

Student: Set Up a Passkey Using Google Password Manager

In brief: Google Password Manager can save a passkey in Chrome. The passkey can then be used with your device screen lock, such as a PIN, fingerprint or face recognition, when the sign-in page offers a passkey.

Before You Start

- Make sure Microsoft Authenticator is already registered on your UHI account.
- Use the latest available operating system and version of Google Chrome on your device.
- Make sure you can sign in to your UHI account and complete multi-factor authentication (MFA).
- Make sure you are signed in to the correct Google profile in Chrome.
- Check that your device has a screen lock set up, such as a PIN, fingerprint or face recognition.
- Keep another authentication method registered in case the passkey is unavailable.

Important: Do not share your device PIN, Google Password Manager PIN, passwords or recovery information with anyone, including the Service Desk.

Set Up the Passkey

The screens may look slightly different depending on your device and Chrome version. Follow the prompts shown on your device.

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.

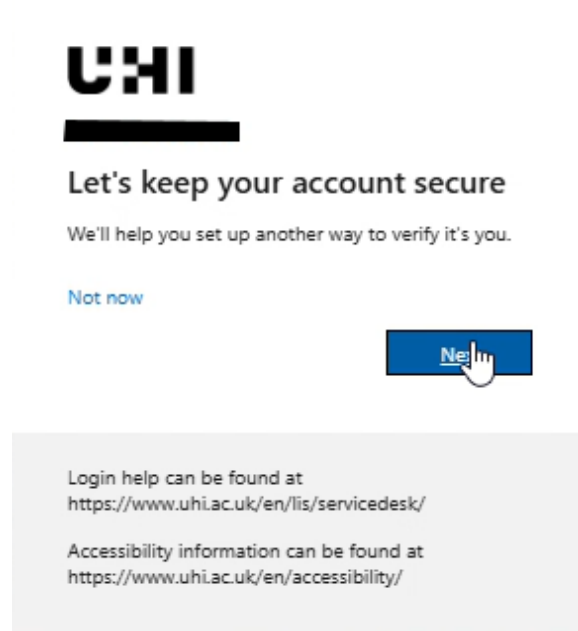


Figure 1. Continue from the security prompt

Step 2: Start passkey creation

When Microsoft offers a faster sign-in using your face, fingerprint or PIN, select “Next”.

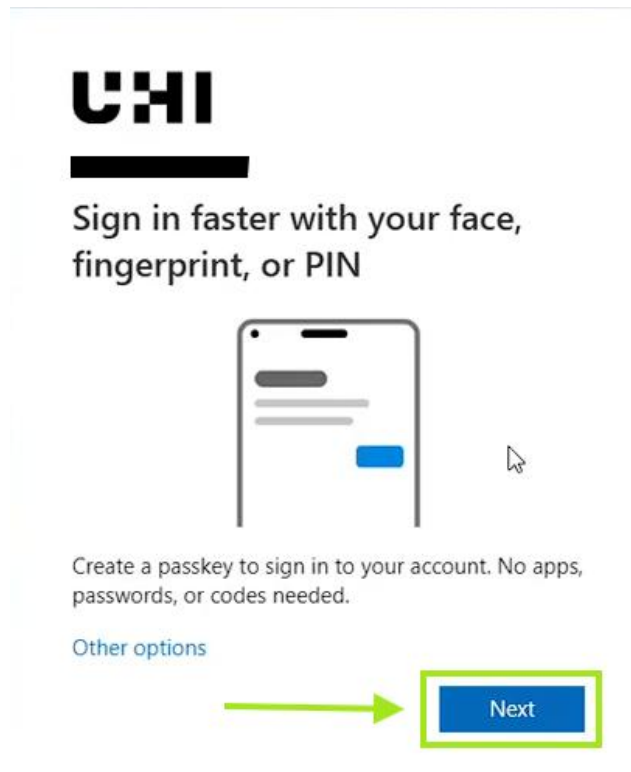


Figure 2. Start creating the passkey

Step 3: Confirm Google Password Manager

Google Password Manager displays the account where the passkey will be saved. Check that the correct account is shown, then select “Next”.

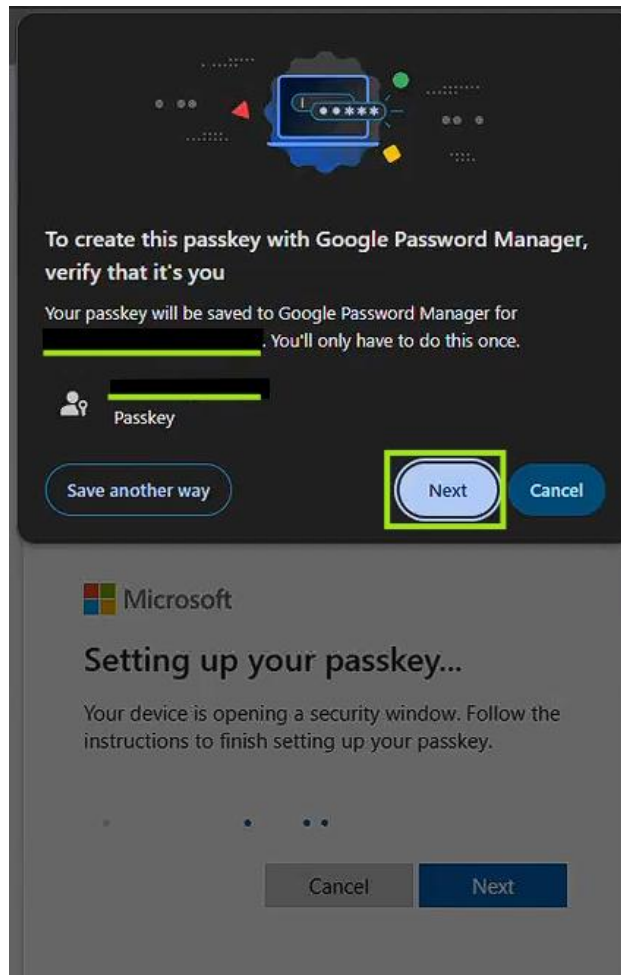
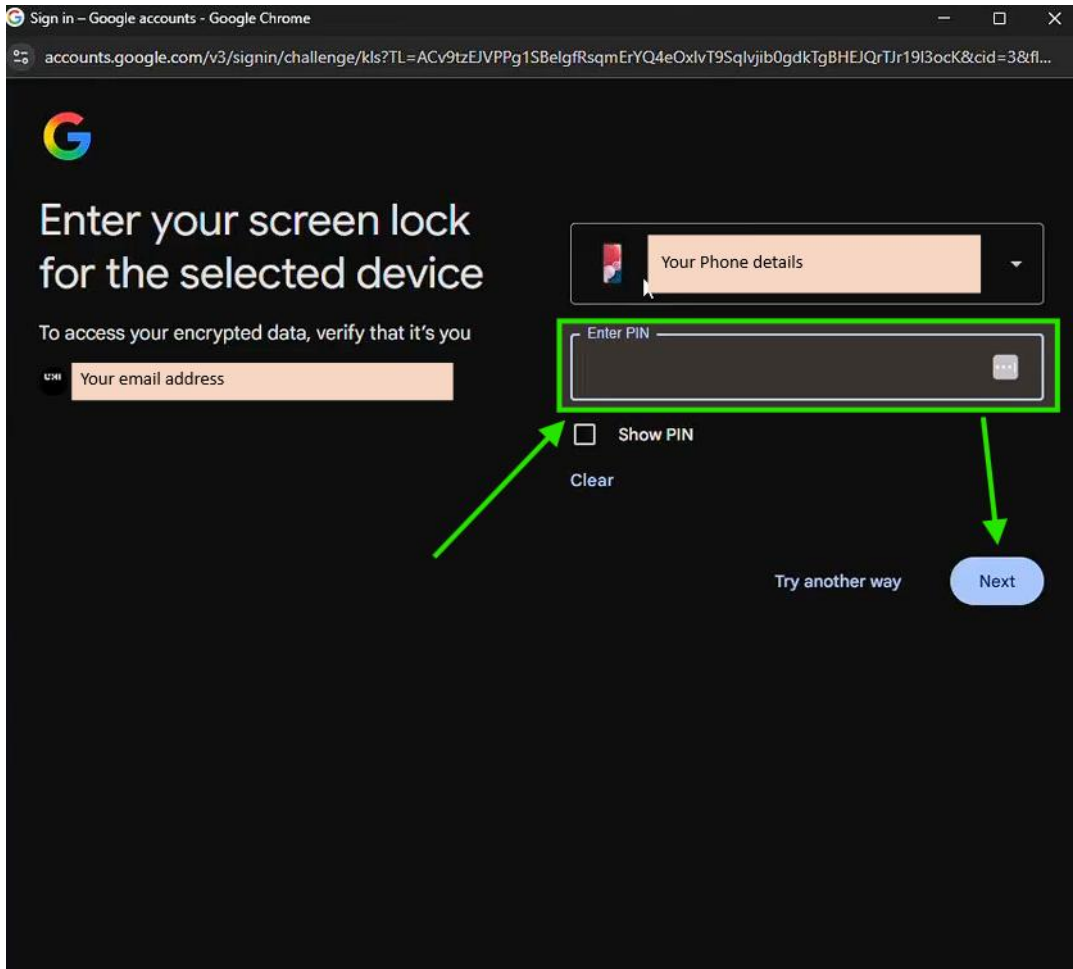


Figure 3. Confirm where the passkey will be saved

If the wrong Google account is shown: Select “Save another way” or cancel the process, check the active Chrome profile, and begin the setup again.

Step 4: Verify your device screen lock

Select the correct device if prompted. Enter the screen-lock PIN for that device, then select “Next”.



The screenshot shows the Google account sign-in page in a Chrome browser window. The page title is "Sign in - Google accounts - Google Chrome". The URL in the address bar is "accounts.google.com/v3/signin/challenge/kls?TL=ACv9tzEJVPPg1SBelgfRsqmErYQ4eOxlvT9Sqvjib0gdkTgBHEJQrTjr19I3ocK&cid=3&fl...". The main heading is "Enter your screen lock for the selected device". Below this, it says "To access your encrypted data, verify that it's you". There is a field for "Your email address" with a UHI logo. To the right, there is a dropdown menu labeled "Your Phone details" with a phone icon. Below this is a "Enter PIN" field, which is highlighted with a green rectangle. To the left of the PIN field is a "Show PIN" checkbox and a "Clear" link. At the bottom right, there are two buttons: "Try another way" and "Next". A green arrow points from the "Show PIN" checkbox to the "Enter PIN" field, and another green arrow points from the "Next" button to the "Enter PIN" field.

Figure 4. Verify using the selected device screen lock

Note: This prompt is asking for the screen lock of the selected device. It is not asking for your UHI account password.

Step 5: Create a Google Password Manager recovery PIN

If prompted, create a Google Password Manager recovery PIN and select “Confirm”. Keep this PIN secure and do not share it.

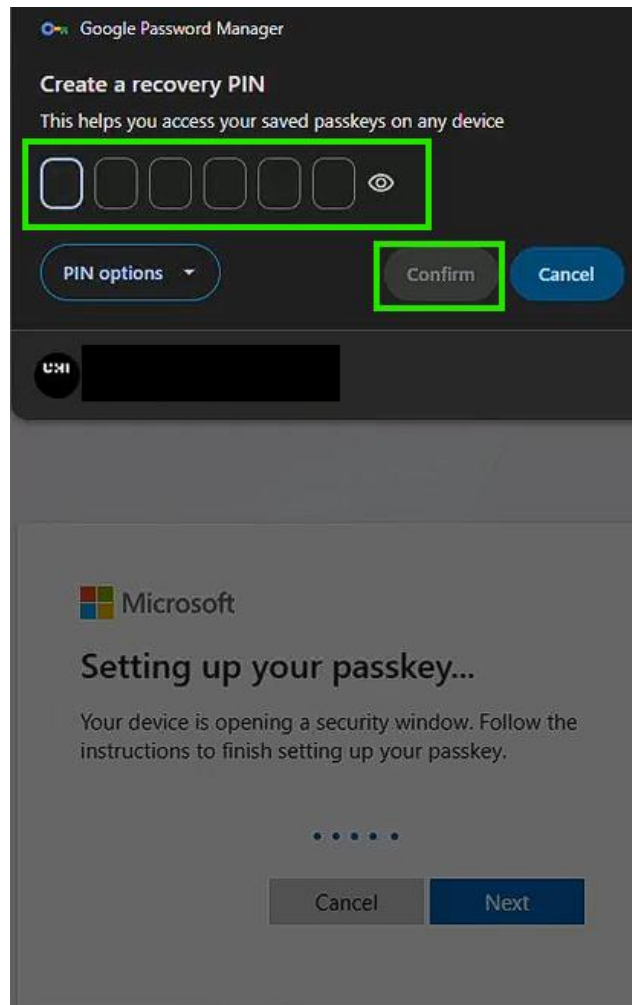


Figure 5. Create a recovery PIN

Step 6: Name the passkey

Enter a clear name that will help you recognise the passkey later, such as “Google Password Manager - personal laptop”, then select “Next”.

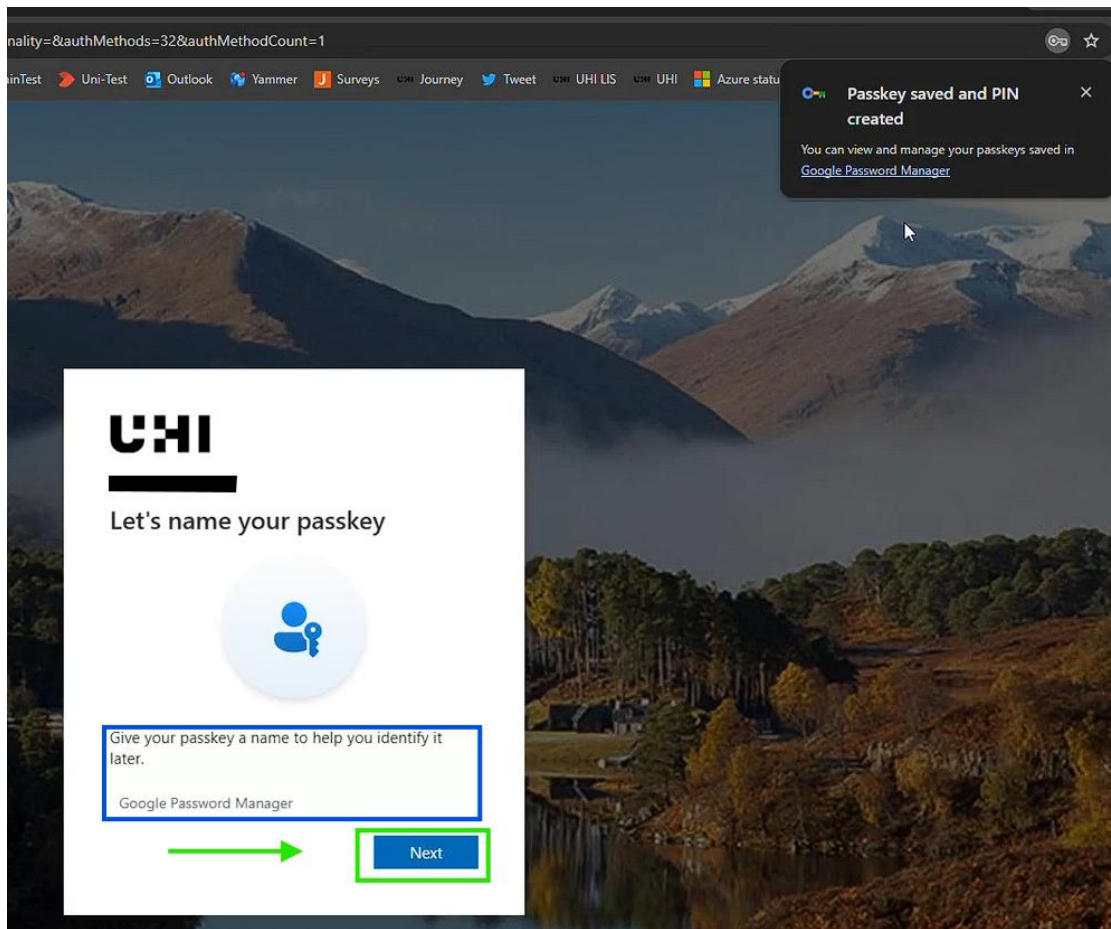


Figure 6. Give the passkey a recognisable name

Step 7: Finish the setup

When “Passkey created” appears, select “Done”.

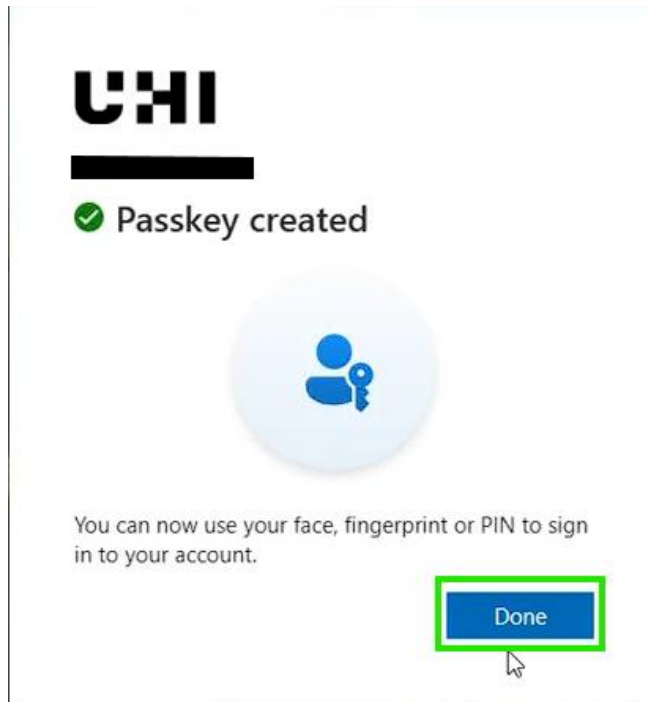


Figure 7. Finish the setup

Security reminder: Keep Microsoft Authenticator or another approved sign-in method registered until you have successfully used the new passkey.

Check That the Passkey Works

- Open a new Chrome window and start signing in to a UHI Microsoft 365 service.
- When offered sign-in options, choose the option for a passkey, face, fingerprint, PIN or security key.
- Approve the Google Password Manager prompt using the requested device verification.
- Confirm that you are signed in successfully.

Forgotten PIN

If the passkey is stored in Google Password Manager

If you created the passkey using Google Password Manager rather than Windows Hello:

- Open Chrome.
- Open Google Password Manager.
- Select “Settings”.
- Select “Change Google Password Manager PIN”.
- Authenticate, then create a new PIN.

If the passkey uses Windows Hello

A Windows Hello PIN is reset through Windows rather than Chrome:

- At the passkey PIN prompt, select “I forgot my PIN”.
- Verify your identity using a registered authentication method, such as Microsoft Authenticator.
- Follow the prompts to create a new Windows Hello PIN.
- Try signing in again using the new PIN.

If the Passkey Is Deleted or Unavailable

Sign in using another registered authentication method, such as Microsoft Authenticator. Open the Security info page for your UHI account, remove the old passkey entry if it is no longer valid, and create a replacement passkey.

No access to any authentication method? Contact the UHI Service Desk or your local ICT team. Provide your username and details of the issue, but never send your password, device PIN, Google Password Manager PIN or recovery information.

Manage or Remove the Passkey

A passkey has an account-side registration and a saved copy in Google Password Manager. When permanently removing it, review both your UHI Security info and Google Password Manager. Create and test a replacement method before removing one you rely on.