

SET UP YOUR MICROSOFT 365 SIGN-IN FOR MULTI-FACTOR AUTHENTICATION

1 Introduction

The multi-factor authentication described in this document refers to signing into an **MS 365 Work or School account**. For the purposes of this document, a Microsoft 365 Work or School account is synonymous with a Microsoft Entra user ID.

The first time signing in to Microsoft Entra user ID on a **new device (phone, tablet, or PC)**, in a **web browser**, or after a **password change**, a user needs a username and password, as well as a second authentication method.

2 Phasing out of the Phone method

Microsoft will retire the Phone authentication method starting **1 September 2026**, with the service being fully discontinued on **1 February 2027**. Users who use only the Phone authentication method should register for and start using the **Microsoft Authenticator app** before the retirement date to avoid disruption to their sign-in experience.

3 MS 365 multi-factor authentication website

<https://services.nwu.ac.za/it-aos/microsoft-multi-factor-authentication-ms-mfa>

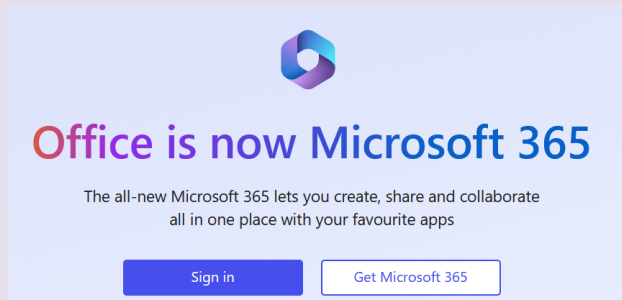
4 Methods

For a short-term strategy, Microsoft **recommends** using an authenticator app to secure a Microsoft Entra user ID. The long-term strategy is to use a phishing-resistant authentication method, such as a passkey. This will be implemented from 2027.

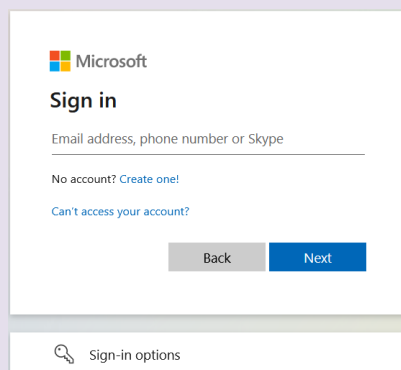
5 Steps to set up multi-factor authentication with the Authenticator App.

5.1 Here are the steps to set up the Microsoft Authenticator App as the primary MFA method.

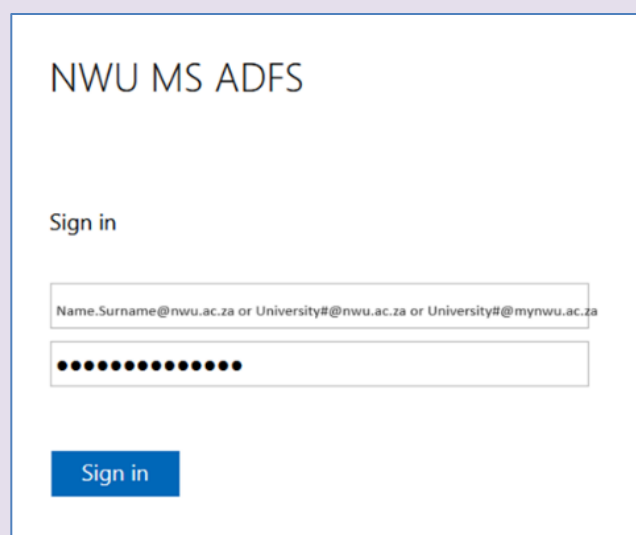
Sign in to your NWU account using a supported web browser (<https://www.office.com/>)



Click Sign in

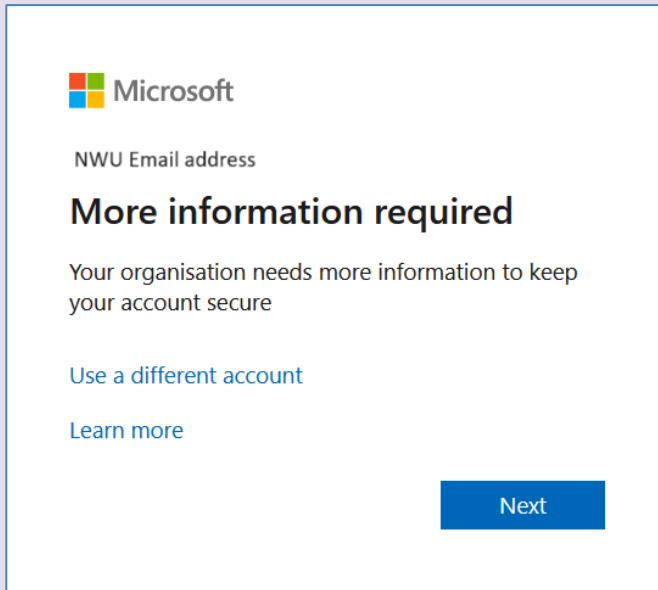
The image shows the Microsoft sign-in page. At the top is the Microsoft logo. Below it, the text "Sign in" is displayed. Underneath, there is a text input field labeled "Email address, phone number or Skype". Below the input field, there are two links: "No account? Create one!" and "Can't access your account?". At the bottom, there are two buttons: a grey "Back" button and a blue "Next" button. Below the main sign-in area, there is a section titled "Sign-in options" with a magnifying glass icon.

Enter your NWU email address and click Next.

The image shows the NWU MS ADFS sign-in page. At the top, the text "NWU MS ADFS" is displayed. Below it, the text "Sign in" is displayed. Underneath, there is a text input field labeled "Name.Surname@nwu.ac.za or University#@nwu.ac.za or University#@mynwu.ac.za". Below the input field, there is a password input field represented by a series of dots. At the bottom, there is a blue "Sign in" button.

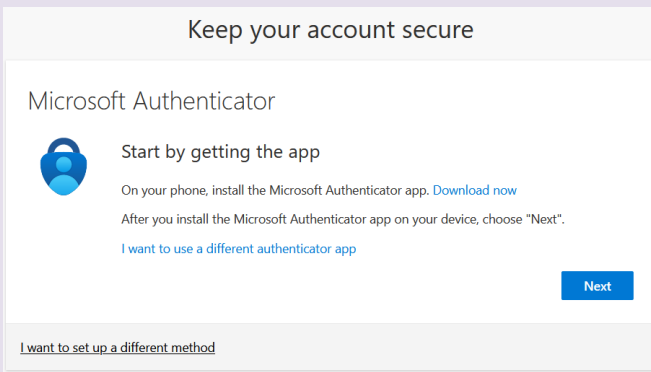
Enter your password and click Sign in.

**When MS MFA is activated for your account, Microsoft will prompt you for more information.
Click Next**



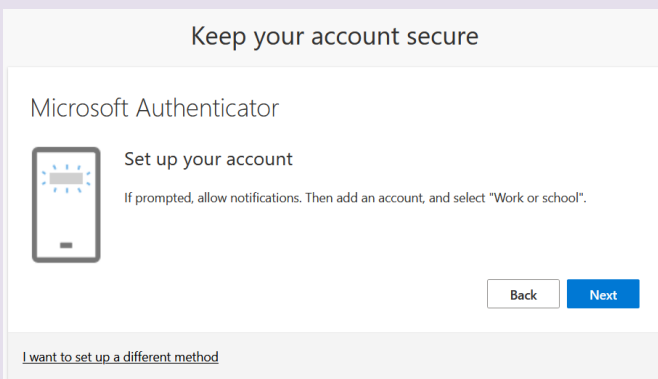
This screenshot shows a Microsoft login page titled 'More information required'. It features the Microsoft logo at the top left, followed by the text 'NWU Email address'. Below this is the heading 'More information required' and a message: 'Your organisation needs more information to keep your account secure'. There are two links: 'Use a different account' and 'Learn more'. At the bottom right is a blue 'Next' button.

Download and install the MS Authenticator app from **the relevant app store on your smart device**.



This screenshot shows the Microsoft Authenticator app setup screen. It has a header 'Keep your account secure' and the title 'Microsoft Authenticator'. Below is an icon of a person and the text 'Start by getting the app'. Instructions follow: 'On your phone, install the Microsoft Authenticator app. [Download now](#). After you install the Microsoft Authenticator app on your device, choose "Next".' There is a link 'I want to use a different authenticator app' and a blue 'Next' button. At the bottom left is a link 'I want to set up a different method'.

Click Next in the browser to continue setting up MFA.



This screenshot shows the Microsoft Authenticator app setup screen. It has a header 'Keep your account secure' and the title 'Microsoft Authenticator'. Below is an icon of a smartphone and the text 'Set up your account'. Instructions follow: 'If prompted, allow notifications. Then add an account, and select "Work or school".' There are 'Back' and 'Next' buttons. At the bottom left is a link 'I want to set up a different method'.

On your device in the Authenticator app: If prompted, allow notifications. Add an account in the app and select "**Work or school**".

In the Browser, click Next.

Keep your account secure

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".



Can't scan image?

Back

Next

[I want to set up a different method](#)

You will be prompted to **scan a QR code with your device**. Scan the QR code **with your device** and click Next in the Browser.

Keep your account secure

Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

78

Back

Next

[I want to set up a different method](#)

Microsoft will send a code to your device. **Enter the code in the Authenticator App on your device.**

Keep your account secure

Microsoft Authenticator



✓ Notification approved

Back

Next

[I want to set up a different method](#)

You will receive a message in the browser that the App was successfully added. Click Next.

Keep your account secure

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:



Microsoft Authenticator

Done

Click Done. The setup of MFA is complete.

6 Check your MS 365 MFA settings

- Use a browser to sign in to your [Microsoft 365](#).
- Select your avatar, then select **View account**.
- Select **Security info** from the left navigation pane to see the account's security information.
- The Security Info page displays your currently registered authentication methods and allows you to add additional sign-in methods. Please note that the Phone authentication method is being retired and will no longer be supported after 1 February 2027. We recommend registering the Microsoft Authenticator app as your preferred sign-in method.