Toyohashi University of Technology

Multi-Factor Authentication Registration Guide

(Authenticator Setup)

Version 1.00

NTT West Corporation

● **Revision History**

Date	Version	Description of Change	Author	Approver
2026/6/16	0.10	Initial version created	SIOS Kawai	
2026/6/18	0.20	Added items pointed out by the university	SIOS Kawai	
2026/6/22	0.30	Revised items pointed out by the university	SIOS Kawai	
2026/6/24	0.40	Revised items pointed out by the university	SIOS Kawai	
2026/6/26	1.00	Partially revised the descriptions	IMC Nakamura	

Table of Contents

1. Introduction

1.1. Purpose of This Document

This document explains the procedure for configuring multi-factor authentication on the Authentication Infrastructure System of Toyohashi University of Technology. The method described here is **one-time password authentication**, which authenticates the user by combining a password with an authenticator app installed on a mobile phone (smartphone) or tablet.

1.2. Required Environment

- PC
- A smartphone or tablet for registration
  (*Note: Registration and setup can be completed on the same single device.*)
  You must install an authenticator app such as Microsoft Authenticator or Google Authenticator in advance. Various authenticator apps can be used, including those listed here, but the Information and Media Center recommends using Microsoft Authenticator.

  Microsoft Authenticator

  Google Authenticator

  (iOS) (Android)

1.3. Terminology

- MFA

Multi-Factor Authentication. A security technology that verifies the user's identity by combining two or more different factors when signing in to web services and the like: in addition to a knowledge factor such as a password, a possession factor such as a smartphone app or SMS, and a biometric (inherence) factor such as a fingerprint or face.

2. MFA Setup Procedure

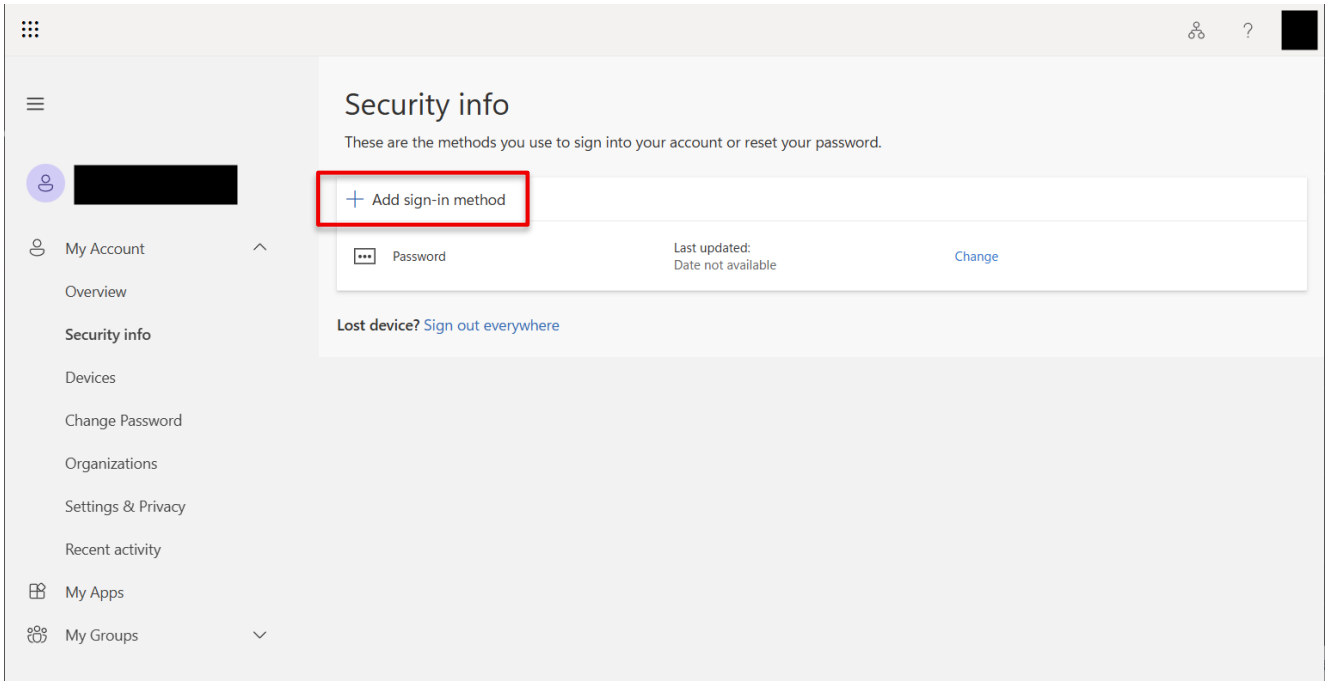
2.1. Microsoft Authenticator Setup Procedure

2.1.1. Setup from a PC

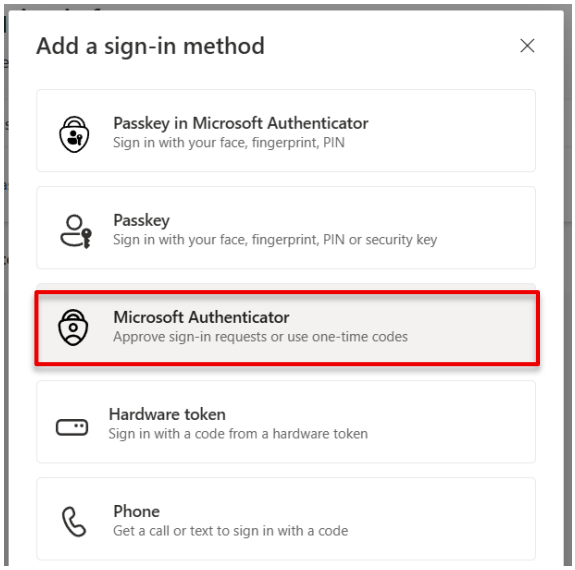
- Working device: PC
- Registration device: Smartphone
  Note: If you are setting up from a smartphone, please start from section 2.1.2 on page 12

1. From the working device, access the URL below and sign in with your permanent email address.
   https://aka.ms/mfasetup

2. Under "Security info," click "Add sign-in method."

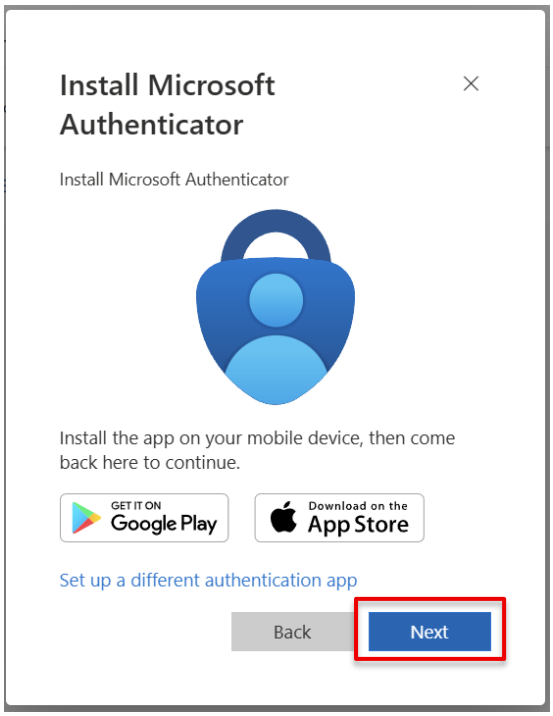


3. Click "Microsoft Authenticator."

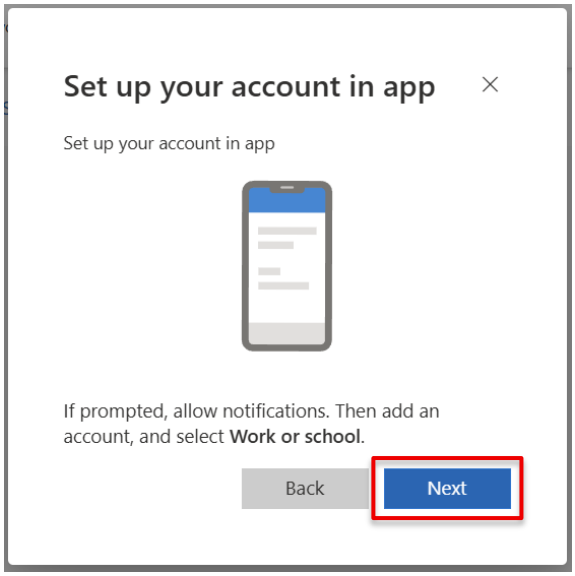


4. Prepare the device on which Microsoft Authenticator is installed (the registration device), and click "Next."

   * If you use a different app such as "Google Authenticator," please follow the steps in Section 2.2.

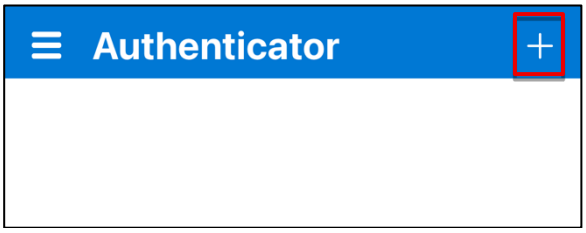


5. Click "Next."



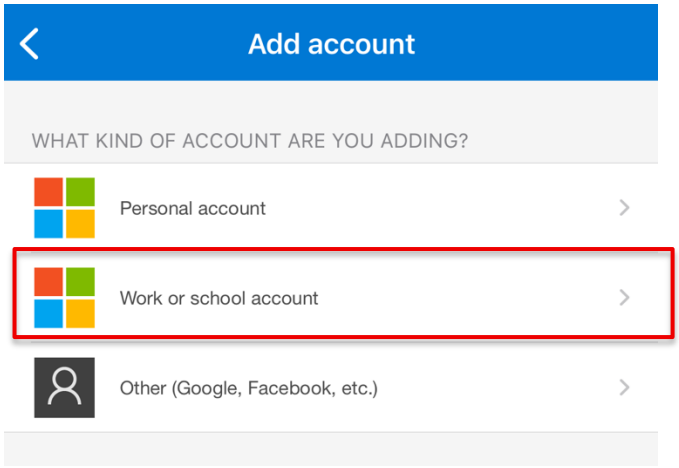
6. On the registration device, launch "Microsoft Authenticator."

7. In the "Microsoft Authenticator" app on the registration device, tap the "+" at the top.

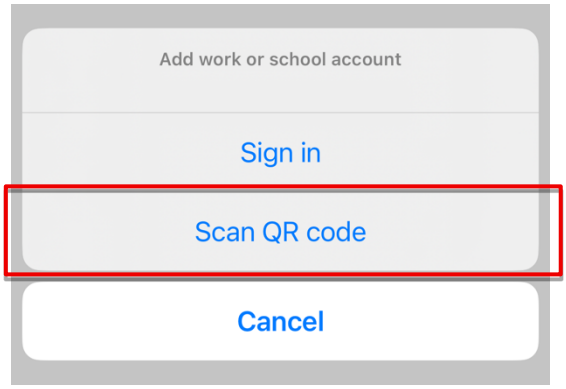


Note: *> iPhone screens are used for illustration. Android screens are similar and follow the same general steps.*

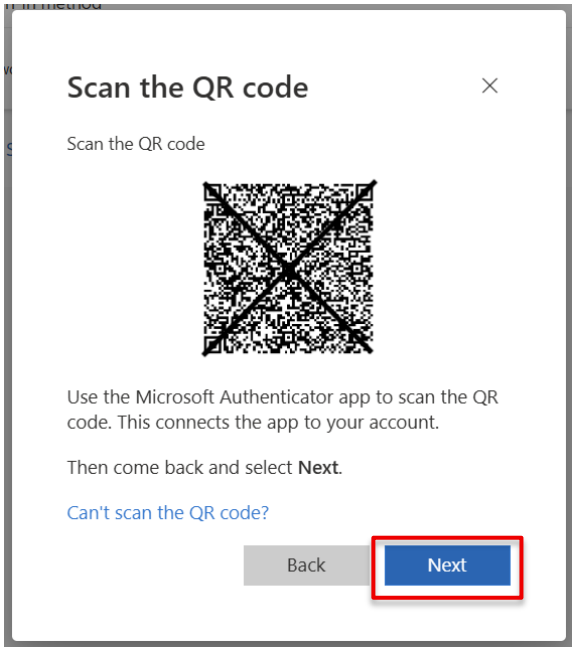
8. Select "Work or school account."



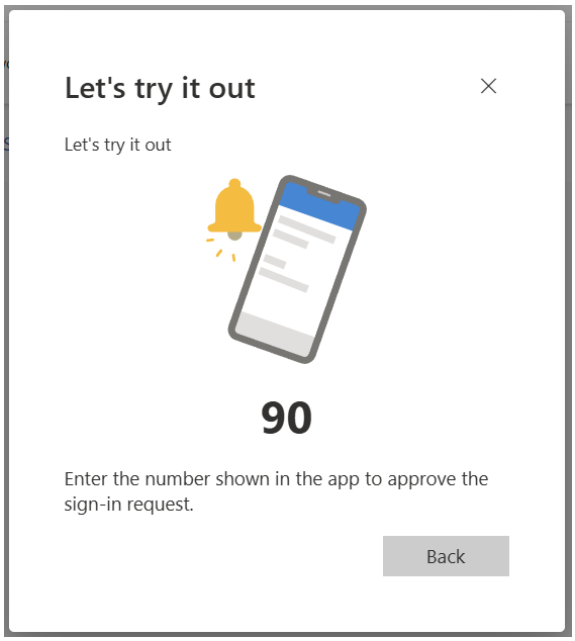
9. Select "Scan QR code." Using the camera that opens, scan the QR code shown on the working device in step 10.



10. Scan the QR code shown on the working device screen with the Authenticator app on the registration device. Once it is registered in the app, click "Next."

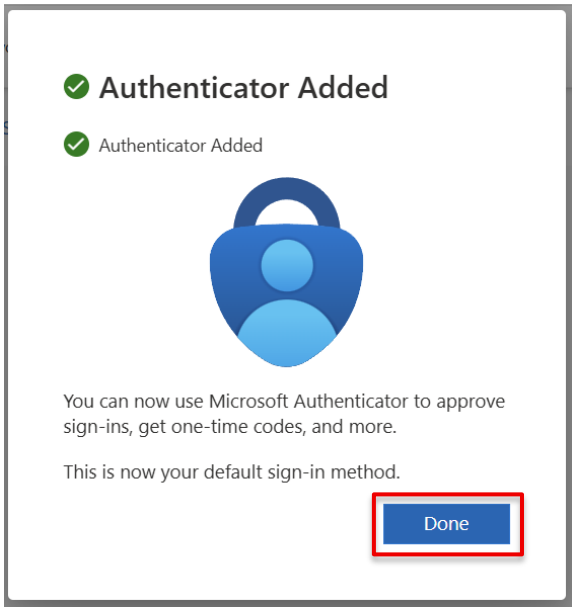


11. A number is shown on the working device screen.

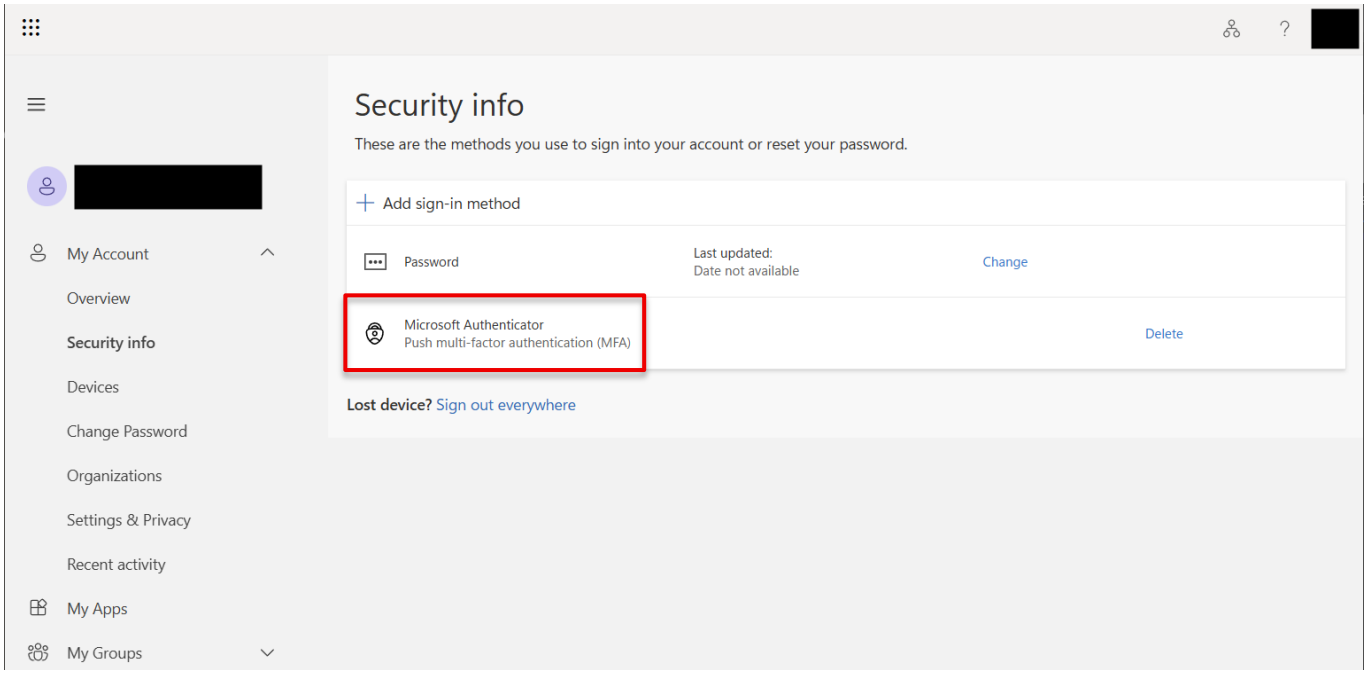


12. Enter the number shown on the working device into the Microsoft Authenticator app on the registration device, and select "Yes."

13. When the following screen appears on the working device, registration is complete. Click "Done."



14. Confirm that "Microsoft Authenticator" appears in the list on the working device.

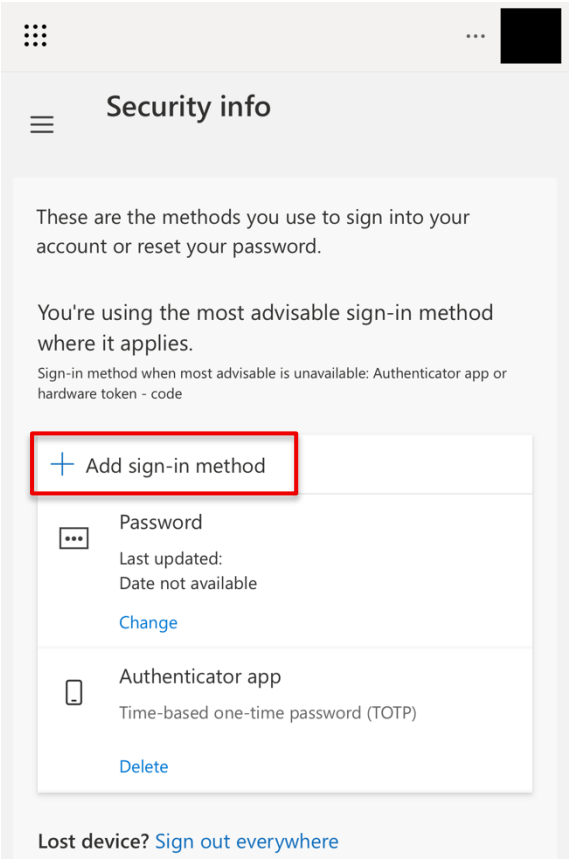


2.1.2. Setup from a Smartphone

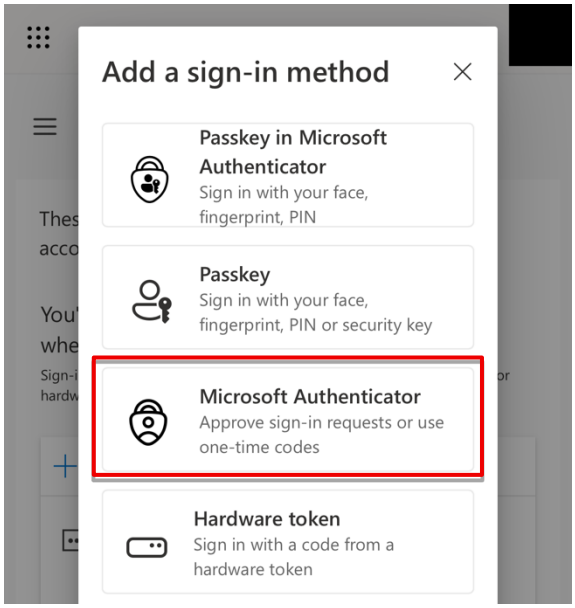
- Working device: Smartphone
- Registration device: Smartphone

1. From the working device, access the URL below and sign in with your permanent email address.
   https://aka.ms/mfasetup

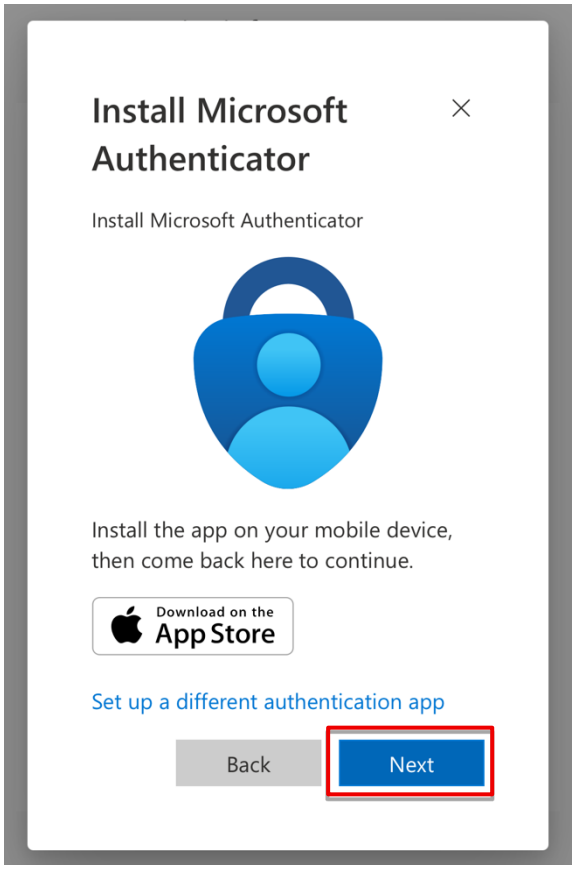
2. Under "Security info," select "Add sign-in method."



3. Select "Microsoft Authenticator."

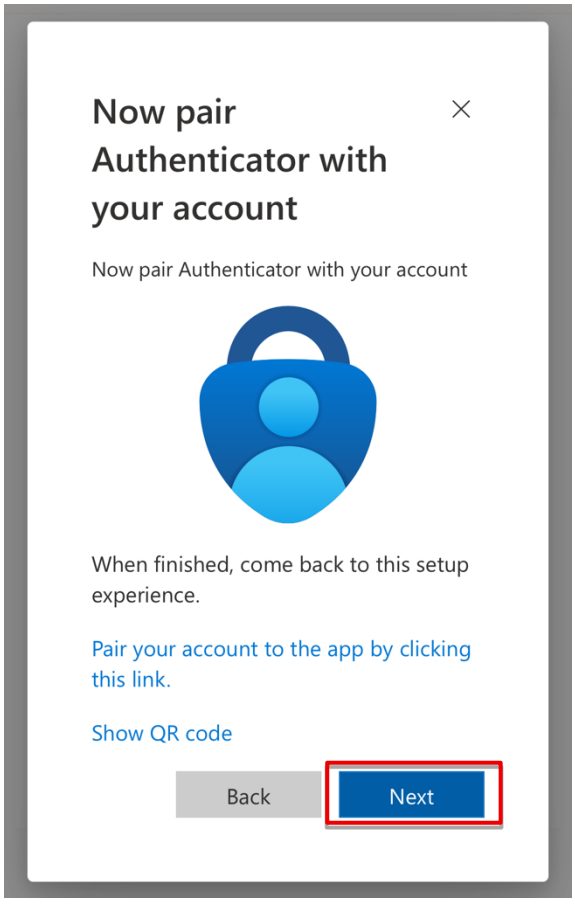


4. Install Microsoft Authenticator, and select "Next."

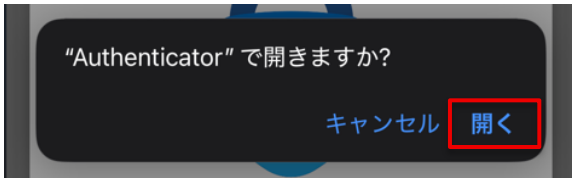


Note: *> iPhone screens are used for illustration. Android screens are similar and follow the same general steps.*

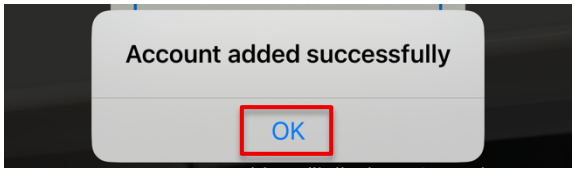
5. Pair Authenticator with your account. Select "Next."



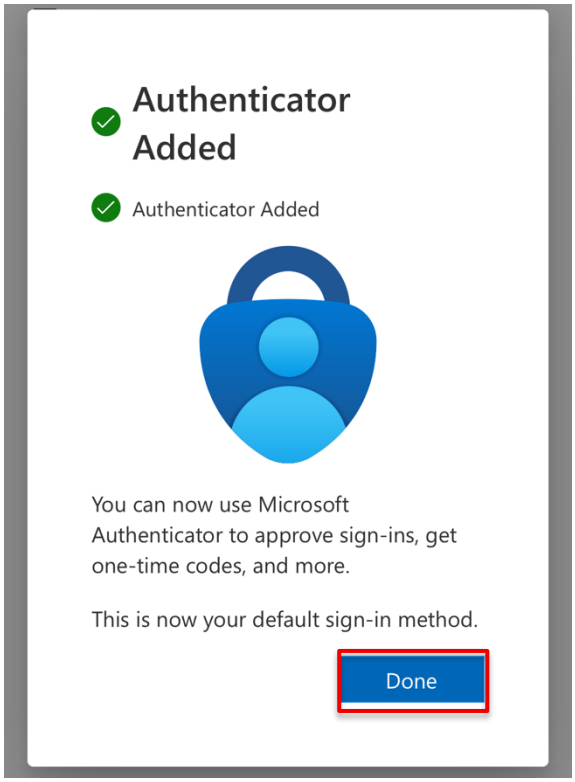
6. Select "Open."



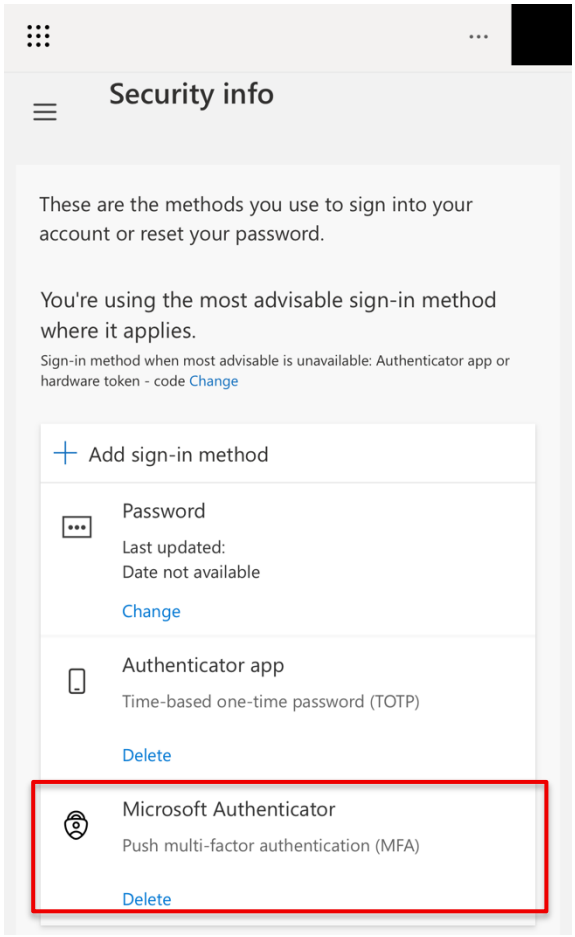
7. A message like the following appears in the Authenticator app. Select "OK."



8. When the following screen appears, registration is complete. Click "Done."



9. Confirm that "Microsoft Authenticator" appears in the list.



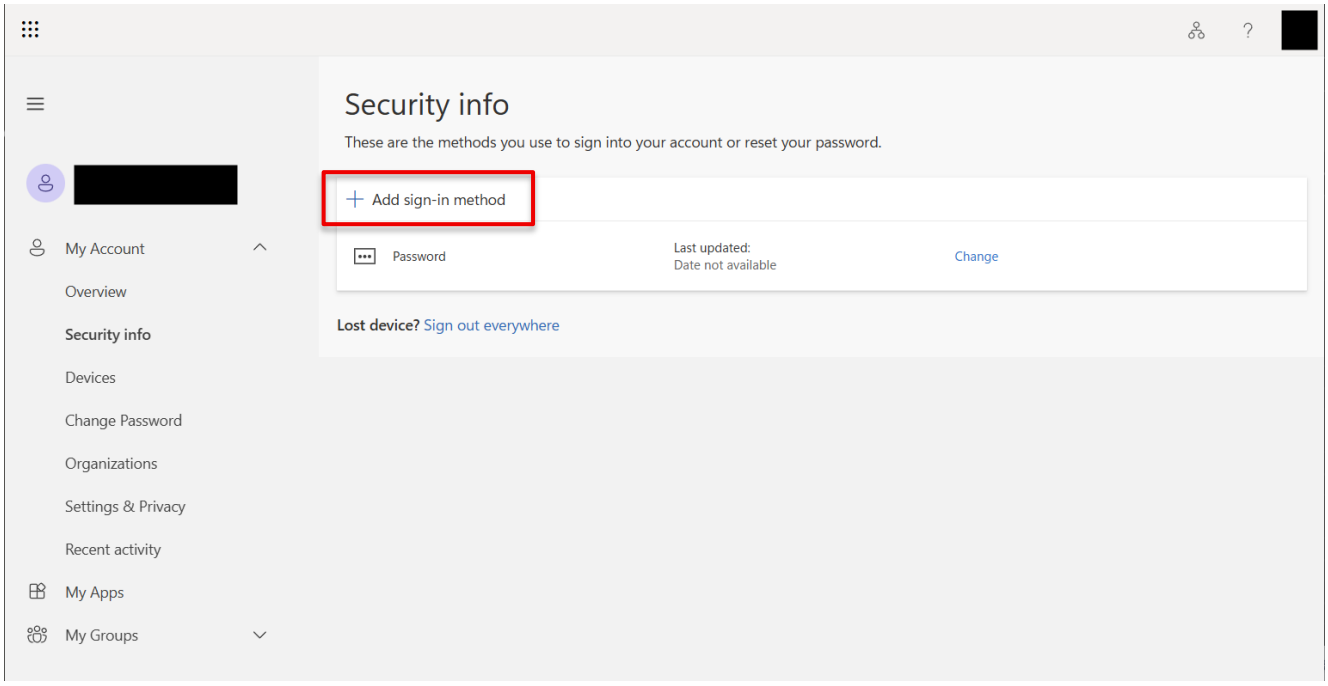
2.2. Other Apps (e.g., Google Authenticator) Setup Procedure

2.2.1. Setup from a PC

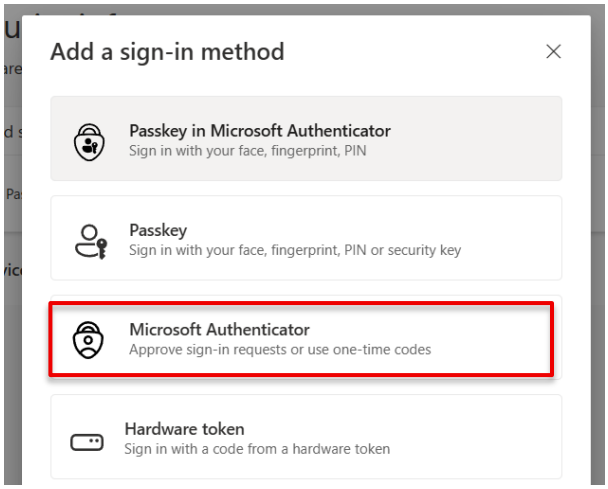
- Working device: PC
- Registration device: Smartphone
  Note: If you are setting up from a smartphone, please start from section 2.2.2 on page 24

1. From the working device, access the URL below and sign in with your permanent email address.
   https://aka.ms/mfasetup

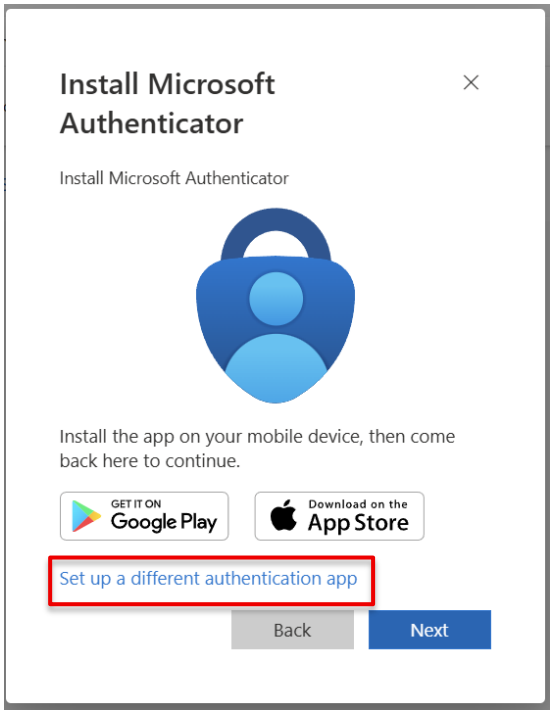
2. Under "Security info," click "Add sign-in method."



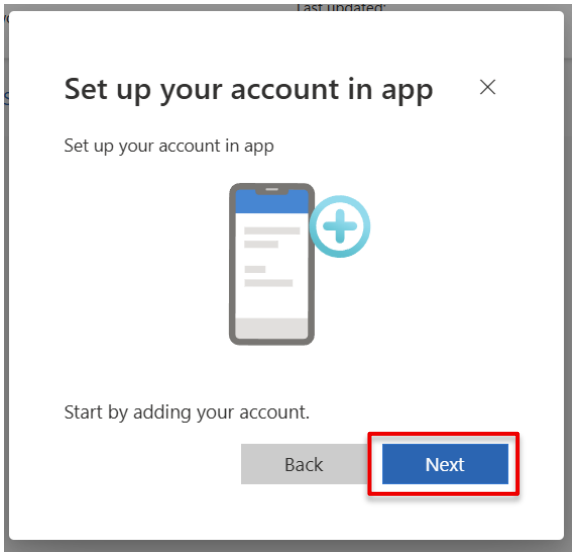
3. Click "Microsoft Authenticator."



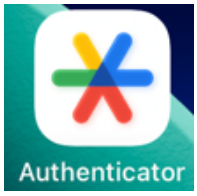
4. Prepare the device on which Authenticator is installed (the registration device), and click "Set up a different authentication app." This guide describes the procedure using "Google Authenticator."



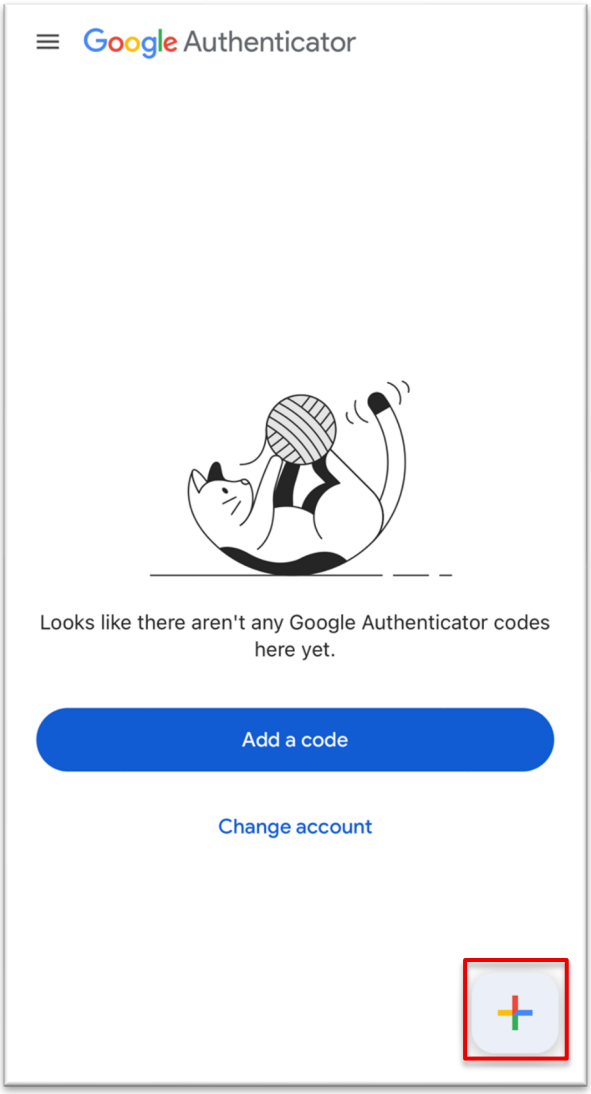
5. Click "Next."



6. On the registration device, launch "Google Authenticator."

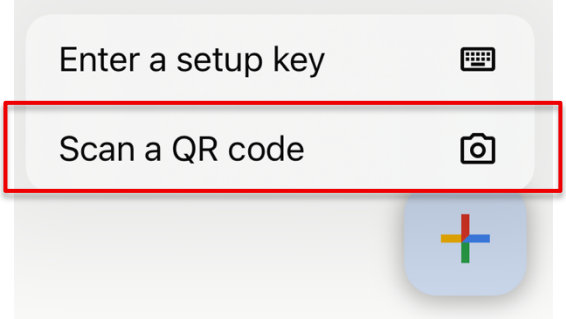


7. In the "Authenticator" app on the registration device, tap the "+" at the bottom.

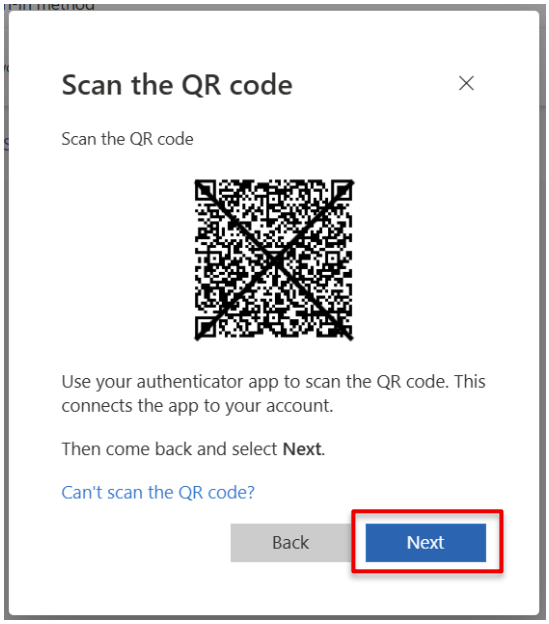


Note: *> iPhone screens are used for illustration. Android screens are similar and follow the same general steps.*

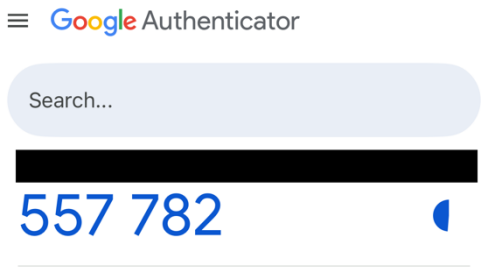
8. Select "Scan a QR code." Using the camera that opens, scan the QR code shown on the working device in step 9.



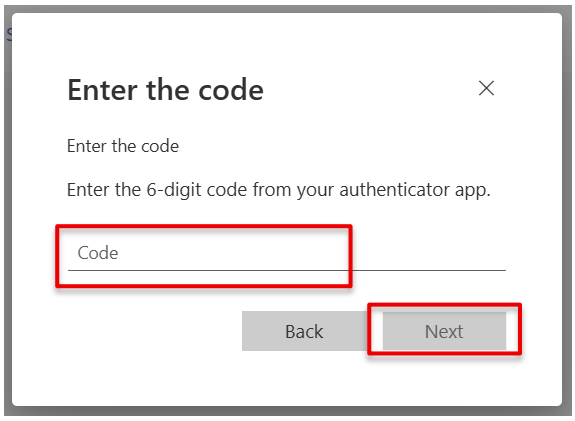
9. Scan the QR code shown on the screen with the Google Authenticator app on the registration device. Once it is registered in the app, click "Next."



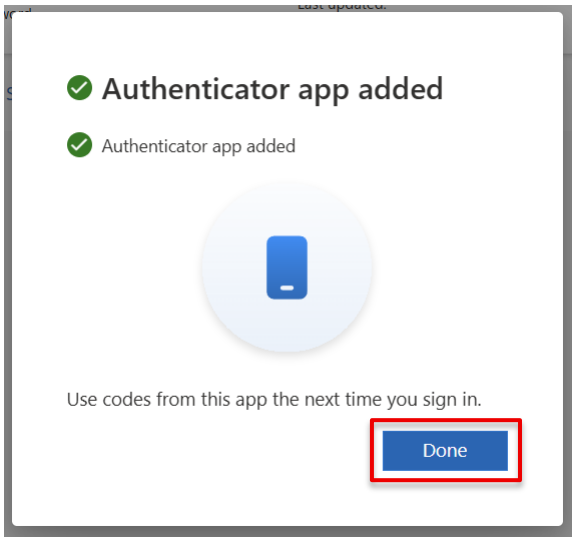
10. Check the six-digit number shown on the registration device.



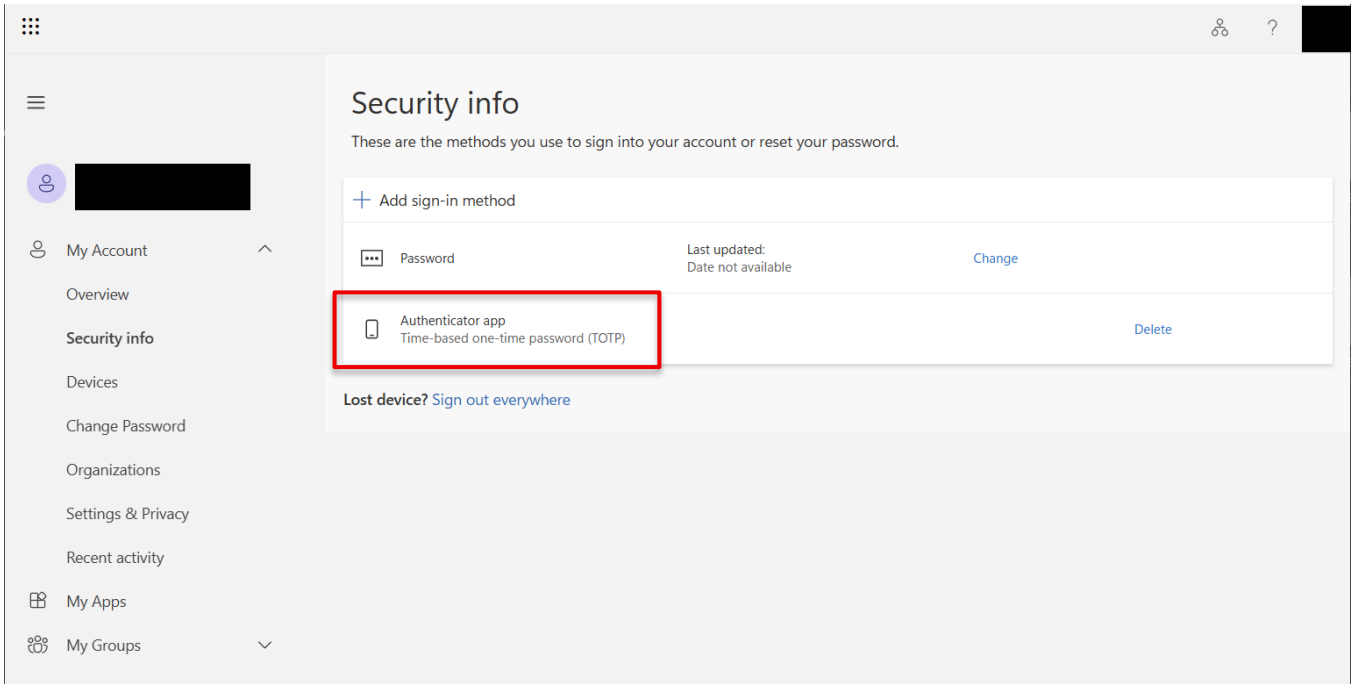
11. A code-entry screen appears on the working device. Enter the six-digit one-time password shown in the Google Authenticator app on the registration device, and click "Next."



12. When the following screen appears, registration is complete. Click "Done."



13. Confirm that "Authenticator app" appears in the list on the working device.

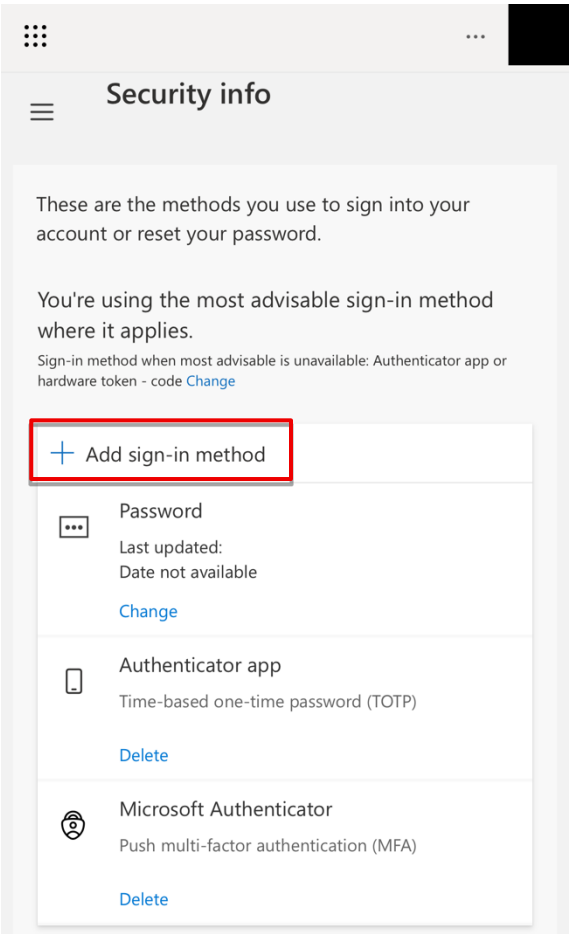


2.2.2. Setup from a Smartphone

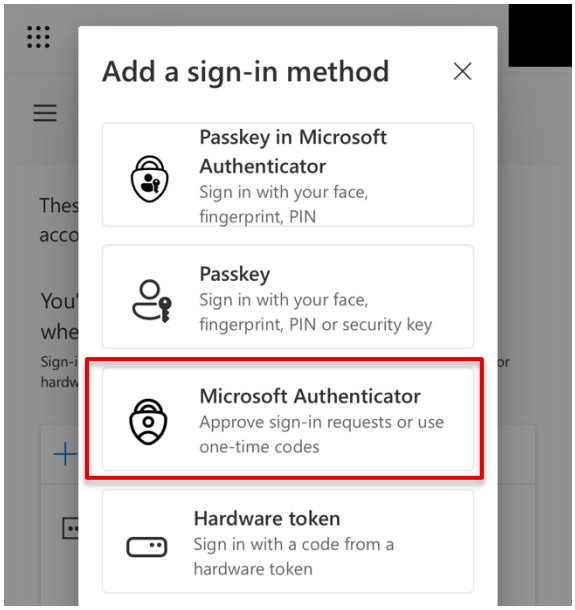
- Working device: Smartphone
- Registration device: Smartphone

1. From the working device, access the URL below and sign in with your permanent email address.
   https://aka.ms/mfasetup

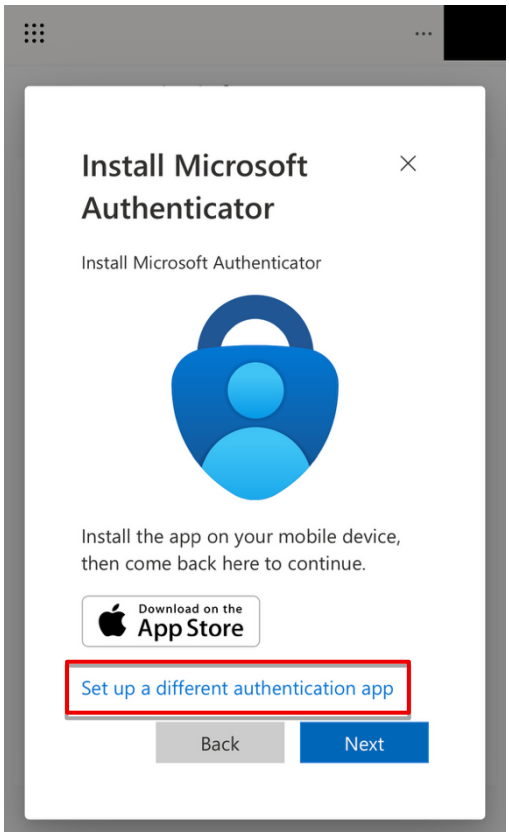
2. Under "Security info," select "Add sign-in method."



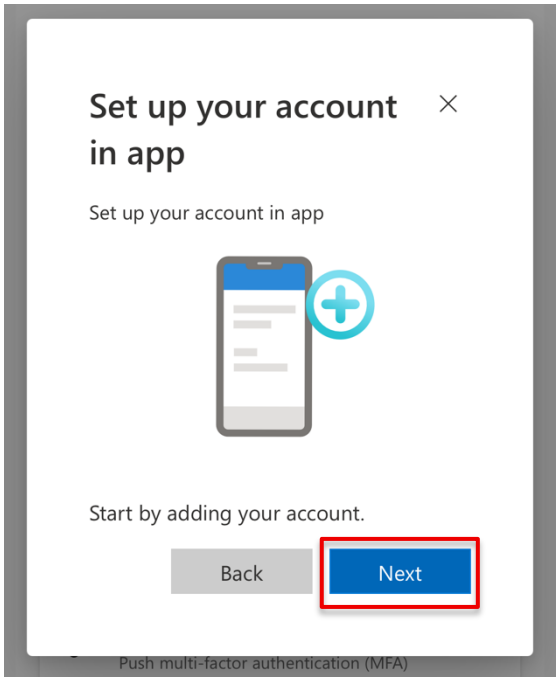
3. Select "Microsoft Authenticator."



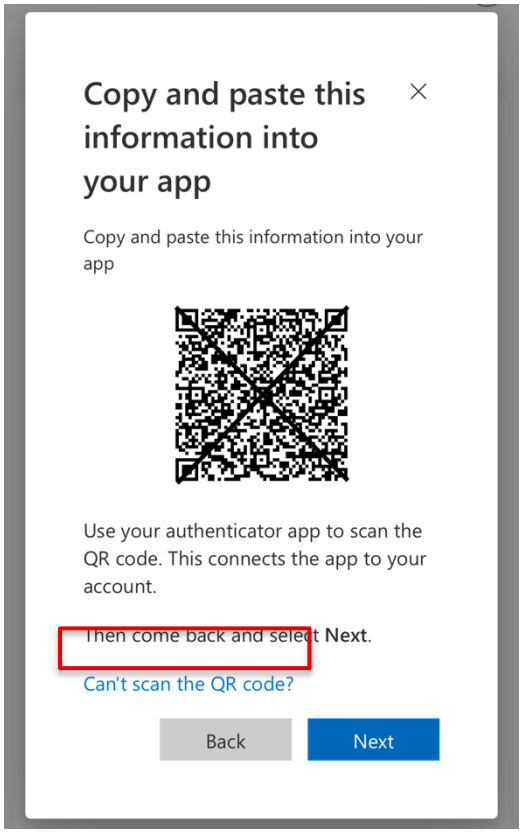
4. Prepare the device on which Authenticator is installed, and select "Setup a different authenticator app."



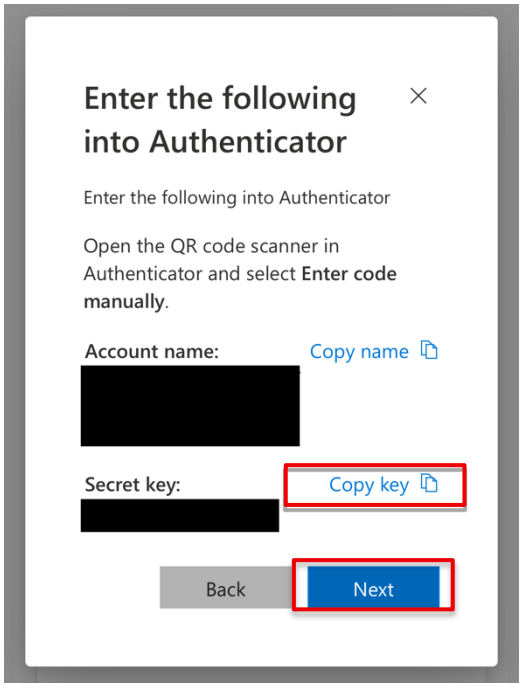
5. Click "Next."


Set up your account in app
Set up your account in app
Start by adding your account.
Back
Next
Push multi-factor authentication (MFA)

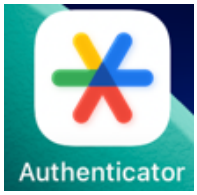
6. Select “Can’t scan the QR code?”



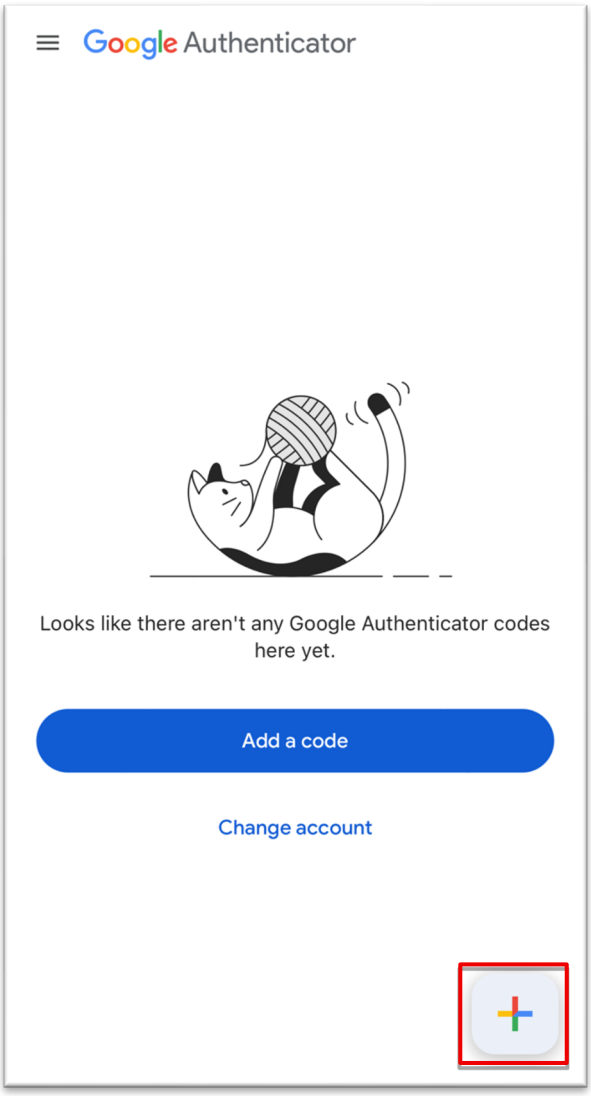
7. Select "Copy key" for the secret key that is displayed, then select "Next."


Enter the following into Authenticator
Enter the following into Authenticator
Open the QR code scanner in Authenticator and select Enter code manually.
Account name:
Copy name
Secret key:
Copy key
Back
Next

8. On the registration device, launch "Google Authenticator."

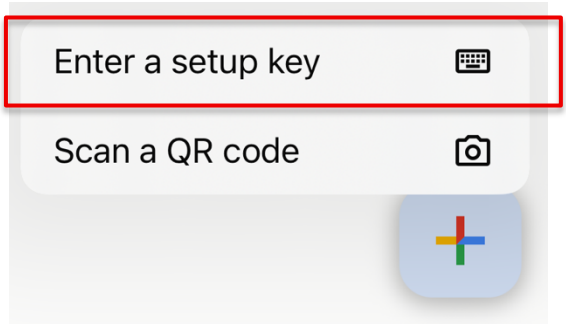


9. In the "Google Authenticator" app on the registration device, tap the "+" at the bottom.

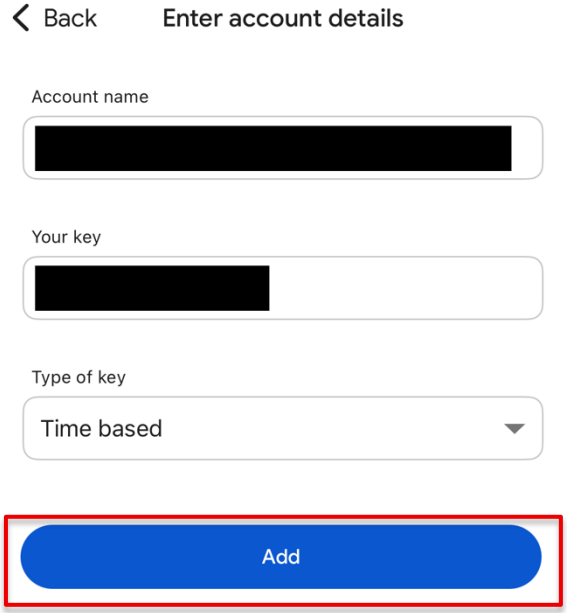


Note: *> iPhone screens are used for illustration. Android screens are similar and follow the same general steps.*

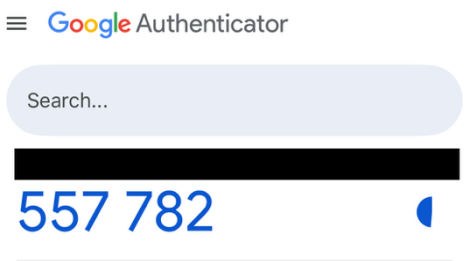
10. Select "Enter a setup key."



11. In the "Account name" field, enter any name; in the "Your key" field, enter the secret key you copied in step 7. For "Type of key," select "Time based," then select "Add."

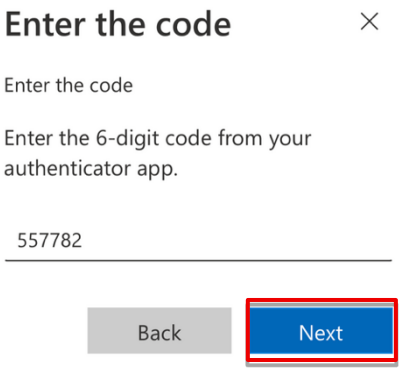


12. Check the six-digit number shown on the registration device.

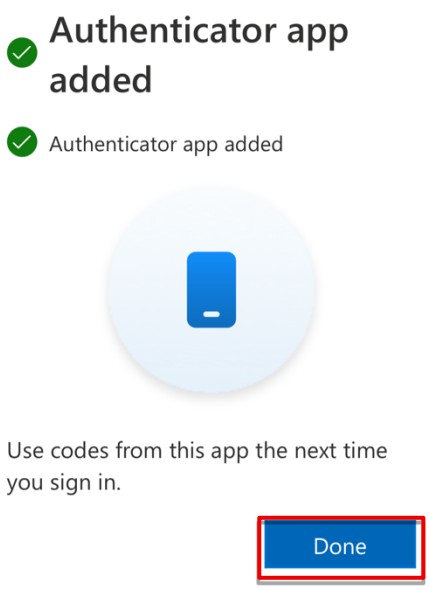


13. A code-entry screen appears. Enter the six-digit one-time password shown in the Google

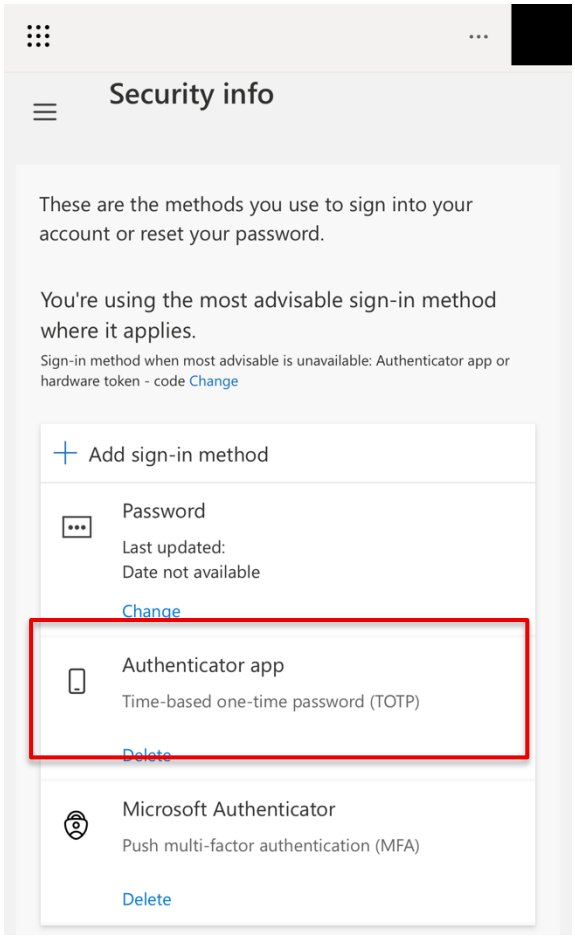
Authenticator app, and select "Next."



14. When the following screen appears, registration is complete. Click "Done."



15. Confirm that "Authenticator app" appears in the list.



3. MFA Registration Verification Procedure

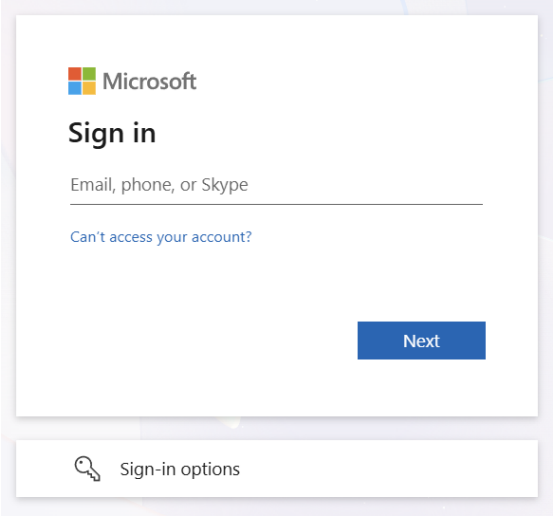
3.1. Verification Procedure (through July 17, 2026)

* Through July 17, 2026, please verify using the procedure below.

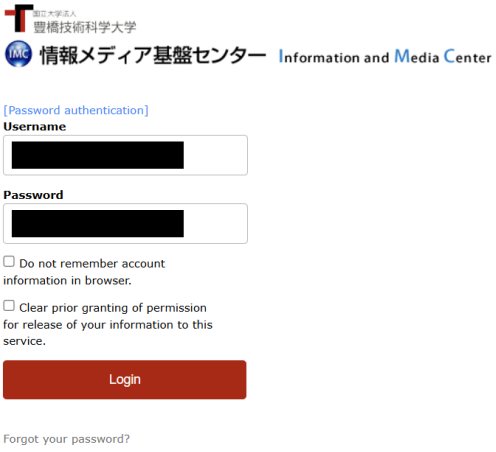
1. Access the MFA verification test site below.
   https://yuadm.edu.tut.ac.jp/

2. Click "Sign in."

3. Enter your permanent email address, and click "Next."



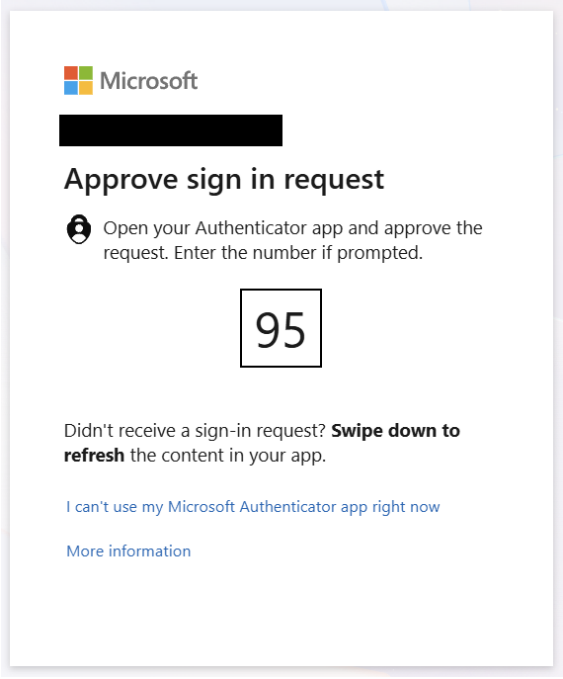
4. The Information and Media Center login screen appears. Enter your user name and password, and click "Login."

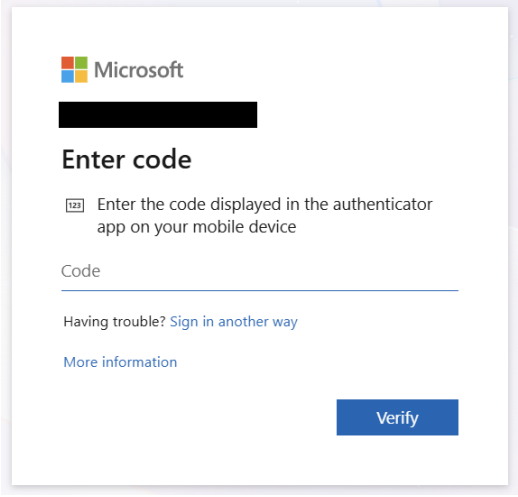


5. The MFA authentication you registered runs.

   * Here, open the Microsoft Authenticator app on your smartphone and enter the number shown.

   For “Google Authenticator,” a code-entry screen appears as shown on the right.





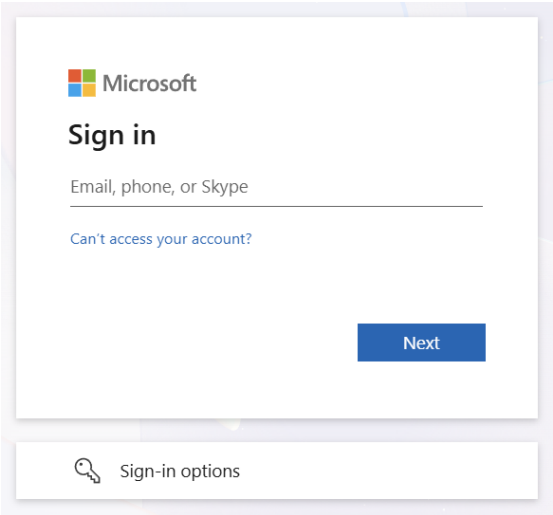
6. Once authentication succeeds and the "MFA verified" screen below appears, MFA verification is complete.

3.2. Verification Procedure (from July 18, 2026 onward)

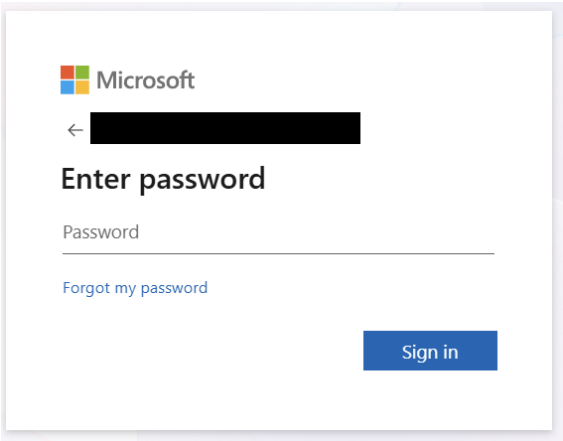
* From July 18, 2026 onward, please verify using the procedure below.

1. Access the password change screen below.
   https://useradm.imc.tut.ac.jp/webmtn/

2. Enter your permanent email address, and click "Next."



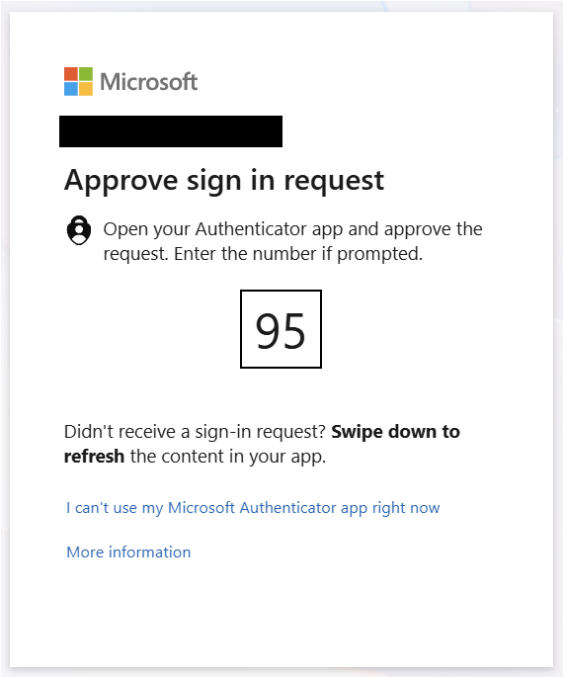
3. Enter the password for your Information and Media Center account, and click "Sign in."

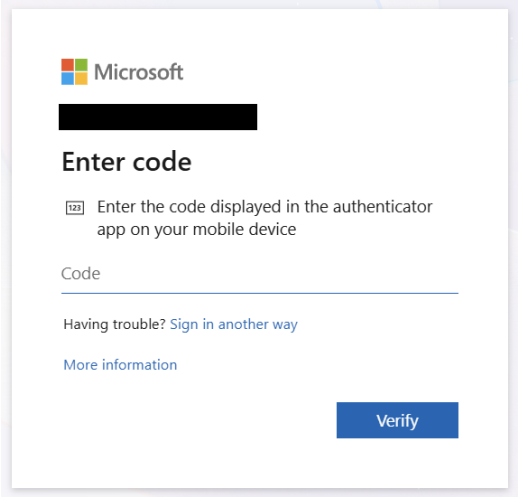


4. The MFA authentication you registered runs.

   * Here, open the Microsoft Authenticator app and enter the number shown.

   For “Google Authenticator,” a code-entry screen appears as shown on the right.





5. Once authentication succeeds and the password change screen appears, MFA verification is complete.