2FA@NTU | Preparing for Two Factor Authentication (2FA) for the First Time for Alumni

Two Factor Authentication (2FA) provides an additional layer of security to protect against unauthorized access to NTU services and data. It requires two methods to verify your identity, which include (1) something you know i.e. your Office365 account username (i.e. username@e.ntu.edu.sg) and password, AND (2) something you have i.e. the Microsoft Authenticator app configured on your mobile device to authenticate access. This guide provides **detailed step-by-step instructions on how you can complete the one-time enrolment process to activate 2FA.**

❶ Install Microsoft Authenticator

a. You'll need both a computer and mobile device / smartphone to setup 2FA.

AND

b. Download and install the **Microsoft Authenticator app** on your iOS or Android mobile device.

NOTE: Microsoft Authenticator app is supported on iOS 12.0 & above AND Android 9.0 & above (varies by devices).

❷ Start the Enrolment

a. Login to www.office.com using your computer from the Internet.
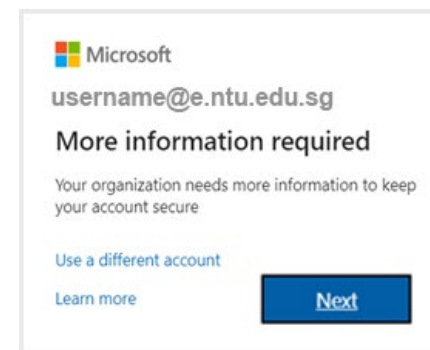
www.office.com

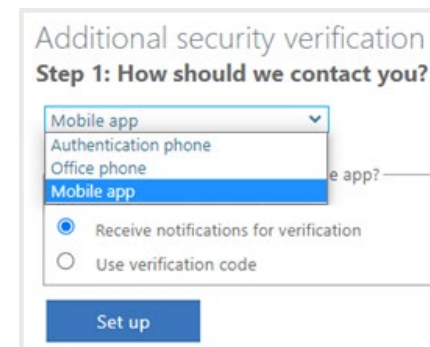Please sign in using your Office365@NTU account credentials in the following format:

username@e.ntu.edu.sg

❸ Configure App and Scan QR Code

a. When you logon click on **Next** to start the 2FA enrolment

Select **Mobile App** from the drop-down box then choose ⦿ **Receive notification for verification** and click **Set Up** Set up

b. Upon clicking the **Set Up** button, there will be a **QR Code** displayed on your computer that looks like this:
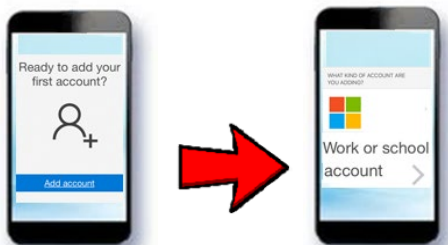

c. Launch the **Microsoft Authenticator** app on your mobile device and when prompted as shown below, select "**Allow**" notifications.

NOTE: Turn on notifications for the Microsoft Authenticator app so that you can receive notification on your phone when there is an access request.
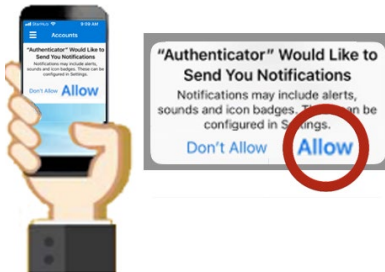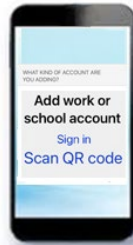

d. In the Microsoft Authenticator app,

select "**Add account**" ✚

and choose "**Work or School account**".

e. Select **Scan QR code**

Point your mobile device / smartphone camera to **scan the QR Code** on the web page.

NOTE: Make sure you allow the Microsoft Authenticator app to access your phone camera.
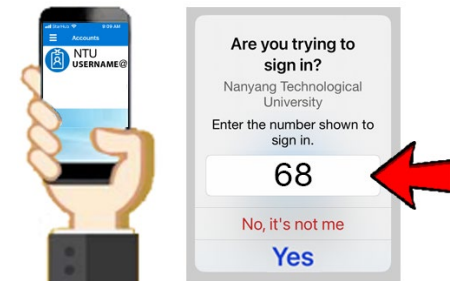

Click on **Next** [Next] on your computer.

❹ **Complete the 2FA Registration**

a. You will then receive an access request on your mobile device / smartphone.

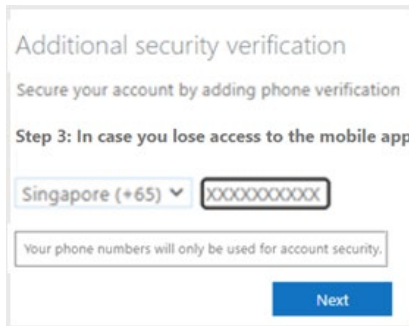On your mobile device / smartphone, **enter** the **number** shown on your computer (in this example is "68")

b. Click on "**Yes**" to complete the 2FA activation.

Your mobile device is now configured as a registered device for 2FA.

❺ Registering Your Mobile Number for Self-Service Password Reset and as an Alternative Backup to MS Authenticator

a. Next proceed to register your mobile number.

International number is supported. Click **Next**

b. Your setup is now fully completed. Click **Done**

Note: Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.
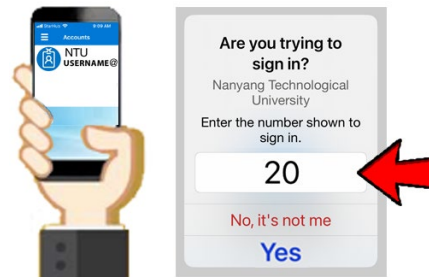
❻ Signing In to Office365@NTU

The next time you access www.office.com when your 2FA is activated you will <u>need</u> the registered mobile device / smartphone to authenticate the access.

a. Login to **www.office.com** through a web browser.

www.office.com
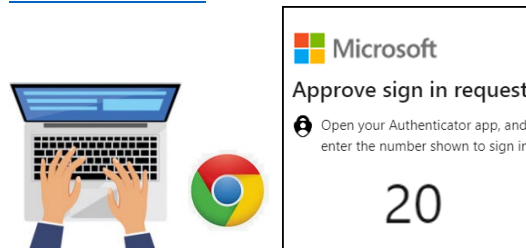
b. On your mobile device / smartphone, **enter** the **number** shown on your computer (in this example is "20") and click **"Yes"** to sign in.

c. You will then be logged in to **Office365@NTU**

NOTE: Microsoft caches user credentials for specific time duration. In most cases you will not be prompted to verify with 2FA for Office365 Apps (unlike web browsers) for **90 days** i.e. if you use the app on your mobile or computer more frequently than every 90 days.

Any changes that cause you to login again, such as a software update, will trigger 2FA verification. Things that could force you to re-authenticate:

- If you sign in and out of the Office clients again

- Not logged on for 14 days on that device

- Changed your password

- Software and App Updates after App restart

- Swapping between multiple Office 365 accounts

- Administrators applying conditional policies to restricted resources you are trying to access.