

NGEE ANN POLYTECHNIC

Setting Up and Using Microsoft Passkey for Staff

A simple step-by-step guide for all NP staff

Why are we making this change?

- NP is moving from push-based MFA (where you approve a notification or key in a number) to a more secure sign-in method using Microsoft **Passkey**
- Microsoft Passkey. Microsoft Passkey improves security and usability by replacing passwords and MFA codes with a single, phishing-resistant sign-in method that cannot be intercepted or reused, while simplifying login and reducing support overhead
- This guide shows you, step by step, how to set up Microsoft Passkey and how to sign in afterwards. Please follow the steps in order.

Document:	Microsoft Passkey Setup & Sign-In Guide for Staff
Version:	Version 1.1
Updated on:	29 Jun 2026
Audience:	All NP staff using Microsoft 365

Introduction

This document shows you how to set up and use Microsoft **Paskey** 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 **Paskey**, you no longer need MFA codes, strengthen security against Adversary in the Middle (AITM) attacks and simplify authentication. Once your Microsoft Paskey 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 Paskey (One-Time Setup)

Step 1 and 2

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

1. Open Security info

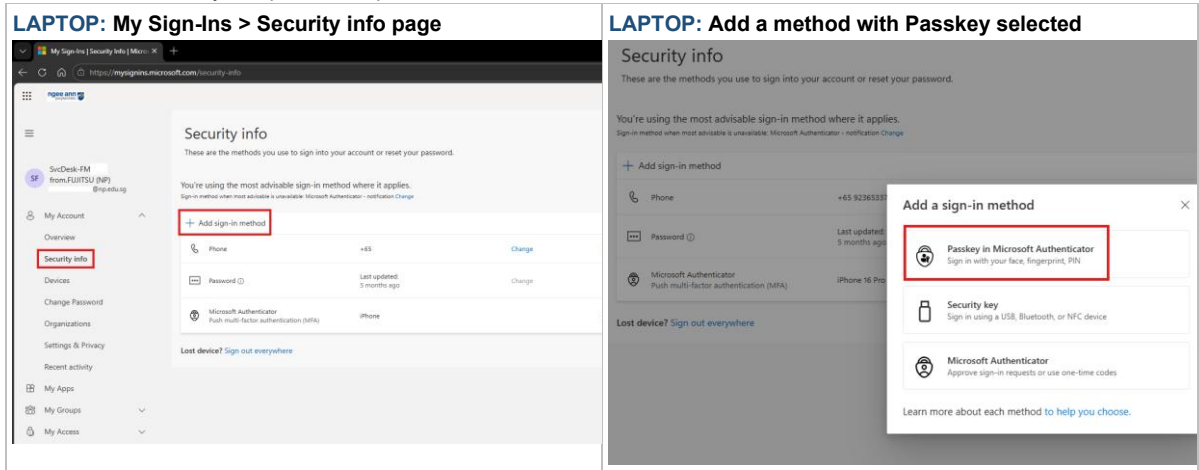
Do: Login to <https://mysignins.microsoft.com/security-info> from your laptop and sign in with your NP account,

Success: Your sign-in methods list appears.

2. Add Paskey in Microsoft Authenticator

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

Success: The Paskey 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.

LAPTOP: Create passkey - Next

Create a passkey in Microsoft Authenticator



A passkey lets you sign in more easily and securely with your face, fingerprint, or PIN.

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.](#)

Back

Next

LAPTOP: Finish creating passkey - Next

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.

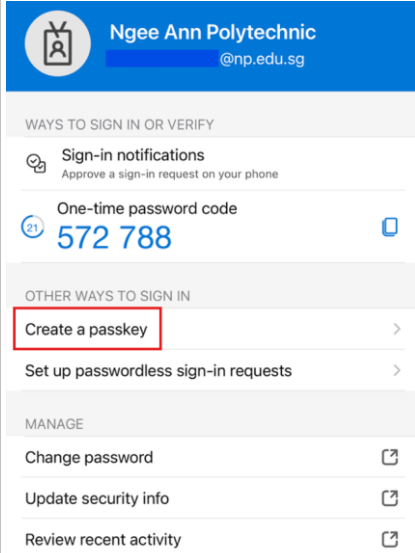
Need to add your account in Authenticator? [Add it now.](#)

Having trouble?

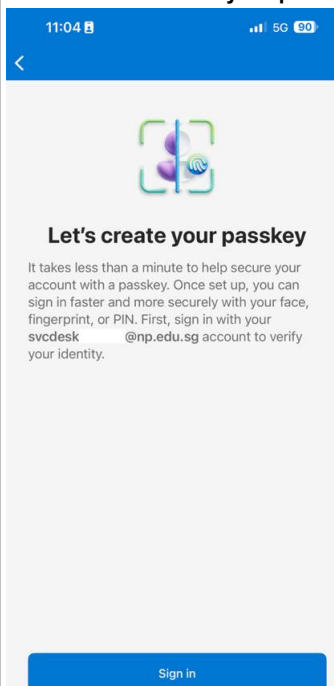
Back

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

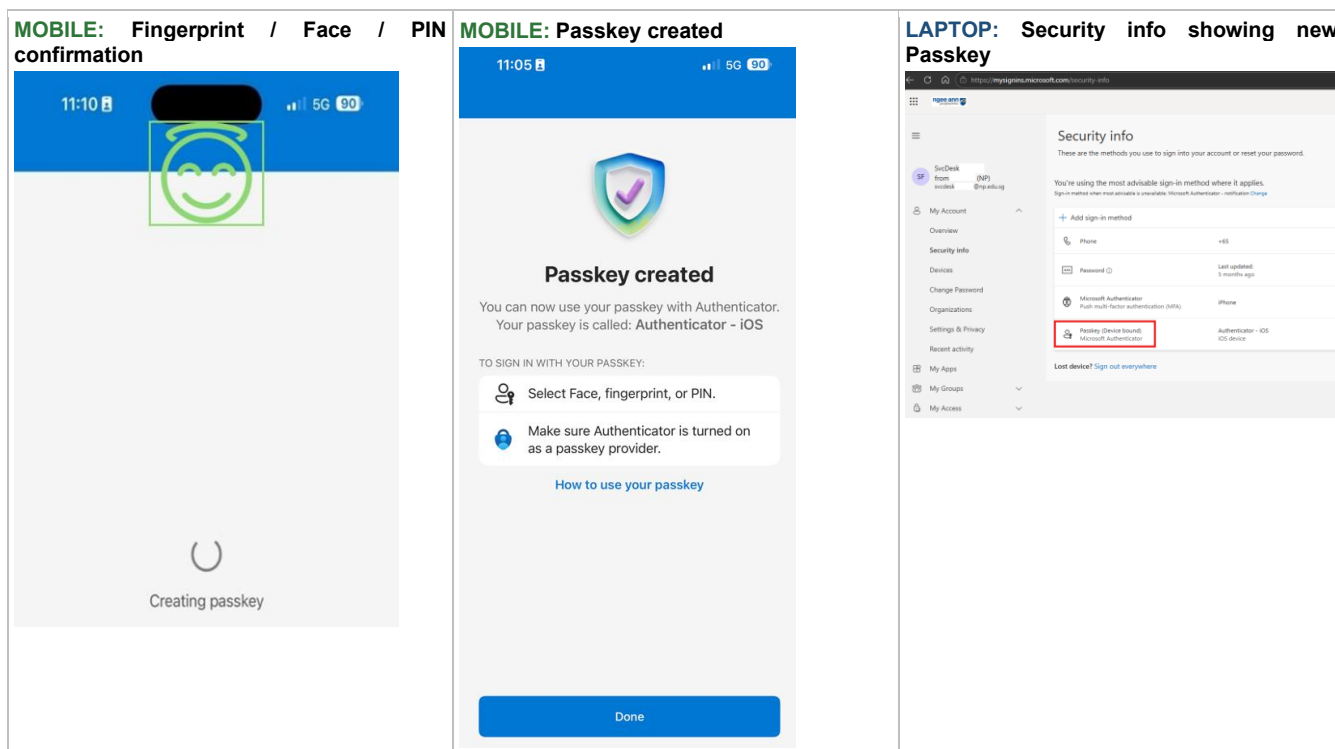
Do: Use fingerprint, face, or PIN on your phone.

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.



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 Paskey 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

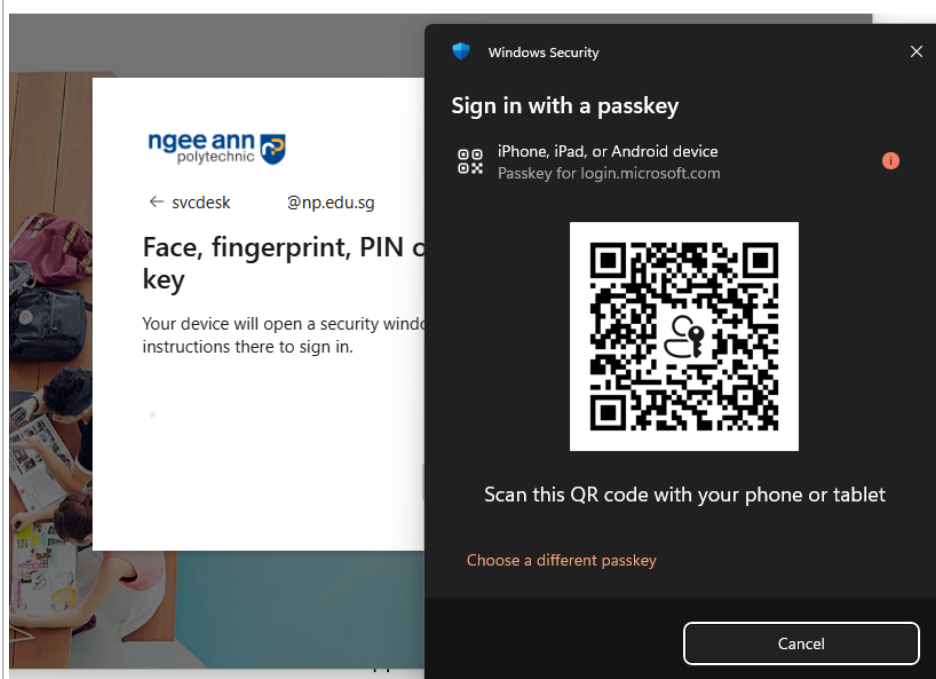
Do: Open the NP system or [Microsoft 365](#) in New In-Private Window in Edge, enter your NP email/password, then wait for the QR code.

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

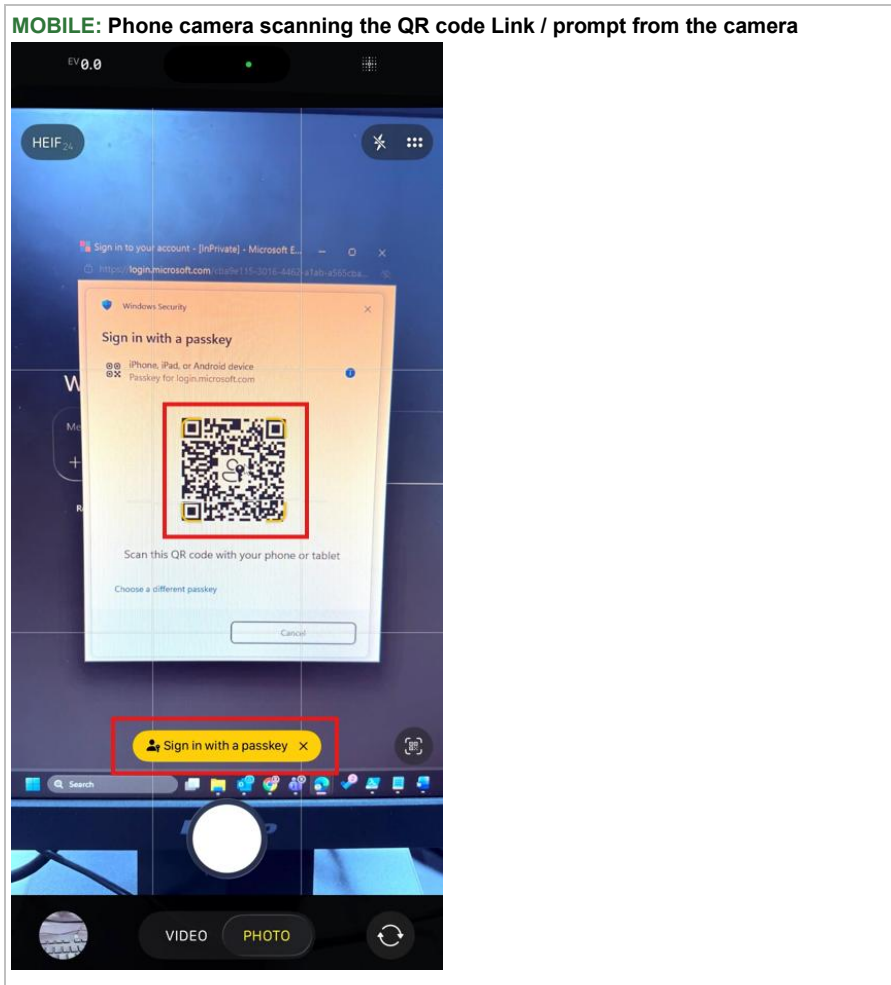
Do: Open the normal phone Camera app and point it at the QR code on the laptop screen. If your device is unable to scan the QR code using the native camera, you may use the scanner within the MS Authenticator app as an alternative.

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

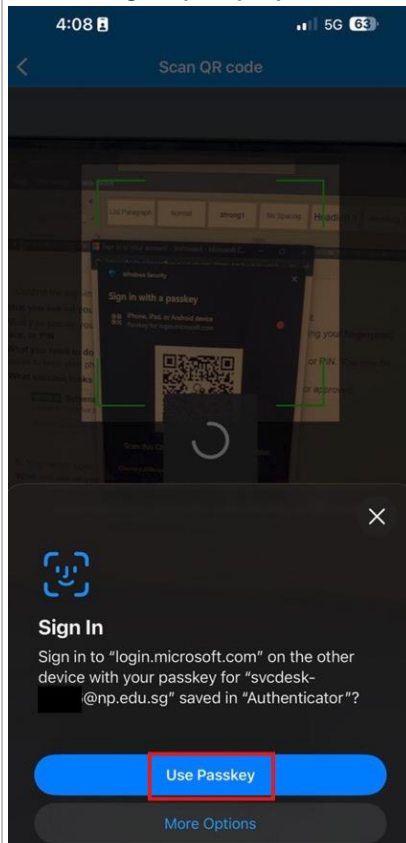
Do: Confirm using your phone screen lock. Keep your phone close to your laptop if prompted.

Laptop: Laptop waits with the QR code.

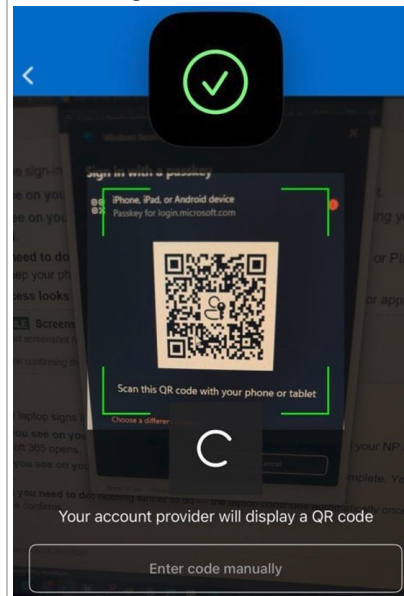
Phone: Phone asks you to confirm.

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

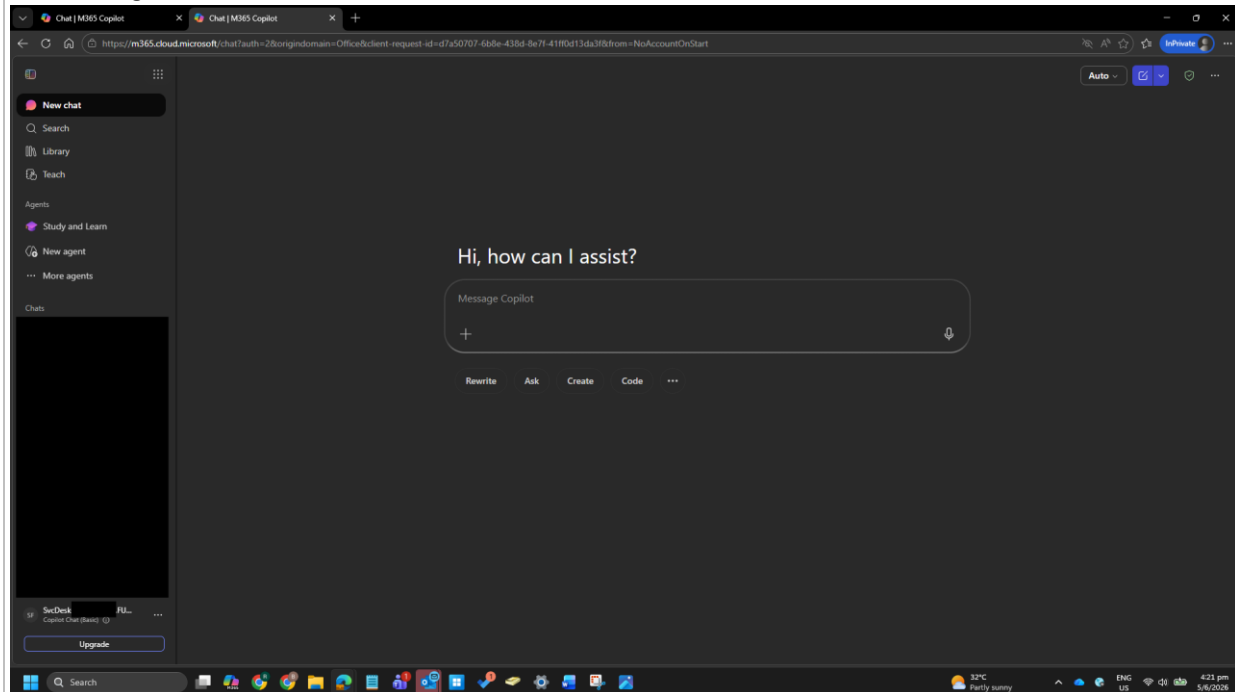
5. Finish sign-in

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



Remember: Camera app to scan - not Authenticator. Leave the QR code screen open until you are signed in.

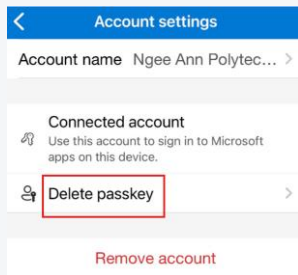
Section 3 - What happens next

- 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 don't see the option to set up a Passkey.	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 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.
3	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.
4	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.
5	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.

No	Question	Answer
6	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.
7	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.
8	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 staff Wi-Fi. Once your phone is online, repeat the sign-in steps in Section 2.
9	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.
10	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.
11	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.

No	Question	Answer
12	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. 
13	I can't access Workday. What should I do?	Verify that the Microsoft Edge profile matches the account you are signing in with (e.g. use your NP account, not a Gov.sg account). Sign out of any incorrect accounts and sign in again with your NP account. Try accessing Workday using an InPrivate window.
14	Who do I contact for help?	If you need help at any step, please contact the NP Service Desk: • Email: Support@np.edu.sg • Hotline: 6460 8111 Please describe what you were doing and what you saw on screen, so we can assist you quickly.

If you are a CPC user using a desktop, kindly enable or turn on the Passkey Access feature outside the CPC app.

- Click **Start** → open **Settings**
- Go to **Privacy & security**
- Select **Passkeys**
- Turn **ON: Passkey access**
- Expand **Let apps create and use passkeys**
- Ensure **login.microsoft.com** (or required app) is set to **ON**

Privacy & security > Passkeys

Allow passkey access



Passkey access

Anyone using this device can choose if their apps can create or use passkeys when this is on

On ☒



Let apps create and use passkeys

Choose which apps can create and use passkeys



Windows App



login.microsoft.com

On ☒



Recent activity

Review passkey creation or passkey usage requests in the last 7 days. The most recent access data is also captured in other sections in this page

0 requests