

Student: Set Up a Passkey Using Bitwarden

In brief: Bitwarden can store passkeys in your encrypted vault and offer them through its browser extension when a supported website requests a passkey.

Before You Start

- Make sure Microsoft Authenticator is already registered on your UHI account.
- Install the Bitwarden browser extension and sign in to your Bitwarden vault.
- Keep the Bitwarden vault unlocked while creating and testing the passkey.
- In the Bitwarden extension, check that Settings > Notifications > Ask to save and use passkeys is enabled.
- Make sure you can sign in to your UHI account and complete multi-factor authentication (MFA).
- Keep another authentication method registered in case Bitwarden is unavailable.

Important: Your Bitwarden master password, PIN and recovery information must not be shared with anyone, including the Service Desk.

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.

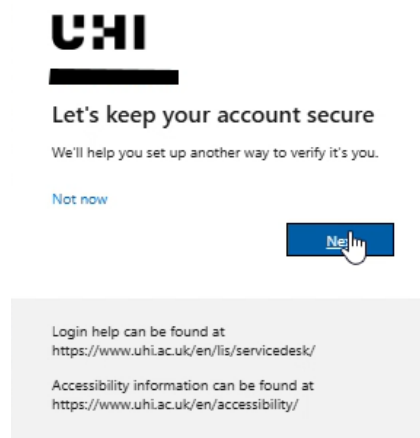


Figure 1. Continue from the security prompt

Step 2: Continue to passkey creation

Follow the Microsoft prompt to create a passkey. When the Bitwarden “Save passkey” window opens, confirm that the UHI login entry is displayed. Select the matching login item to save the passkey to it.

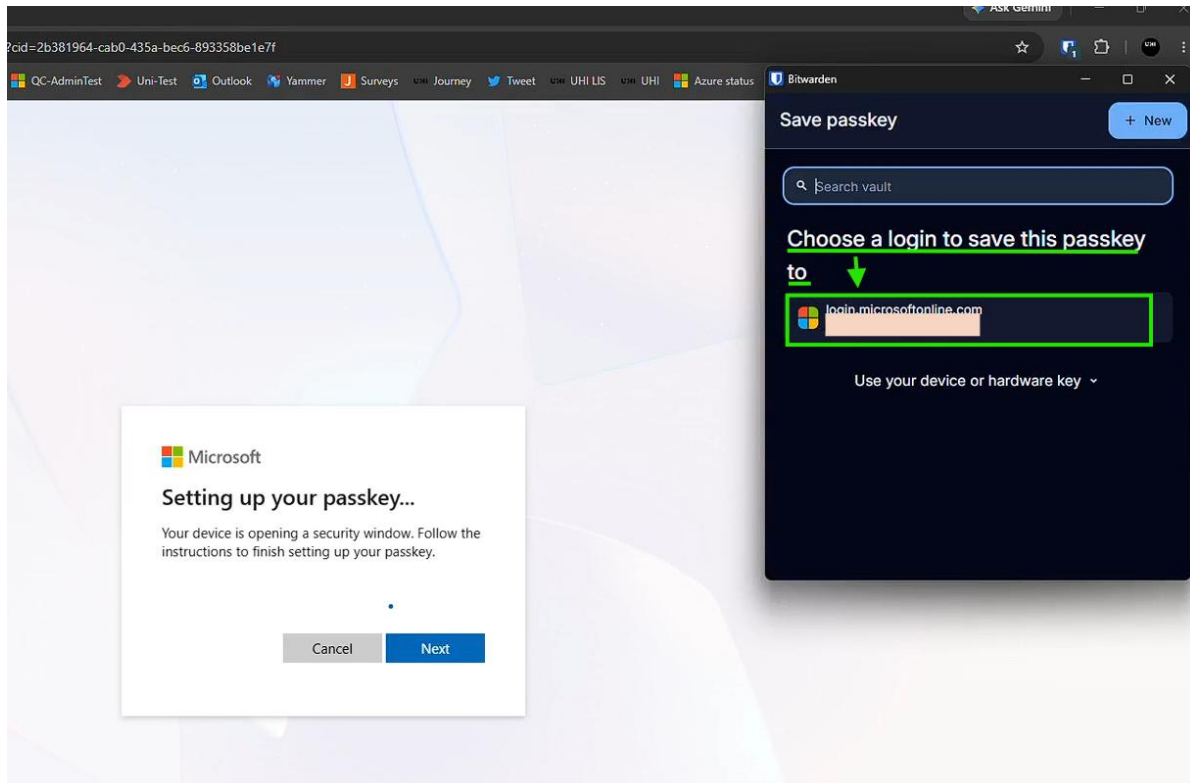
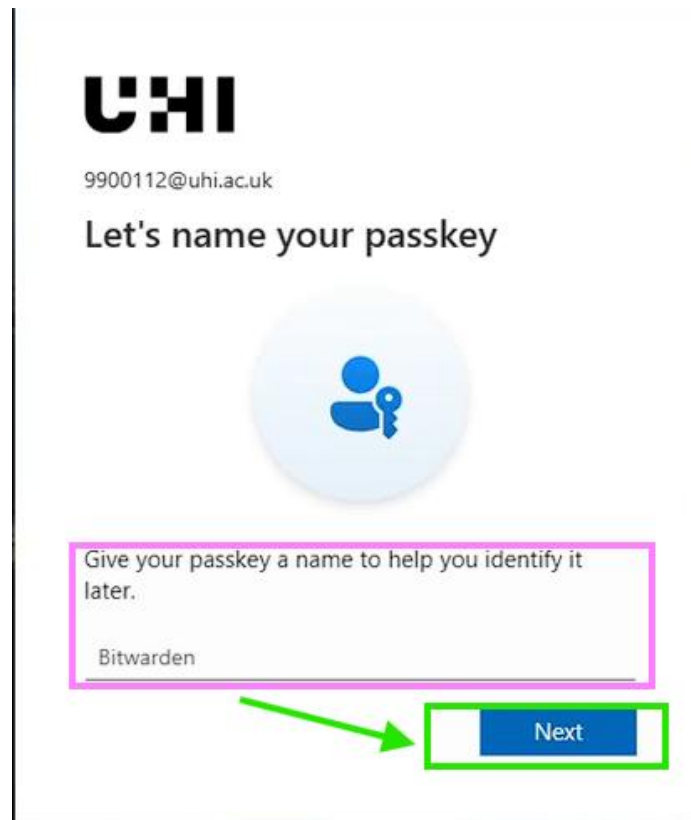


Figure 2. Continue to passkey creation

If the correct login is not shown: Use the option in Bitwarden to create a new login item, or cancel and check that the UHI account details stored in Bitwarden are correct.

Step 3: Name the passkey

When Microsoft asks you to name the passkey, enter a clear name such as “Bitwarden - personal laptop”, then select “Next”. The name helps you identify the passkey later in your account security information.



The screenshot shows the Microsoft account setup interface. At the top, the UHI logo is displayed above the email address 9900112@uhi.ac.uk. The main heading is "Let's name your passkey", accompanied by a blue circular icon containing a person and a key. Below this, a text box prompts the user: "Give your passkey a name to help you identify it later." The text "Bitwarden" is entered into the input field. A green arrow points from the input field to a blue "Next" button, which is also highlighted with a green border.

Figure 3. Name the passkey

Step 4: Finish the setup

When “Passkey created” appears, select “Done”. The passkey is now associated with your UHI account and stored in the selected Bitwarden vault item.

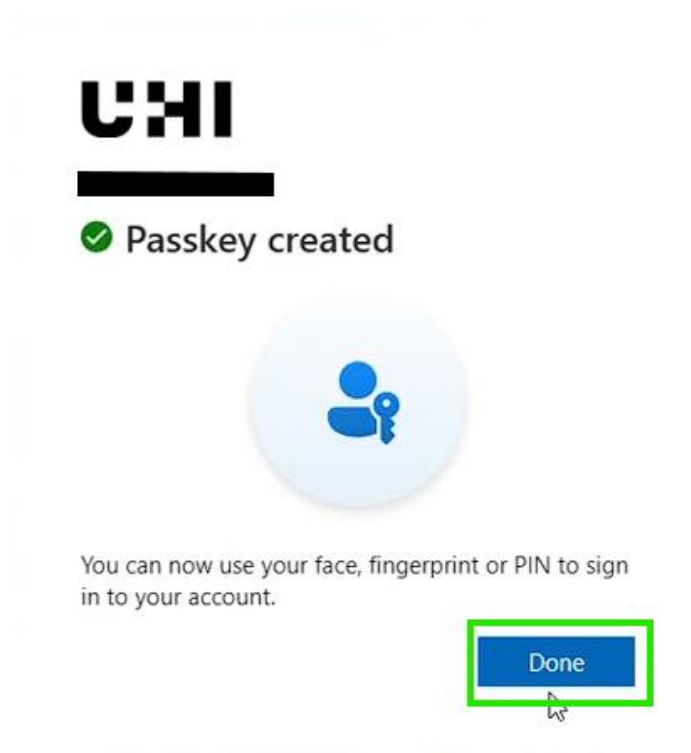


Figure 4. Finish the setup

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

Test the Bitwarden Passkey

Step 5: Choose the passkey sign-in option

Open a new browser tab and start signing in to a UHI Microsoft 365 service. If the password screen appears, select Sign-in options, then choose Face, fingerprint, PIN or security key.

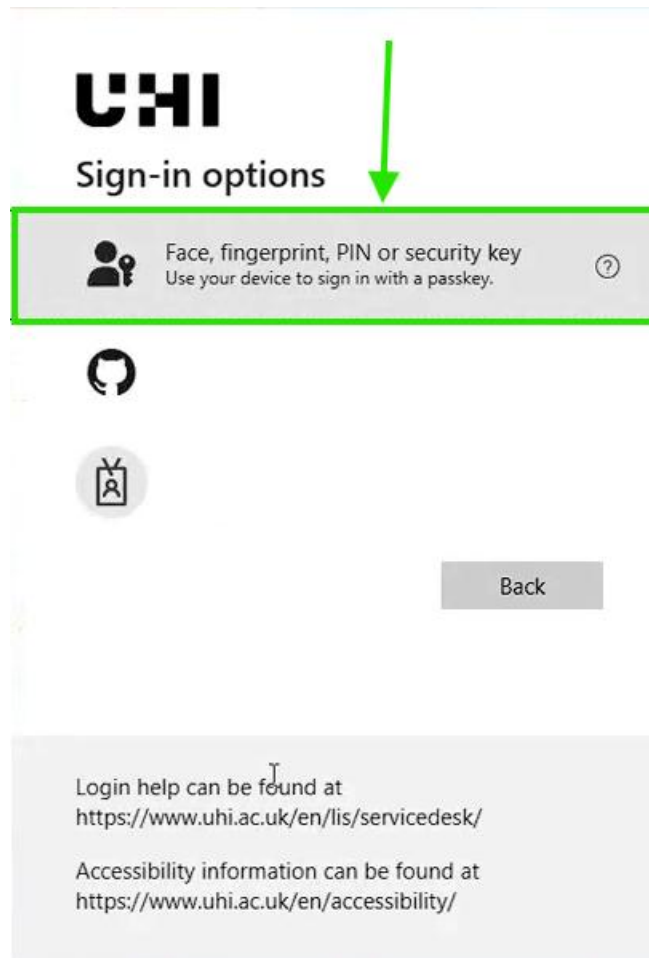


Figure 5. Choose the passkey sign-in option

Step 6: Select the saved Bitwarden passkey

When Bitwarden opens “Log in with passkey?”, select the UHI login item containing the saved passkey. If required, unlock your Bitwarden vault first, then approve the sign-in.

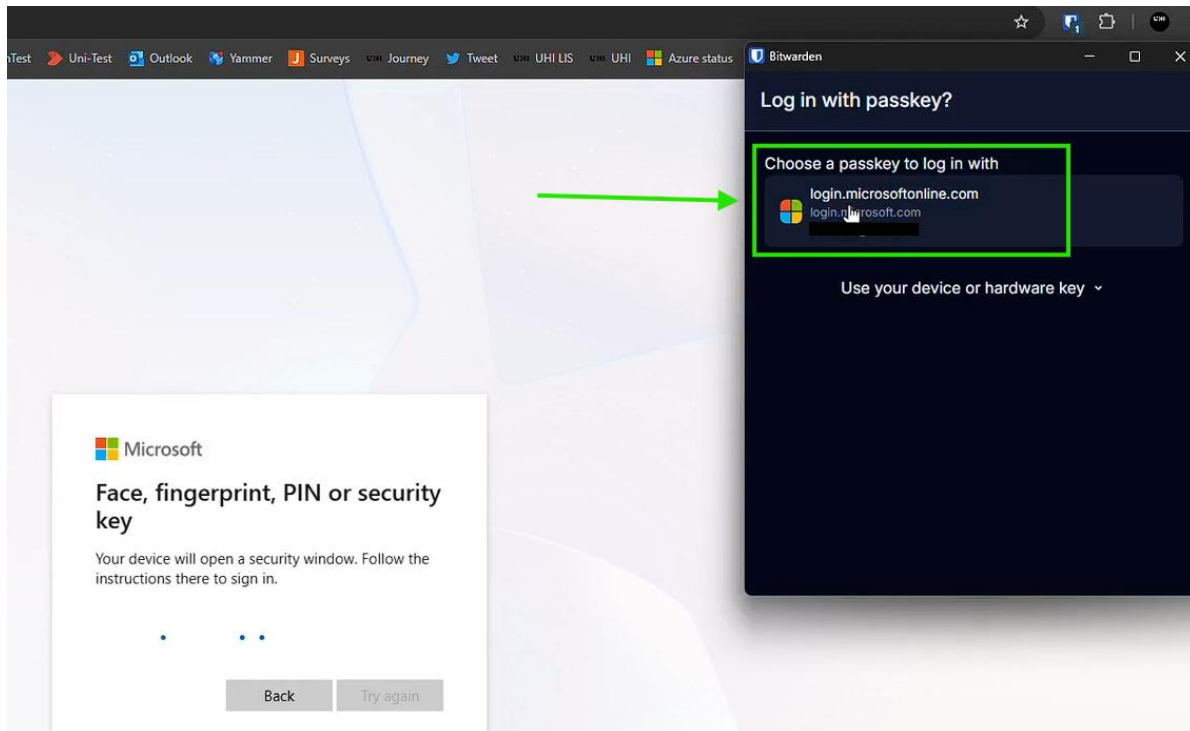


Figure 6. Select the saved Bitwarden passkey

Successful test: You should be signed in to the UHI service after approving the passkey through Bitwarden.

If Bitwarden Does Not Appear

- Check that the Bitwarden browser extension is installed, enabled, signed in and unlocked.
- Open the Bitwarden extension and confirm that Settings > Notifications > Ask to save and use passkeys is enabled.
- Check that the UHI sign-in domain has not been added to Bitwarden’s excluded domains.
- Refresh the sign-in page or close and reopen the browser, then try again.
- If another passkey manager opens instead, cancel that prompt and make sure the Bitwarden extension is allowed to save and use passkeys.

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. During setup, select the correct Bitwarden login item when the extension asks where to save it.

No access to any authentication method? Contact the UHI Service Desk or local ICT team. Provide your username and details of the issue, but never send your password, Bitwarden master password, PIN or

recovery information.

Manage or Remove the Passkey

A Bitwarden passkey has an account-side registration and a saved copy in your Bitwarden vault. When permanently removing it, review both your UHI Security info and the associated Bitwarden login item. Create and test a replacement method before removing one you rely on.