Frequently Asked Questions

Windows Hello for Business (WHFB) – Passwordless authentication

Updated: 7 Aug 2025

Windows Hello for Business (WHFB) provides a passwordless authentication login method that allows you to login to your University-managed device in a modern, convenient, and secure way. Passwordless allows you to choose a biometric method (depending on what is available on your device) and PIN to login instead of entering your zID password.

The WHFB is currently in pilot phase.

Please visit the Passwordless project page for more information, User Guide and other support materials. Contact the UNSW IT Service Centre for technical assistance. Please have ID verification with you.

Contents - Click on the question to be taken to the answer.

1. What is passwordless authentication?

Passwordless authentication is a method of verifying your identity without requiring you to input a password, making the authentication process simpler and more secure. With Windows Hello for Business, you can use:

- PIN
- Your fingerprint
- Face recognition

Note: Sign-in methods are limited by device hardware. You will be prompted for whichever methods are available on your device.

Return to Contents

2. What are the benefits of using passwordless login methods?

The key benefits of passwordless include:

- **Security**: Passwordless methods are more secure, as they are bound to the single device and reduce the risk of password-related threats such as phishing and stolen login details.
- **Convenience:** Passwordless authentication is often faster and more user-friendly than remembering and typing a password.
- **Better User Experience:** Passwordless methods are typically faster and easier for users, providing a smoother login experience.
- **Compliance:** When you log into your device using PIN/Biometric, this is a form of MFA, you will not need to MFA using Microsoft Authenticator.

Return to Contents

3. What are the risks to providing my biometric data?

Biometric data — such as fingerprints and facial recognition templates — is considered personal information under the **Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).** Because biometric identifiers are unique to you and tied to your body, they carry specific privacy risks. Unlike a password, your biometric data cannot be changed if compromised. A breach of this kind of information could have long-term consequences, such as identity theft or unauthorised surveillance.

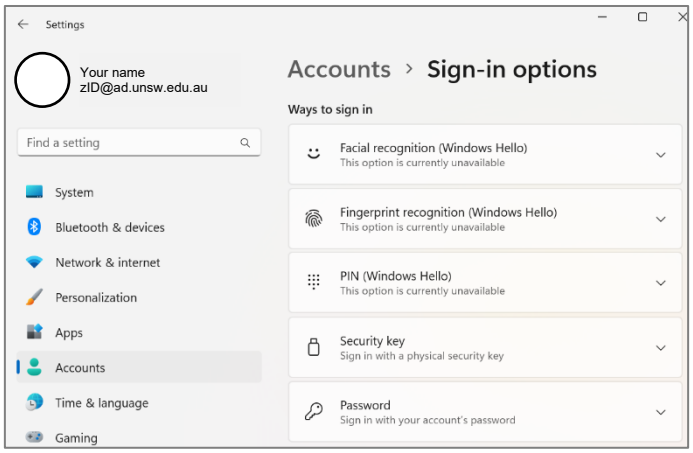
The WHFB system is designed with strong security protections. When you enrol, your biometric data is securely stored locally on your UNSW-issued device and is never transmitted to UNSW or Microsoft. The data is protected by hardware-based security using a Trusted Platform Module (TPM), which includes encryption, isolation, and tamper-resistant mechanisms. Any attempt to physically access the biometric data on the chip will render it inaccessible, making it extremely challenging for attackers to compromise.

While no system is completely immune to compromise, these safeguards significantly reduce the likelihood of unauthorised access. Even so, by enrolling, you should understand the nature of the data being collected, how it will be used, and that your participation in the trial is voluntary. UNSW adheres to strict privacy obligations under the PPIP Act and follows our internal Privacy Management Plan to minimise risks and ensure informed consent. If you have concerns or prefer not to use biometrics, an alternative login method is available.

Return to Contents

4. How do I know which biometric options my device supports?

On your device press the windows key and select **Settings** then **Accounts** and then **Sign-in options** for available ways to sign in on your device.



Note: When starting the setup process with Windows Hello for Business, your setup options will include all compatible biometric options available on your device.

Return to Contents

5. Is it mandatory to set up a PIN?

Yes**.** Your PIN can be used as an alternative when fingerprint or facial recognition methods fail. When setting up WHFB with fingerprint or facial recognition, follow the prompts to create a PIN.

UNSW requires a minimum of 6 characters (numbers, letters and special characters) for a PIN.

Return to Contents

6. Can I set up multiple biometric authentication methods such as fingerprint and facial recognition on my device?

Yes. Windows Hello for Business allows multiple biometric authentication methods to be configured simultaneously, provided your device has the necessary hardware (a fingerprint sensor and an infrared camera that supports Windows Hello for Business). Where biometrics are unavailable, your device will indicate "*This option is currently unavailable*."

Return to Contents

7. Does this mean I no longer have to remember my passphrase/password?

You still need to remember your password when logging into shared devices, devices that are not University-managed or where you have not set up Windows Hello for Business.

Return to Contents

8. What do I do if my camera or fingerprint fail to recognise me?

Your PIN can be used as an alternative when fingerprint or facial recognition methods fail. When setting up fingerprint or facial recognition, follow the prompts to create a PIN.

Return to Contents

9. Can I use Windows Hello for Business on a shared device?

No. WHFB is limited to university-managed Windows devices and will not be applicable to shared devices, e.g. in laboratories or the library.

Return to Contents

10. How can I reset my PIN if I forget it?

There are two ways to reset your PIN if you have forgotten it. You will need internet connection for both these methods.

Reset PIN from Settings

1. Sign-in to your device using your zID password.
2. Press the windows key and select **Settings** then **Accounts** and then **Sign-in options.**
3. Select PIN (Windows Hello) and then **I forgot my PIN** and follow the instructions.

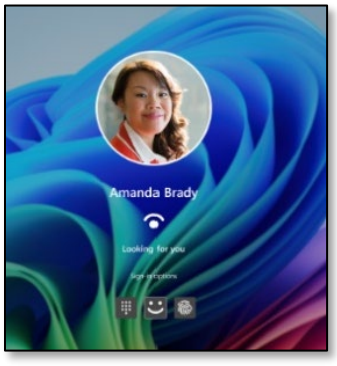
Reset PIN from the lock screen

1. On your lock screen, click the **Sign-in options** link, and select the **PIN pad icon.**
2. Select **I forgot my PIN.**
3. Select an authentication option from the list presented.
4. Follow the instructions provided.
5. When finished, unlock your desktop using your newly created PIN.

Return to Contents

11. Can I choose which login method I want to use after setting up Windows Hello for Business?

Yes. Once you have setup Windows Hello for Business, you will be presented with all eligible sign-in options on your lock screen for you to choose from:



- Password
  This is your current zID password.
- PIN
- Facial Recognition
- Fingerprint Recognition

Return to Contents

12. Does the face recognition work with my glasses, or a hat?

Yes. Face recognition usually works if you have a hat or prescription glasses on, however please:

- Remove any face coverings (such as face masks) for better recognition of your face.
- Poor lighting can impact the accuracy of the sensor. If you are in a poorly lit area, try turning on a light or moving to another location.

Return to Contents

13. Can I set-up Windows Hello for Business login on my Apple Mac device(s)?

Windows Hello for Business is specifically designed for Windows devices.

While Apple Mac devices support various forms of authentication like Touch ID, Face ID, and Apple's own passwordless options (via iCloud Keychain or Apple ID), they do not directly integrate with Windows Hello for Business.

Return to Contents

14. Can I set up Windows Hello for Business on my personal device(s) or my phone?

No. This capability is limited to University-managed Windows devices only.

Return to Contents

15. Where is Windows Hello for Business biometrics data stored?

When you enrol in Windows Hello for Business, a representation of your biometrics, called an enrolment profile, is created. The enrolment profile biometrics data;

- is device specific,
- is stored locally on the device in an encrypted format,
- does not leave the device,
- doesn't roam,
- never leaves the module, and is
- never sent to Microsoft cloud or external server.

Return to Contents

16. Why is a PIN or biometric gesture better than an online password?

A PIN or biometric gesture is local to a device. One important difference between a zID password and a biometric/PIN is that the biometric/PIN is tied to the specific device on which it is set up.

While someone who obtains your zID password can sign in to your account from anywhere, they can't do so if they obtain your PIN because it is tied to the device.

The PIN can't be used anywhere except on that specific device.

Return to Contents

17. What happens to my biometric if my device is stolen? Is it safe?

Please contact the UNSW IT Service Centre to report your stolen device immediately.

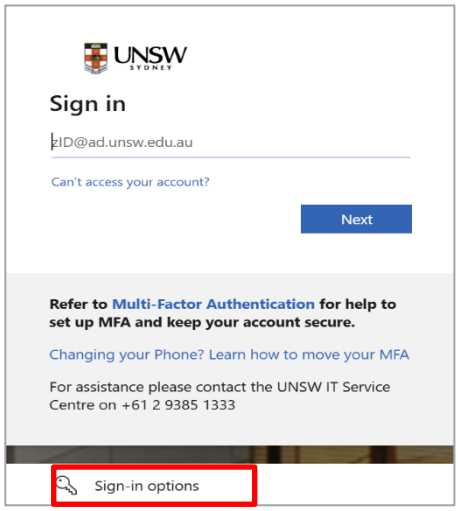
If your device is stolen, your biometric data, such as fingerprints or facial recognition, remain secure. Modern devices store biometric data in a secure enclave, which is a separate and isolated part of the device hardware.

Return to Contents

18. Does the PIN/Biometrics work with the Incognito or InPrivate window?

Yes. When accessing UNSW applications like SharePoint in Chromes' Incognito or Edges' InPrivate window, you will be prompted to sign in.

In this case you can continue to use your zID password or select Sign-in options where you can select your preferred method (PIN, Fingerprint, Facial).



Return to Contents

19. How many user profiles can enrol for Windows Hello for Business on a single Windows device?

The maximum number of supported enrolments on a single device is 10. This lets 10 users each enrol their face and up to 10 fingerprints.

Return to Contents

20. How can I wipe biometric data from my device?

You can wipe Windows Hello for Business and your biometric data from your device by running a command in Command Prompt.

1. To open the command prompt press windows key  +R to open the Run dialog.
2. Type cmd and press Enter.
3. In the command prompt window, type the following: certutil.exe -DeleteHelloContainer
4. Press Enter
5. In the same Command Prompt window, type: logoff.exe
6. Press Enter

This will sign you out and complete the deletion process.

Return to Contents

21. Will WH4B cause issues for mapping a Network Drive?

No, users doing the Network Drive mapping for first time will simply need to login first using their password and complete the mapping. Once the mapping setup is complete, users can access the Network Drive without issues.