

Student: Set Up a Passkey Using Windows Hello

In brief: A passkey lets you confirm sign-in using a secure method such as a PIN, fingerprint or facial recognition. It removes the need to type a password or enter a one-time code during supported sign-ins.

Before You Start

- Use the Windows device (Windows 11 or greater) on which you want to set up the passkey.
- Make sure you can sign in to your UHI account and complete multi-factor authentication (MFA).
- Make sure the device supports Windows Hello. A PIN can be used even if fingerprint or facial recognition is unavailable.
- Use an up-to-date browser and keep the device connected to the internet.
- Do not remove your existing Microsoft Authenticator method. Keeping more than one authentication method helps prevent loss of access.

Important: The wording and appearance of the prompts may differ slightly depending on your version of Windows and browser. Follow the option names shown on your screen.

Set Up the Passkey

Step 1: Continue from the security prompt

After signing in and completing MFA, review the “Let’s keep your account secure” message. Select “Next” to continue. If you are not ready to set up the passkey, selecting “Not now” may postpone the prompt.

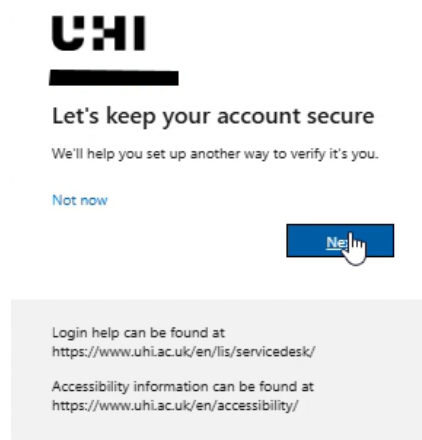


Figure 1. Continue from the security prompt

Step 2: Start creating the passkey

On the “Sign in faster with your face, fingerprint, or PIN” screen, select Next. Windows will open a secure prompt to begin creating the passkey.

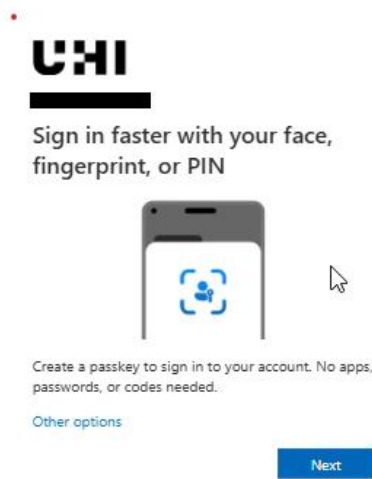


Figure 2. Start creating the passkey

Step 3: Choose a different save location

When the “Create a passkey” window appears, select “Save another way”. This lets you choose where the passkey will be stored.

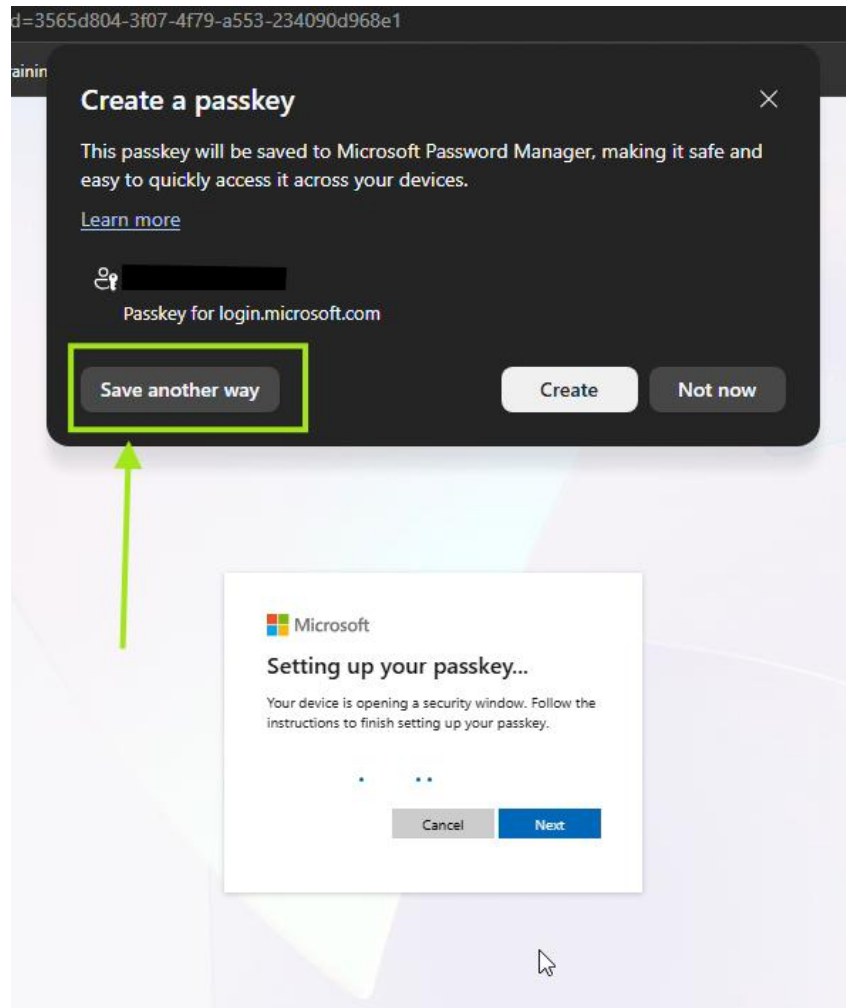


Figure 3. Choose a different save location

Step 4: Select Microsoft Password Manager

On “Select where to save your passkey”, choose “Microsoft password manager”. The other option shown can be used to save the passkey to a phone, tablet or security key, but this guide follows Microsoft Password Manager.

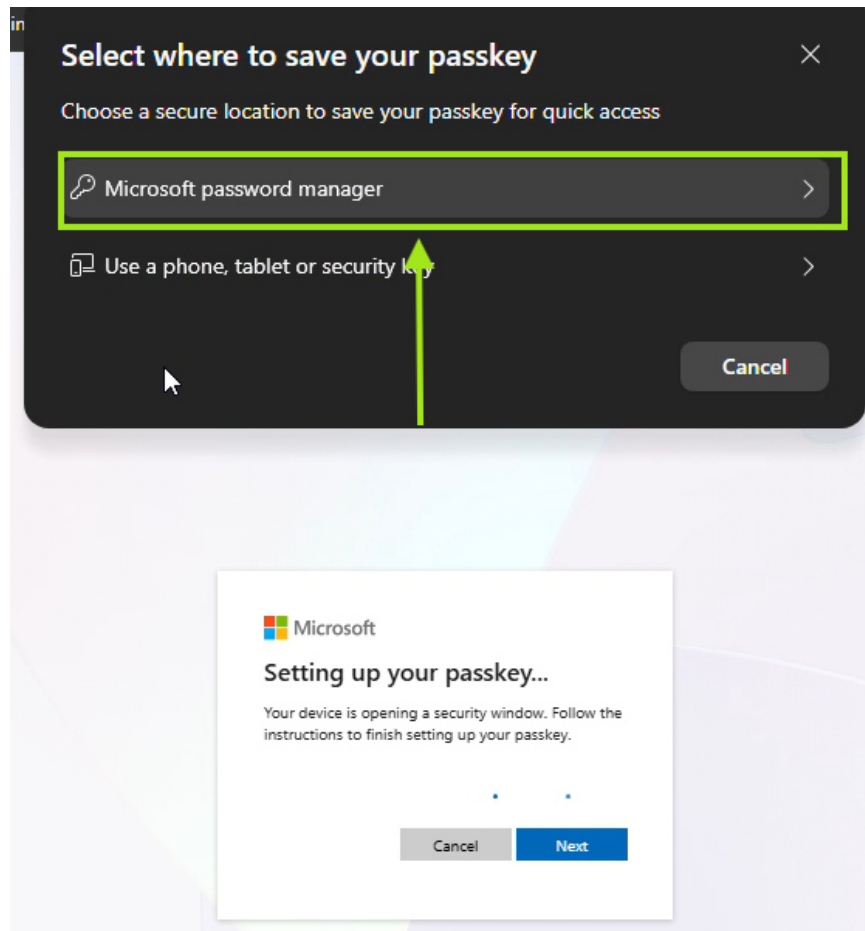


Figure 4. Select Microsoft Password Manager

Step 5: Confirm that you want to create the passkey

Review the account shown in the prompt. If it is your UHI account, select “Create”. If the wrong account is displayed, cancel the process and sign in again with the correct account.

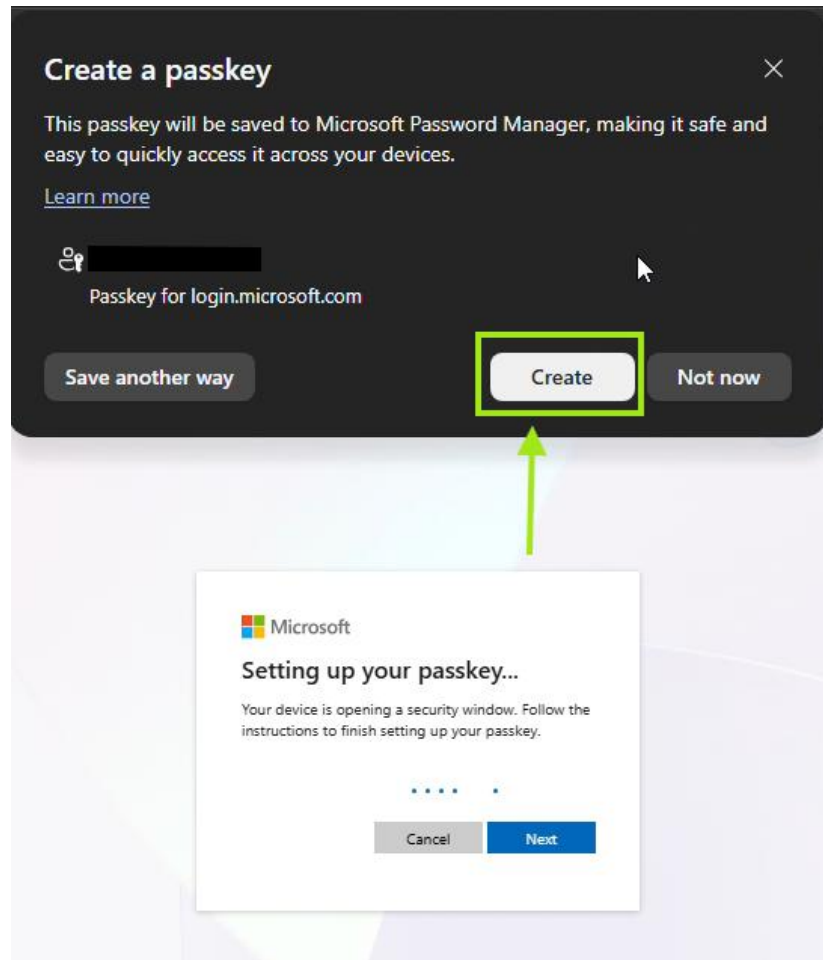


Figure 5. Confirm that you want to create the passkey

Step 6: Create a Microsoft Password Manager PIN

Enter a PIN for Microsoft Password Manager, choose the available PIN options if required, and select “Create”. Choose a PIN you can remember and **do not share it** with anyone.

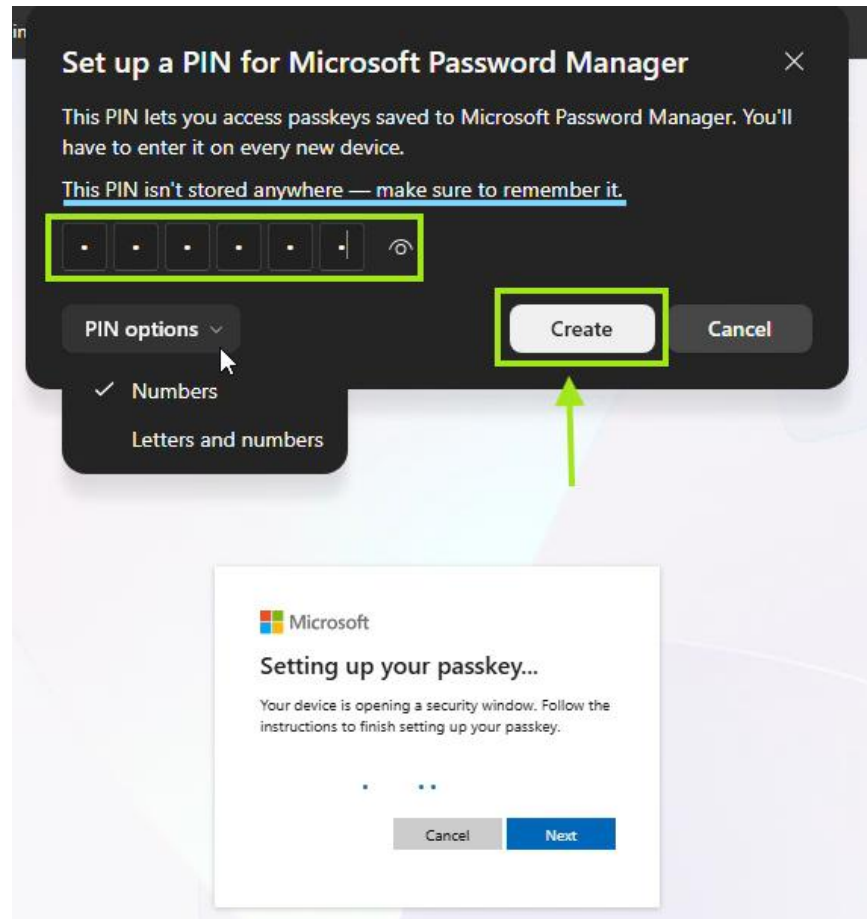


Figure 6. Create a Microsoft Password Manager PIN

Note: This prompt refers to the PIN used to unlock passkeys held in Microsoft Password Manager. Follow the wording displayed on your device.

Step 7: Give the passkey a recognisable name

Enter a short name that will help you identify the passkey later, for example “Personal Windows laptop”, then select “Next”.

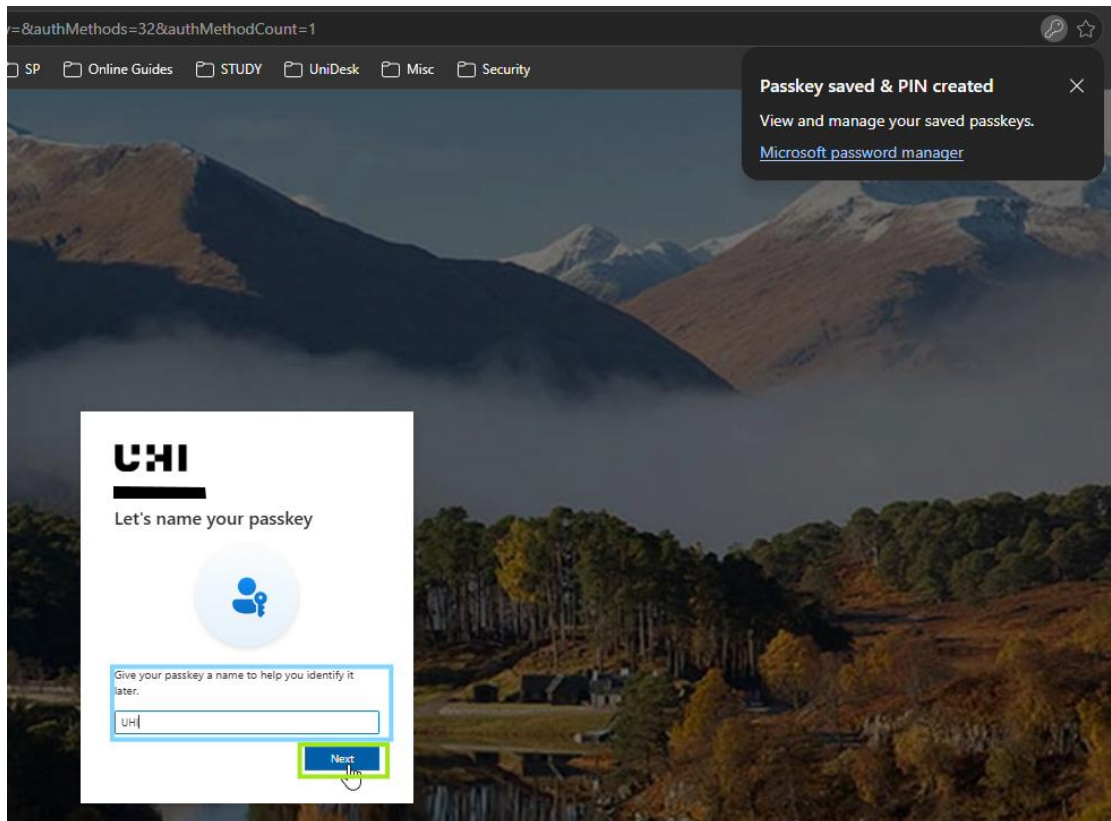


Figure 7. Give the passkey a recognisable name

Step 8: Finish the setup

When “Passkey created” appears, select “Done”. A separate notification may also confirm that the passkey and PIN were created.

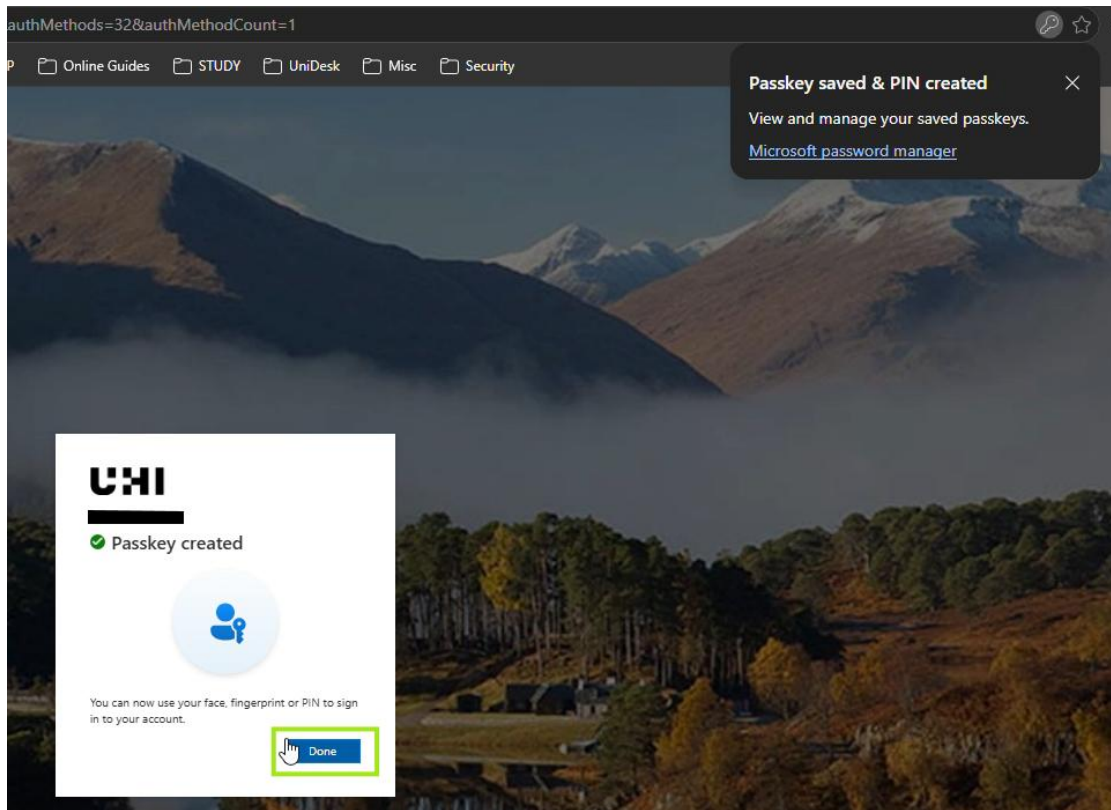


Figure 8. Finish the setup

Test the Passkey

Step 9: Open a fresh sign-in page

Open a new browser tab and go to Outlook on the web or another UHI Microsoft 365 service. Enter your UHI email address if prompted, then select your account.

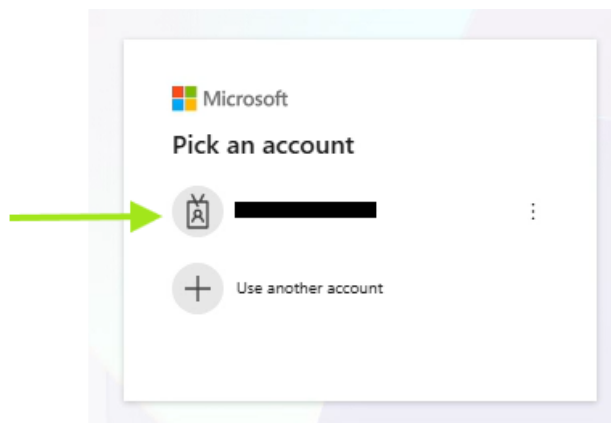


Figure 9. Open a fresh sign-in page

Step 10: Approve the sign-in

When prompted, enter the Microsoft Password Manager PIN you created and select “Confirm”. Windows may then ask you to complete the sign-in using an available Windows Hello method such as a PIN, fingerprint or facial recognition.

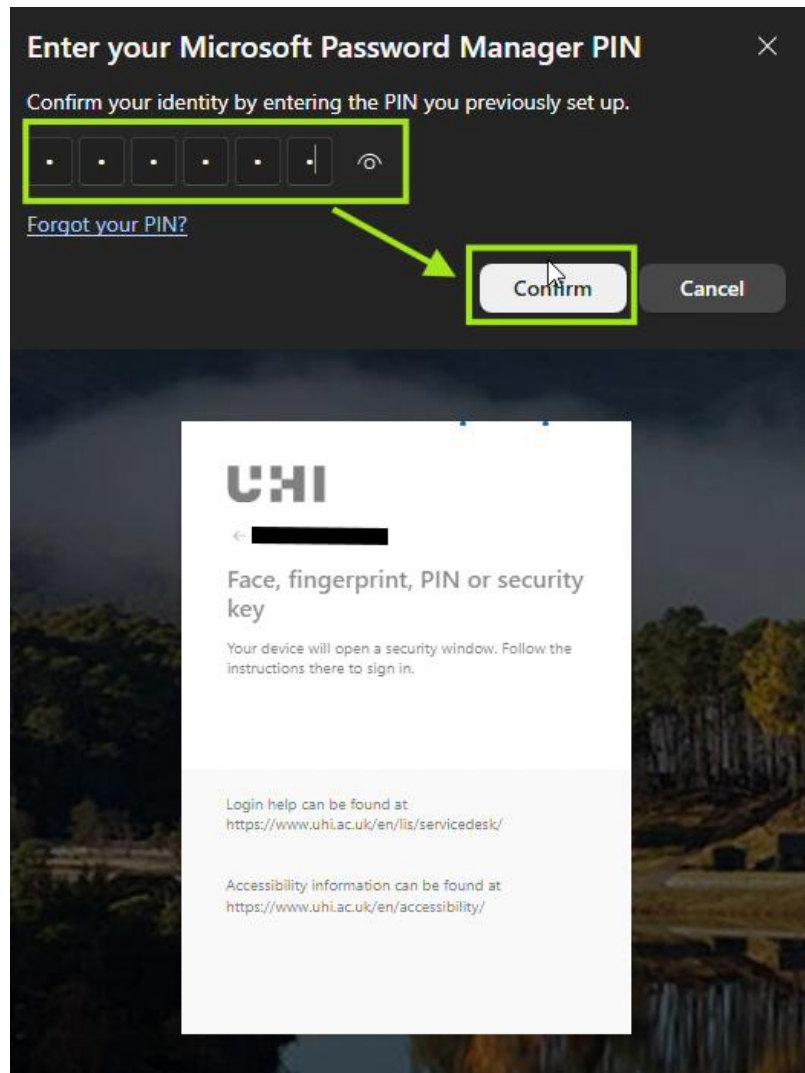
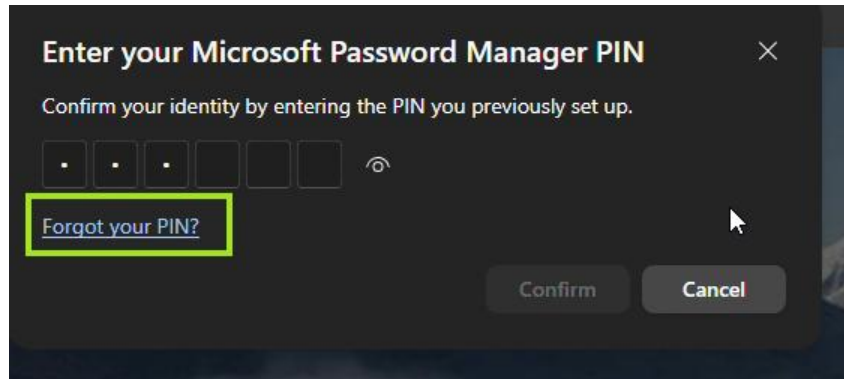


Figure 10. Approve the sign-in

Successful test: You should be signed in to your UHI account without being asked to enter your account password or authentication step.

If You Forget the Microsoft Password Manager PIN

On the “Enter your Microsoft Password Manager PIN” prompt, select [Forgot your PIN?](#) and follow the on-screen instructions to verify your identity and reset the PIN.



Security reminder: Only approve authentication prompts that you initiated. If you receive an unexpected prompt, deny it and contact the UHI Service Desk.

If You Cannot Complete the Setup

- Check that you are signed in with the correct UHI account.
- Close and reopen the browser, then try again.
- Restart the Windows device and repeat the process.
- If the passkey option is missing, the setup repeatedly fails, or you cannot access any registered MFA method, contact the UHI Service Desk or local ICT support.
- When contacting the Service Desk or your local ICT support, provide the device type, Windows version, browser name, exact error message and a screenshot where possible.

Manage or Remove a Passkey

For a work or school account, review registered sign-in methods in your Security info page. If you remove a passkey, also remove the saved copy from the place where it was stored. Add and test another sign-in method before removing one that you currently rely on.