Hardware tokens

A hardware token, or Security key, is a dedicated physical device held by an authorised user. It is a device that carries its own security PIN so as to grant access to computer resources. Physically, they are similar to a small USB stick that you plug into your computer.

Before you can set up a hardware token on your account, you must first set up another method of authentication.

The University will support the use of FIDO2 Hardware tokens. Departments, colleges or individuals will need to purchase and fund their preferred type of FIDO2 token themselves. After setting up a hardware token this will become your new first factor log in. There will be no requirement to enter an SSO password, this will be replaced by the hardware token.

Setting up a hardware token

1. Go to the Microsoft Account page
2. Click Security Info
3. On the security info page click +Add Method
4. In the drop-down menu click Security Key
5. Click Add

6. A warning message will populate explaining that you need to sign in with your multi-factor authentication method. Click Next

7. If prompted, enter your multi-factor authentication details

8. Pick what type of security key you have

9. A warning message will appear asking you to have your security key ready. The message will be different depending on whether you choose USB device or NFC device
10. Click **Next**

11. Your PC will direct you to a new window

![Image of the Windows Security window](image)

12. Enter your security key PIN. Make sure you enter a PIN you remember

13. Confirm the security key. You will see a different screen depending whether you used a USB device or an NFC device

![Image of the Windows Security window with a NFC prompt](image)

14. Enter a name for your key

![Image of the Security key window](image)
Multi-Factor Authentication Project
Setting up a hardware token

15. Click Next

16. The system will confirm that the hardware token is set-up appropriately

Security key

You're all set!
You can use your security key instead of a username and password the next time you sign in.
Be sure to follow your security key manufacturer’s guidance to perform any additional setup tasks such as registering your fingerprint.

17. The hardware token will appear on your security info page

Security info
These are the methods you use to sign into your account or reset your password.

<table>
<thead>
<tr>
<th>Default sign-in method: Microsoft Authenticator - notification Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add method</td>
</tr>
<tr>
<td><img src="image-url" alt="Security info image" /></td>
</tr>
</tbody>
</table>

![Security info image](image-url)
Making a hardware token your default sign-in method

Setting up a hardware token can only be done after another multi-factor authentication method has been set-up. This means that the hardware token is not your default sign-in method. This section will guide you through the process of how to make the hardware token your default sign-in method.

1. When you access an application or web page that is protected by SSO, the SSO account box will populate on the screen.

If you are already signed in and you don’t see this box you need to sign out of your account, close the application or web page and start again.

2. Click Use another account

3. The Oxford Single Sign-On page will display

Sign in
to continue to Outlook

Can’t access your account?
Sign in with a security key

Back Next
4. Click **Sign in with a security key**
   Depending on how you’ve accessed this page the line might say ‘*Sign in using a different method*’.

5. Either insert the USB hardware token and enter the PIN or touch the NFC key, whichever is your designated method.

6. Check that the account you want to access is displayed on the screen.
   If you have set up the hardware token for multiple accounts then a list of available accounts will appear.

7. Once you have the right account selected, or if there is only one available, click **Ok**

8. The multi-factor authentication process is complete and the hardware token is now the default sign-in method.
   For future sign-in processes, you will be prompted for the pin to unlock the hardware token, rather than username and password

**Resetting your hardware token**

The IT Services Service Desk doesn’t have the capability to reset the credentials for a hardware token. This must be done by the user. To reset your hardware token, follow the steps outlined in the guide on the Yubico website