS mobile devices:

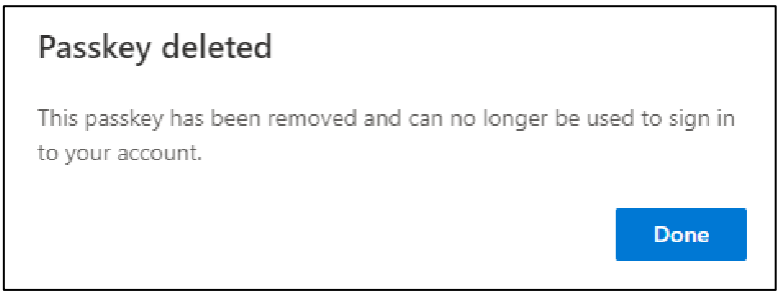


4. Open browser on your computer and access My Sign-Ins. In the top right corner, click your picture and ensure you are signed in with the account from which you plan to remove your passkey (e.g., -CA).
5. Select **Remove** to delete the passkey from the sign-in methods on My Security info page.

6. When Prompted, Select **Delete** to confirm the passkey removal.



7. You have successfully deleted Passkey from My Security info. Select **Done**.



Additional Help

Please review these Frequently Asked Questions for assistance. If you don't see your question addressed, we encourage you to post it to the Adopting Identity Services community.

For technical assistance not addressed in the FAQs or Job Aids, use ChatNow in Teams or the ChatNow app on your Lilly mobile device (iPhone, iPad). Create an incident and assign it to the MFA-SUPP-GLB queue.