

NGEE ANN POLYTECHNIC

Multi-Factor Authentication (MFA) for O365 Guide

This document shows how to set up MFA and Passkey for your O365 account and answers frequently asked questions.

Please take note of the following:

If you are facing issues, please contact us at:

Email: ITCare@connect.np.edu.sg

Phone: 6460 8111

Multi-Factor Authentication (MFA) for Microsoft O365 Applications

Microsoft O365 applications are public cloud applications. It is possible that attackers use brute force to break into your account and compromise the data in your O365 apps.

As such, Multi-Factor Authentication (MFA) will be enabled to secure NP Apps such as Connect Email, MS Teams, OneDrive, POLITEMall etc.

What's the MFA Experience like?

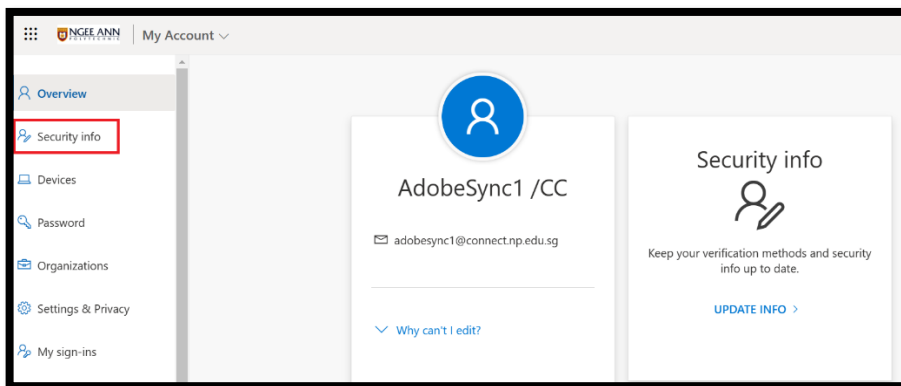
When an application is secured with MFA, you will be prompted for a MFA code/prompt when attempting to access the application from a computer/ iPad/ mobile **Web Browser**.

Other scenarios where you will be challenged for the MFA code /prompt are when:

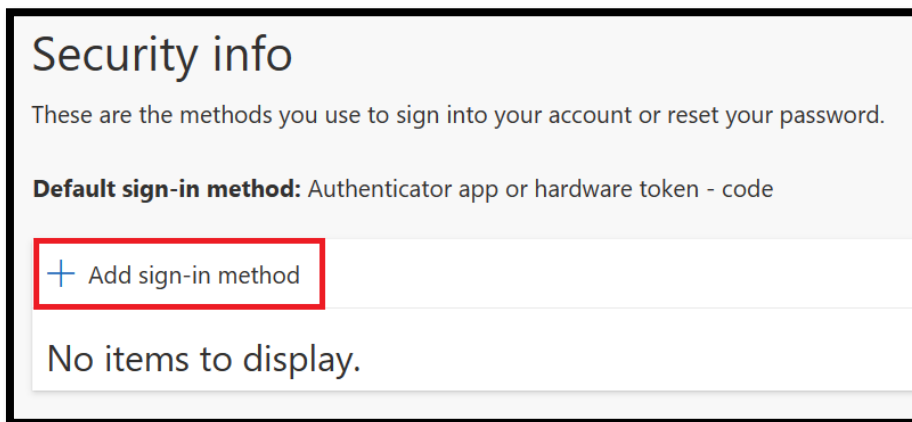
- you have changed your NPNet password
- you have removed Office credentials under Credential Manager
- you have changed notebook
- you are using Incognito or Private browsing

Steps to setup MFA prior to enforcement

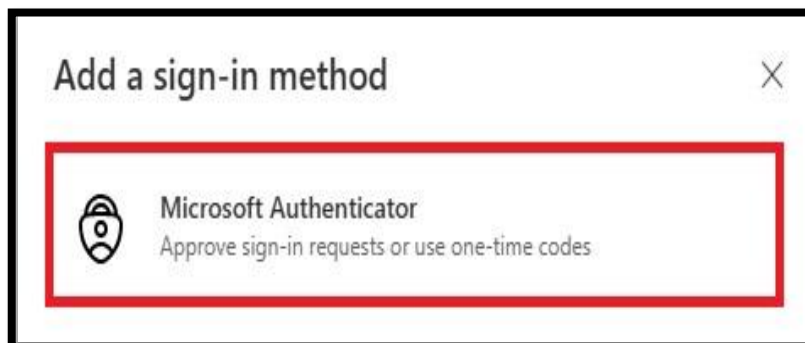
1. Using a computer, go to <https://myprofile.microsoft.com> using your Connect email address e.g. s12345678@connect.np.edu.sg and password.
2. Upon successful login, your name and email address will be displayed.
 - a. Click on **My Account > Security Info** option on the left menu bar.



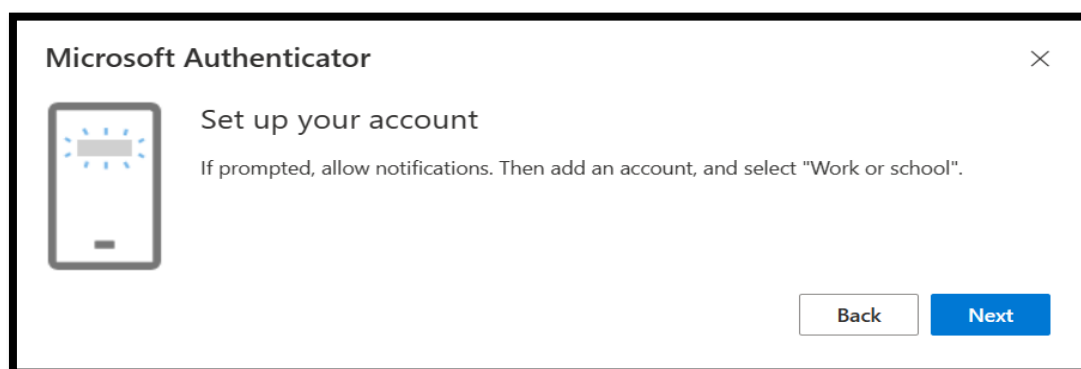
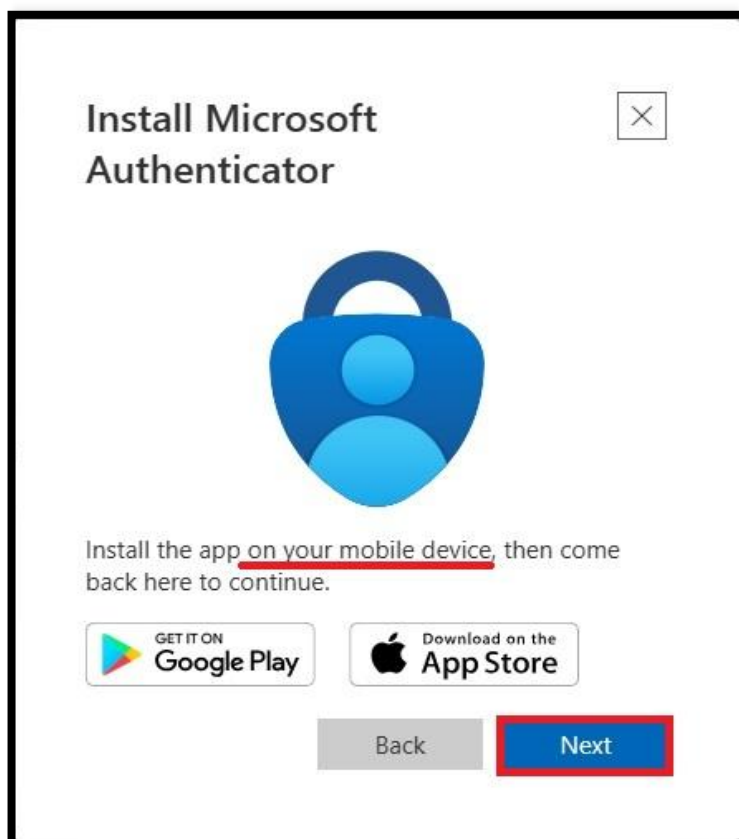
- b. Click on **+ Add sign-in method** in Security Info section.



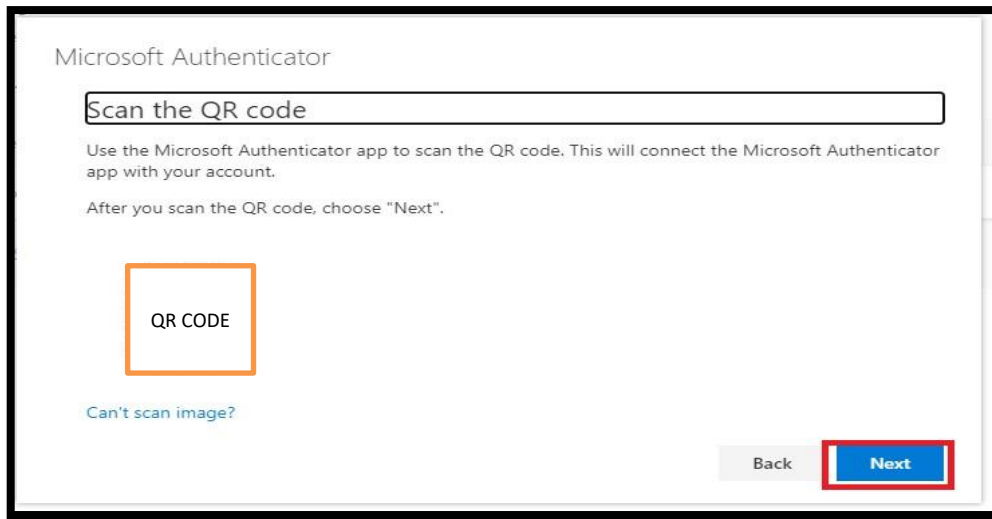
- c. Select the Microsoft Authenticator App.



3. You will be prompted to install the Microsoft Authenticator app on your **mobile device**. Download it from the App store for iOS devices or Google Playstore for Android devices. On your computer, click the **Next** button to generate a QR code. It will be needed.



4. After installation of Microsoft Authenticator app on your mobile device, click on **+** then choose “Work or school account”. Choose “Scan QR code”. Scan the QR code shown on the computer using your mobile device.



5. Upon successful installation, you will receive a notification alert on your mobile phone. Key in the number shown on the computer into the mobile device Authenticator app and you will see the 'Notification approved' prompt on your computer. Click the **Next** button to finish up.



6. Now that your Microsoft Authenticator MFA is working, please proceed to set up your **Passkey** by following the next section of this guide.

Introduction to Passkey

This section shows you how to set up and use Microsoft **Passkey** to sign in to your Microsoft 365 account. Please read it together with your phone and laptop on hand.

What is changing at NP

At present, you sign in using push-based MFA. After entering your password, you receive a prompt on the Microsoft Authenticator app and either approve it or key in a number shown on your laptop.

By switching to Microsoft **Passkey**, **you no longer need MFA codes, strengthen security against Adversary in the Middle (AITM) attacks and simplify authentication.** Once your Microsoft Passkey is set up, you will no longer approve push notifications. Instead, you confirm your sign-in using your phone's fingerprint, face, or screen lock. It is quicker, and there is no number to type.

Safer Cannot be guessed, copied, or phished.	Easier No number matching. Confirm using your phone lock.	Faster Sign-in usually takes only a few seconds.
--	--	--

What you need before you start

- Laptop/desktop with internet and a web browser.
- Mobile phone with working camera.
- Microsoft Authenticator installed and updated.
- Phone screen lock enabled: fingerprint, face, or PIN.
- Android 14+ / 15+ | or iOS 17+.
- Bluetooth ON for both laptop and phone.
- Keep laptop and phone close together during setup/sign-in.
- Do not close any screen until the final done message.

Section 1 – Setting Up Your Microsoft Passkey (One-Time Setup)

Step 1 and 2

Set aside about 5 minutes. Keep both laptop and phone nearby and online.

1. Open Security info

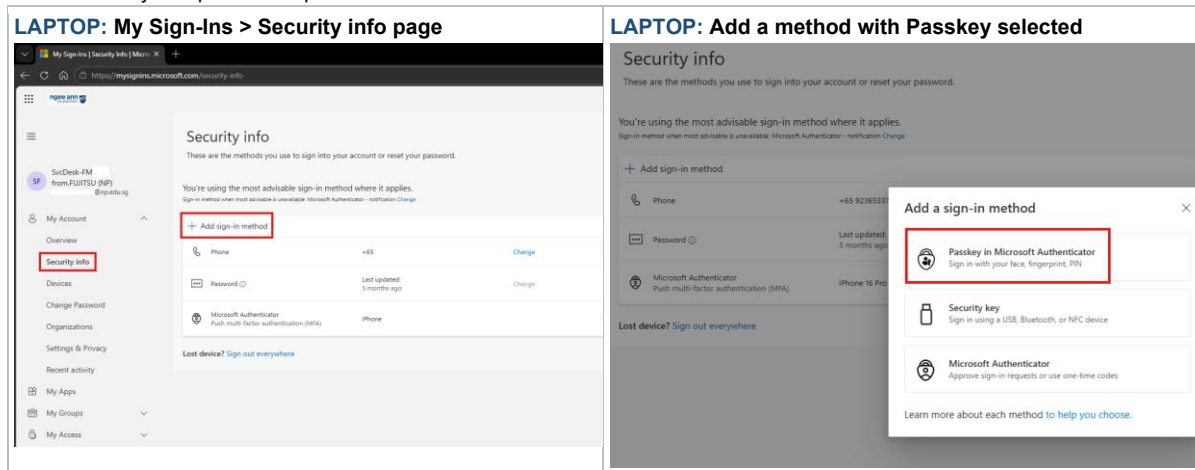
Do: Login to <https://mysignins.microsoft.com/security-info> from your laptop and sign in with your NP account,

Success: Your sign-in methods list appears.

2. Add Passkey in Microsoft Authenticator

Do: Click + Add sign-in method, choose Passkey in Microsoft Authenticator, then click Add.

Success: The Passkey setup window opens.



If you do not see the Microsoft Passkey option, update Microsoft Authenticator and try again. If it still does not appear, contact NP Service Desk.

Step 3 - Create the Passkey on your phone

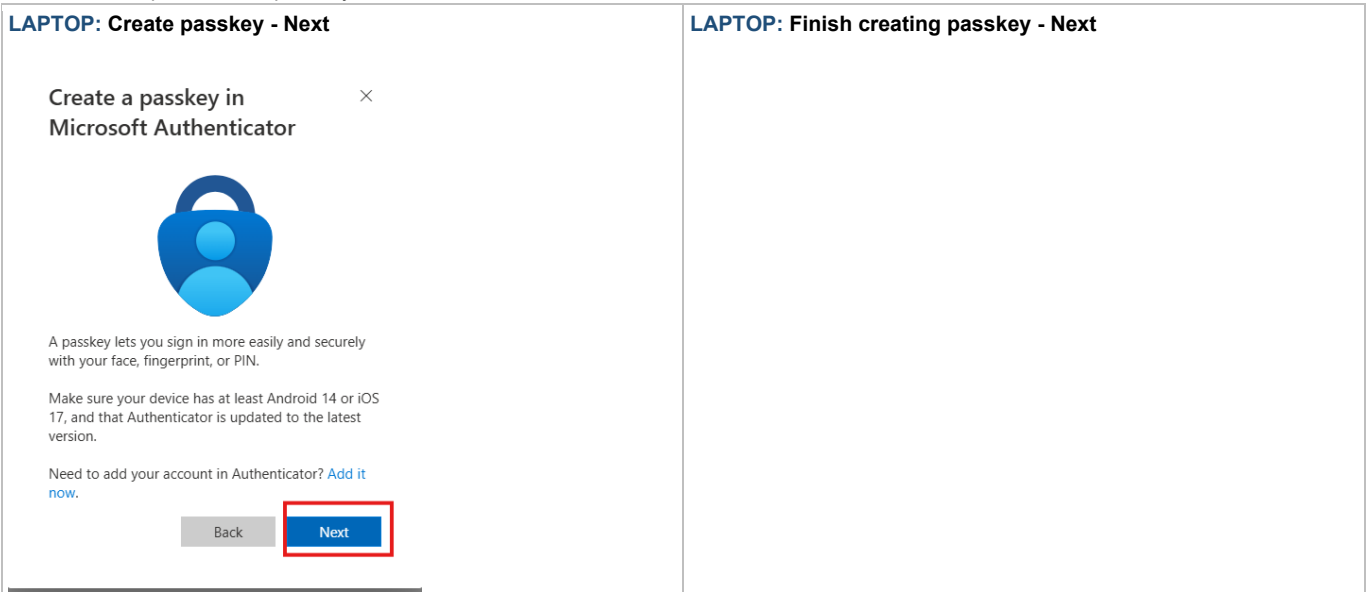
3. Continue on your phone

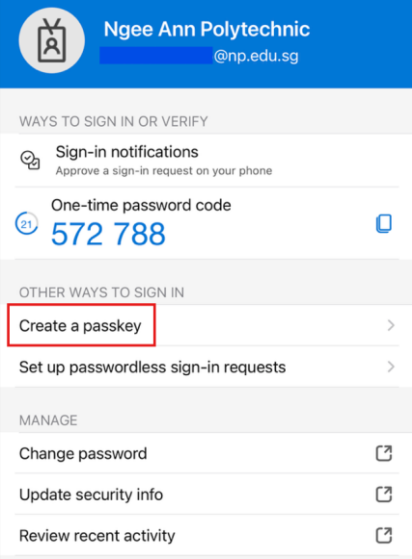
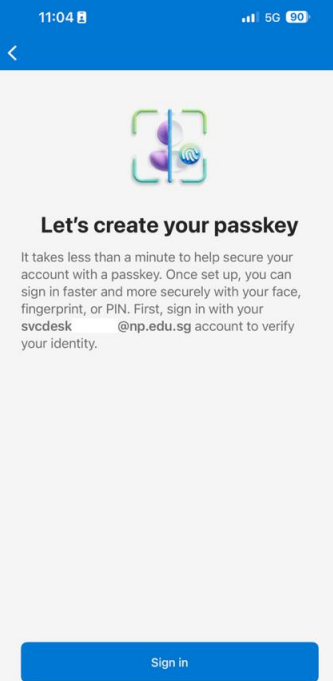
Do: On the laptop, click Next. On your phone, open Microsoft Authenticator, tap your NP account, and select Create a passkey.

Laptop: A Continue / Next screen is shown.

Phone: Authenticator shows the Create a passkey option.

Success: The phone starts passkey creation.



	Finish creating your passkey ✕ in Authenticator  1. In Authenticator select your work or school account, svcdesk-@np.edu.sg. 2. Select Create a passkey and follow the instructions in the app. Make sure your device has at least Android 14 or iOS 17, and that Authenticator is updated to the latest version. Need to add your account in Authenticator? Add it now. Having trouble? Back Next
MOBILE: Authenticator > Create a passkey 	MOBILE: Let's create your passkey - Sign in 

Keep the laptop screen open while completing the phone prompts.

Steps 4-5 - Confirm and finish setup

4. Confirm with phone lock

Do: Use fingerprint, face, or PIN on your phone.

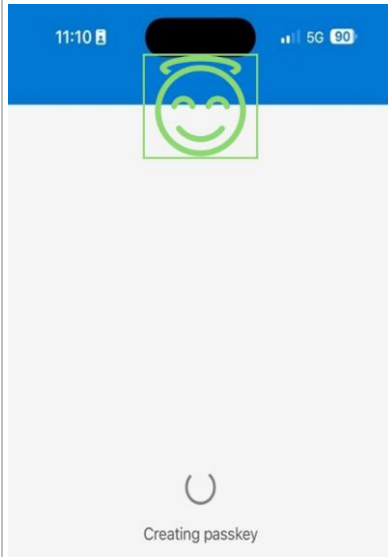
Success: The phone shows the Passkey has been created.

5. Finish setup

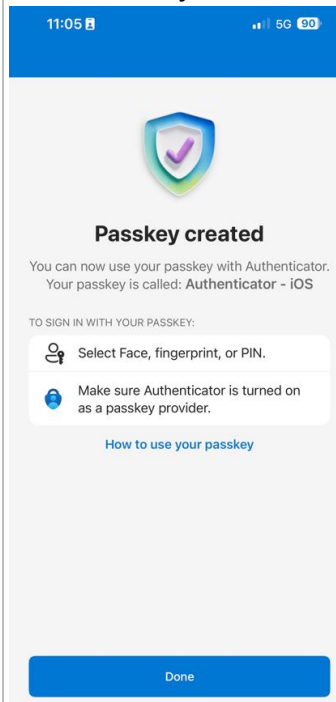
Do: Click Done if prompted. You may then close the browser tab.

Success: Security info shows Passkey in Microsoft Authenticator.

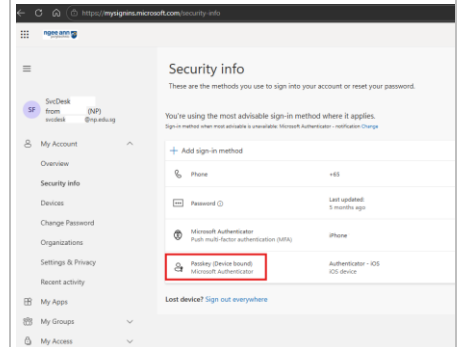
MOBILE: Fingerprint / Face / PIN confirmation



MOBILE: Passkey created



LAPTOP: Security info showing new Passkey



Well done - your Microsoft Passkey is now set up. Use the next section when signing in after setup.

Section 2 - Sign in after your Microsoft Passkey is set up

After setup, a QR code may appear when signing in to an NP system or Microsoft 365. You complete the sign-in on your phone.

- Use your phone CAMERA app. If your device is unable to scan the QR code using the native camera, you may use the scanner within the MS Authenticator app as an alternative.
- Do NOT close the QR code screen on your laptop until sign-in completes.

Step 1

1. Sign in on your laptop as usual

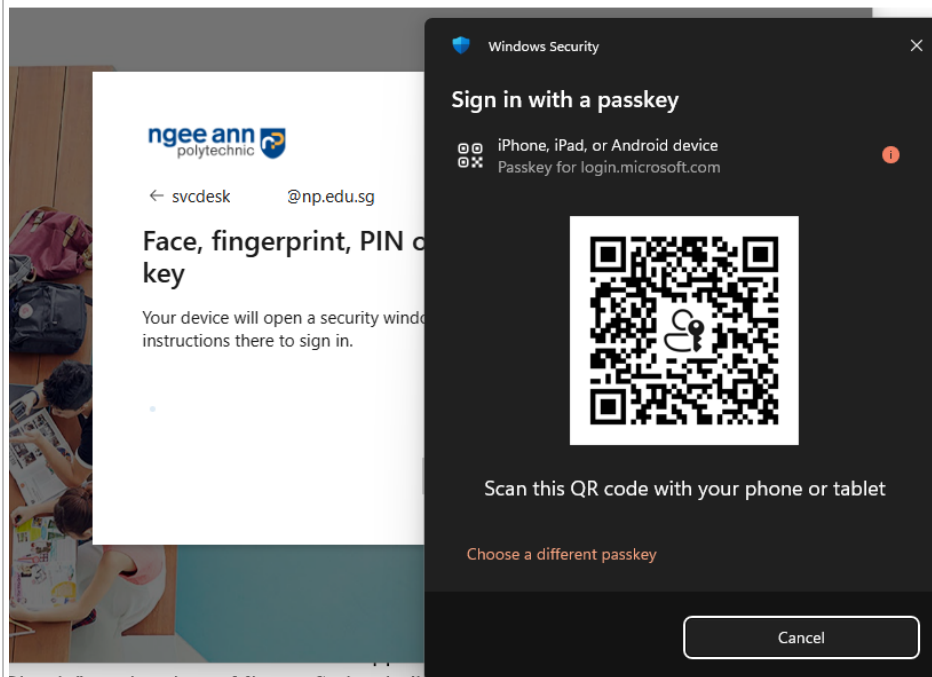
Do: Open [Microsoft 365](#) in **New In-Private Window** in Edge, enter your NP email/password, then wait for the QR code.

Laptop: QR code appears.

Phone: No action yet.

Success: A clear QR code is shown on the laptop.

LAPTOP: NP QR code sign-in screen



Steps 2-3 - Scan with Camera and tap the link

2. Open the phone Camera app

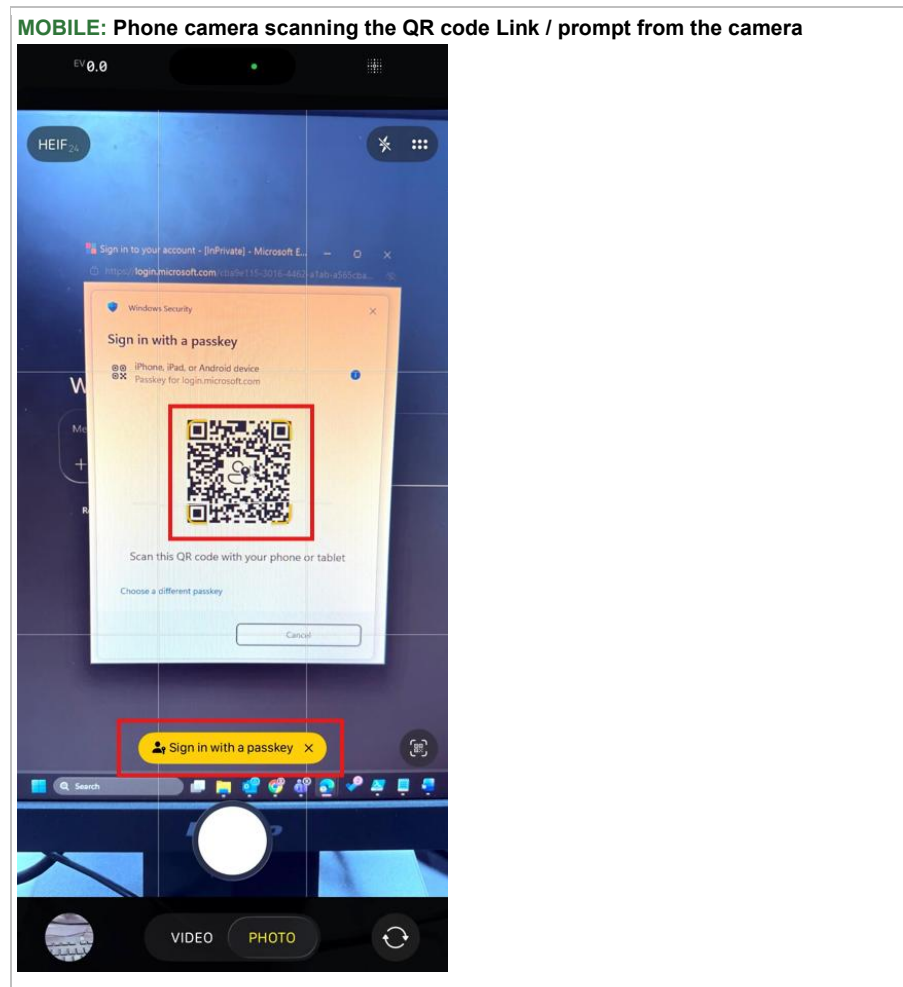
Do: Open the normal phone Camera app and point it at the QR code on the laptop screen. If your device is unable to scan the QR code using the native camera, you may use the scanner within the MS Authenticator app as an alternative.

Success: A small link or banner appears on your phone.

3. Tap the link or prompt

Do: Tap the link or notification that appears. It opens a Microsoft sign-in page or prompt on your phone.

Success: The sign-in confirmation page opens on your phone.



Step 4 - Confirm the sign-in on your phone

4. Use fingerprint, face, or PIN

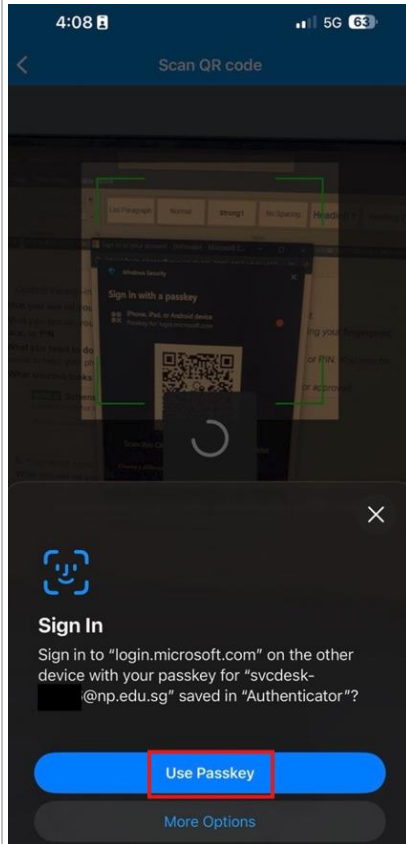
Do: Confirm using your phone screen lock. Keep your phone close to your laptop if prompted.

Laptop: Laptop waits with the QR code.

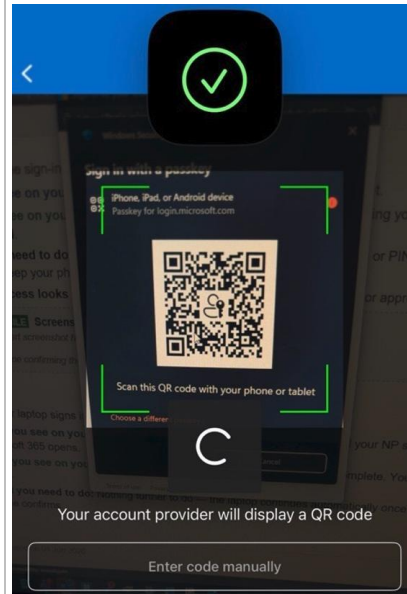
Phone: Phone asks you to confirm.

Success: Phone shows sign-in confirmed/approved.

MOBILE: Sign-in prompt opened from QR link



MOBILE: Sign-in confirmation screen



If the QR code expires or the screen is closed too early, start again and keep the QR code open until the phone confirms.

Step 5 - Laptop signs in automatically

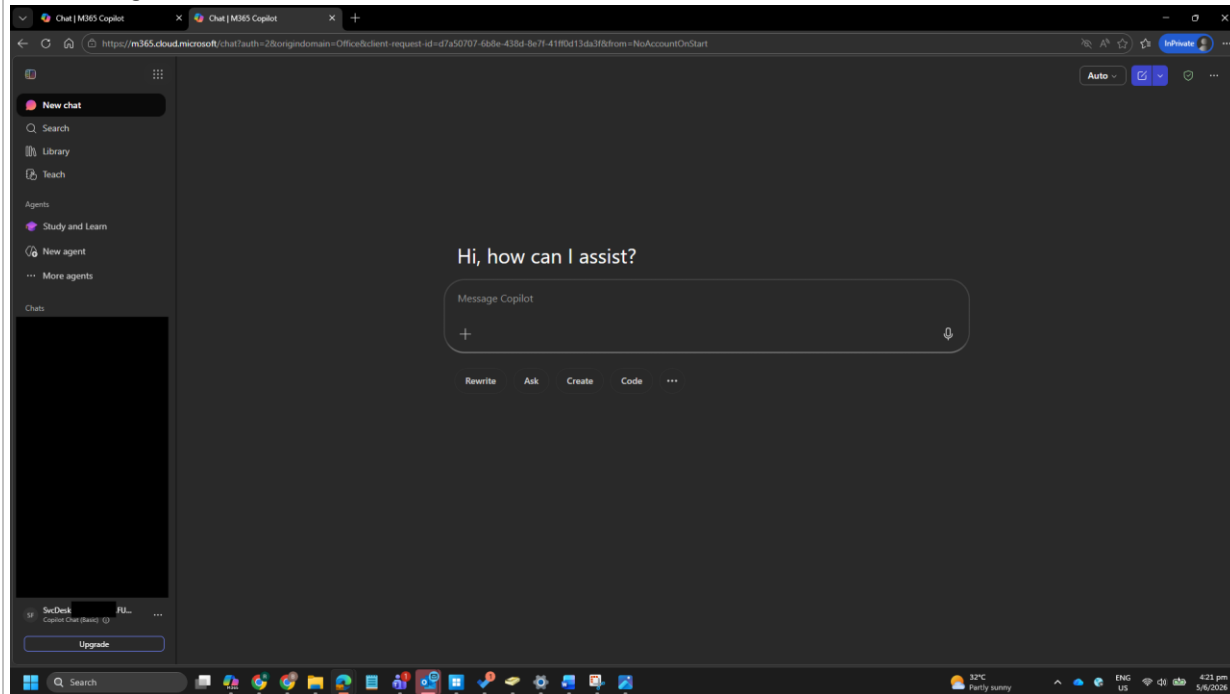
5. Finish sign-in

Do: After your phone confirms, wait for the laptop to continue automatically.

Laptop: QR code screen closes and the NP/Microsoft 365 page opens.

Phone: Sign-in complete. **Success:** You are signed in on the laptop.

LAPTOP: Signed-in NP / Microsoft 365 screen



Section 3 - What happens next

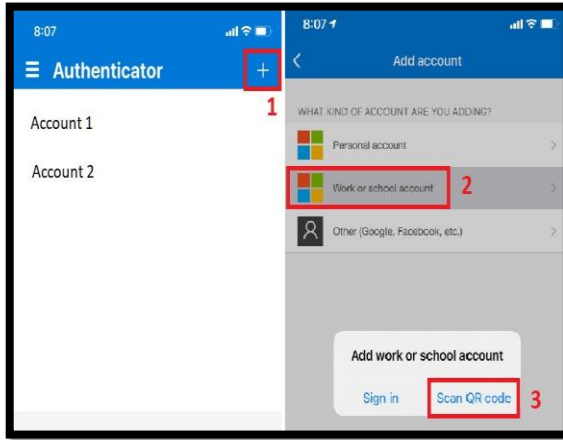
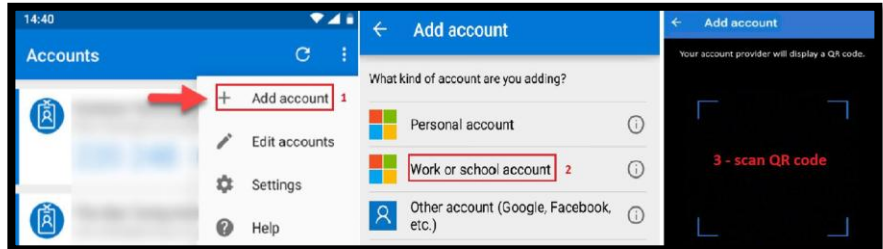
Future NP sign-ins will use your Passkey. Usually this means scanning the laptop QR code with your phone Camera app, then confirming with fingerprint, face, or PIN.

Push notifications and number matching will no longer be used after the Passkey is active.

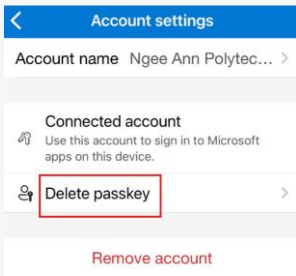
On a new or shared laptop, use the same QR code sign-in steps. Your Passkey stays safely on your phone.

If you change phone, install/update Microsoft Authenticator and set up the Passkey again on the new phone.

Quick FAQ / troubleshooting

No	Question	Answer
1	I already have an existing account on my MS Authenticator app, how do I add a new account?	For iOS:  For Android:  Why this happens: Your Microsoft Authenticator app may be out of date, or the Passkey option may not have reached your account yet. What to do: On your phone, open the App Store (iPhone) or Google Play Store (Android) and update Microsoft Authenticator to the latest version. Then return to https://myprofile.microsoft.com > Security info > + Add sign-in method and look for Passkey in Microsoft Authenticator. If it still does not appear, please contact the NP Service Desk.
2	I don't see the option to set up a Passkey.	Why this happens: Some sign-in screens ask you to first choose how you want to sign in, so the QR code may not appear straight away. What to do: On the sign-in screen, look for an option such as "Sign in with a Passkey" or "Use Face, fingerprint, PIN or security key" and select it. The QR code should then appear. If you only see options to approve a notification, your Passkey may not be set up — please follow Section 1 first.
3	I don't see a QR code when signing in.	Why this happens: Some sign-in screens ask you to first choose how you want to sign in, so the QR code may not appear straight away. What to do: On the sign-in screen, look for an option such as "Sign in with a Passkey" or "Use Face, fingerprint, PIN or security key" and select it. The QR code should then appear. If you only see options to approve a notification, your Passkey may not be set up — please follow Section 1 first.

No	Question	Answer
4	I opened Microsoft Authenticator instead of the camera.	Why this happens: During setup you used the Authenticator app to scan a QR code, so it is easy to do the same out of habit. What to do: It is okay to use the scanner in your MS Authenticator app to scan the QR code. Tap the link that appears, then confirm with your fingerprint, face, or PIN.
5	My phone camera doesn't detect the QR code.	Why this happens: The camera may be too close or too far, the screen may be dim, or your camera app may be old. What to do: Hold your phone about 15–25 cm from the laptop screen and keep it steady so the whole QR code is in view. Increase your laptop screen brightness. Make sure nothing is blocking the camera lens, and that your phone's software is up to date. If it still fails, refresh the laptop sign-in page to show a new QR code and try again.
6	I changed or replaced my phone.	Why this happens: Your Passkey is stored securely on your old phone and does not move across automatically. What to do: On your new phone, install and set up Microsoft Authenticator with your NP account, then follow Section 1 of this guide to set up your Passkey again. If you can no longer sign in to do this, please contact the NP Service Desk for assistance.
7	I deleted Microsoft Authenticator.	Why this happens: Removing the app also removes the Passkey stored in it. What to do: Reinstall Microsoft Authenticator from the App Store (iPhone) or Google Play Store (Android), sign in with your NP account, and set up your Passkey again using Section 1. If you are unable to sign in, please contact the NP Service Desk.
8	My phone is lost.	Why this happens: Your Passkey is on the lost phone, so you cannot use it to sign in. What to do: Please contact the NP Service Desk as soon as possible. We can temporarily help you sign in and set up your Passkey on a new phone. For your security, report a lost phone promptly.
9	I don't have internet on my phone.	Why this happens: Setting up and using a Passkey needs your phone to be online for part of the process. What to do: Connect your phone to Wi-Fi or mobile data, then try again. If you are on NP premises, you may connect to the NP Wireless. Once your phone is online, repeat the sign-in steps in Section 2.
10	I keep getting sent back to the sign-in page.	Why this happens: The sign-in may have timed out, the QR code screen may have been closed too early, or your browser may be holding old sign-in information. What to do: Start again and leave the QR code screen open until your phone confirms the sign-in. If it keeps happening, close all browser windows and try again, or use a private/incognito browser window. If the problem continues, please contact the NP Service Desk.

No	Question	Answer
11	What are the minimum device requirements for Passkey?	Android - Minimum OS version: Android 14 or later iOS (Apple) - Minimum OS version: iOS 17 or later Authenticator app must be updated to the latest version.
12	I get an error when creating passkey (Android / iOS Device)	Why this happens: The error may occur if your Android/iOS version does not support passkeys, the Microsoft Authenticator app is outdated, or your device model does not support passkey functionality (common on older devices). What to do: Update your Android/ iOS and ensure the Microsoft Authenticator app is on the latest version. If the issue persists, try creating the passkey on a different supported device. If the problem continues, please contact the NP Service Desk.
13	I am unable to add passkey, while setting up.	Why this happens: The Microsoft Authenticator app may not be registered correctly, or the account configuration may be outdated. What to do: Ensure Microsoft Authenticator is installed and updated to the latest version. Verify that the correct NP account is added in the app. Delete the Passkey (by accessing the account settings and delete the passkey as shown below) for that account and re-set up the passkey again.  The screenshot shows the 'Account settings' screen in the Microsoft Authenticator app. It displays the account name 'Ngee Ann Polytec...' and a 'Connected account' section with instructions to 'Use this account to sign in to Microsoft apps on this device.' Below this, the 'Delete passkey' option is highlighted with a red rectangular box. At the bottom, there is a 'Remove account' button.
14	Who do I contact for help?	If you need help at any step, please contact the NP Service Desk: • Email: ITcare@connect.np.edu.sg • Hotline: 6460 8111 Please describe what you were doing and what you saw on screen, so we can assist you quickly.