

Multi-factor Authentication: Smartphone App Initial Setup Guide

STEP 1: Install the Microsoft Authenticator App

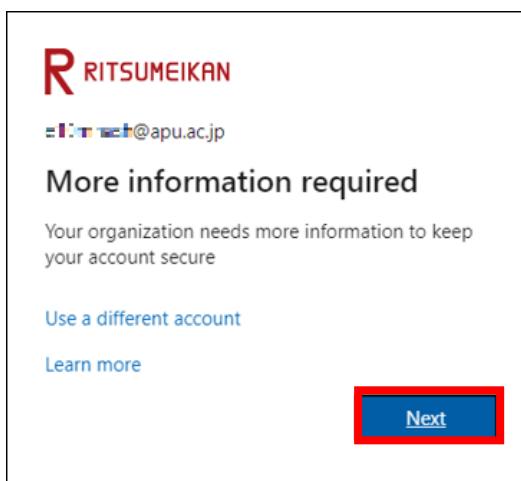
Operating on a smartphone

- 1 Install the [Microsoft Authenticator App] from the App Store or Google Play.

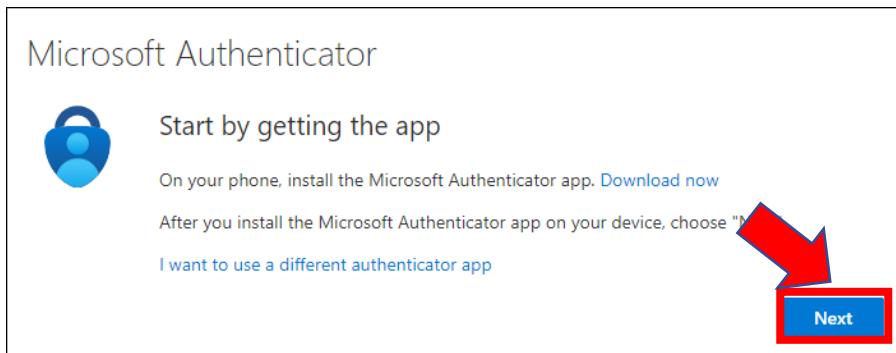
STEP 2: Initial Setup for Multi-factor Authentication

Operating on a computer

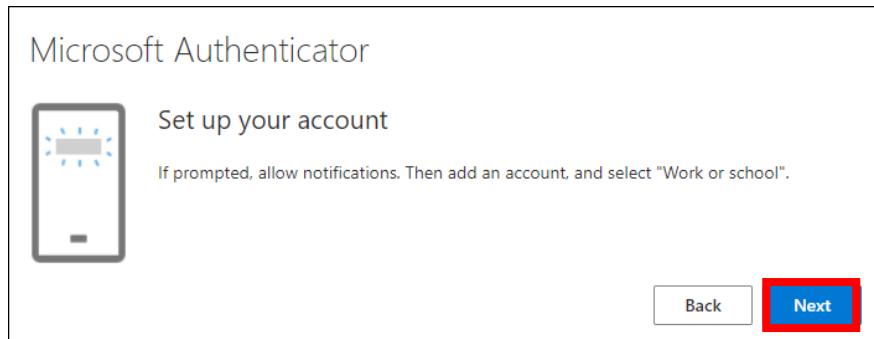
- 1 Use a web browser to sign in to the Multi-factor Authentication page (<https://aka.ms/mfasetup>).
- 2 When the [More information required] box shows up, click [Next].



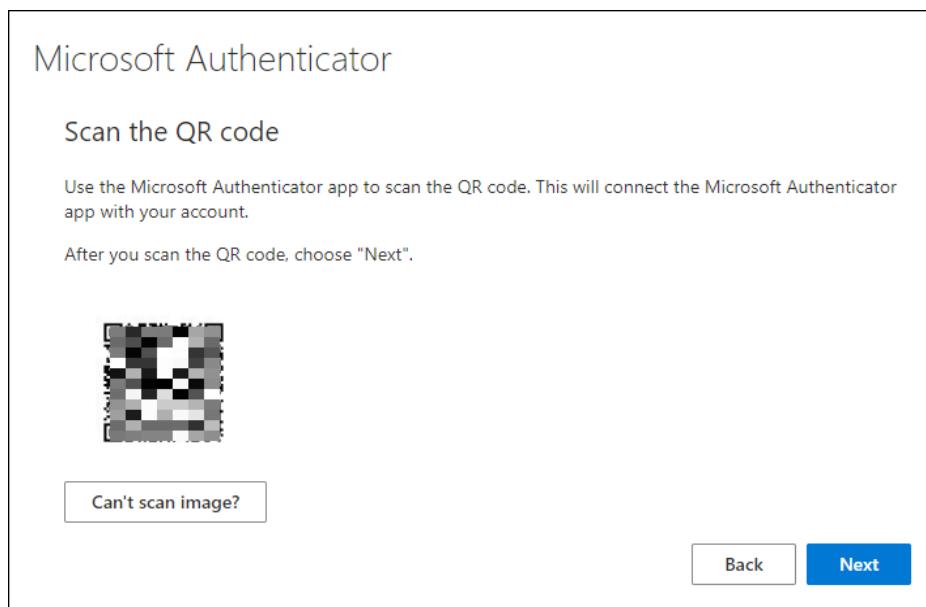
- 3 When the [Start by getting the app] screen appears, **click [Next] as the app has already been obtained in STEP 1 of this manual.**



④ When the [Set up your account] box shows up, click [Next].

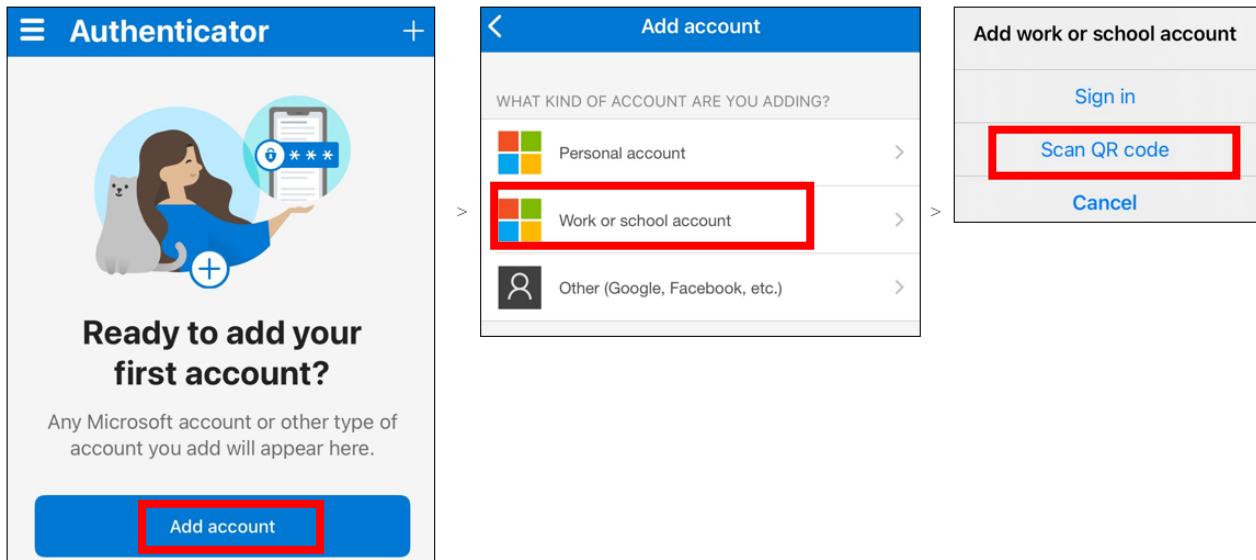


⑤ Display the [Scan the QR code] box.

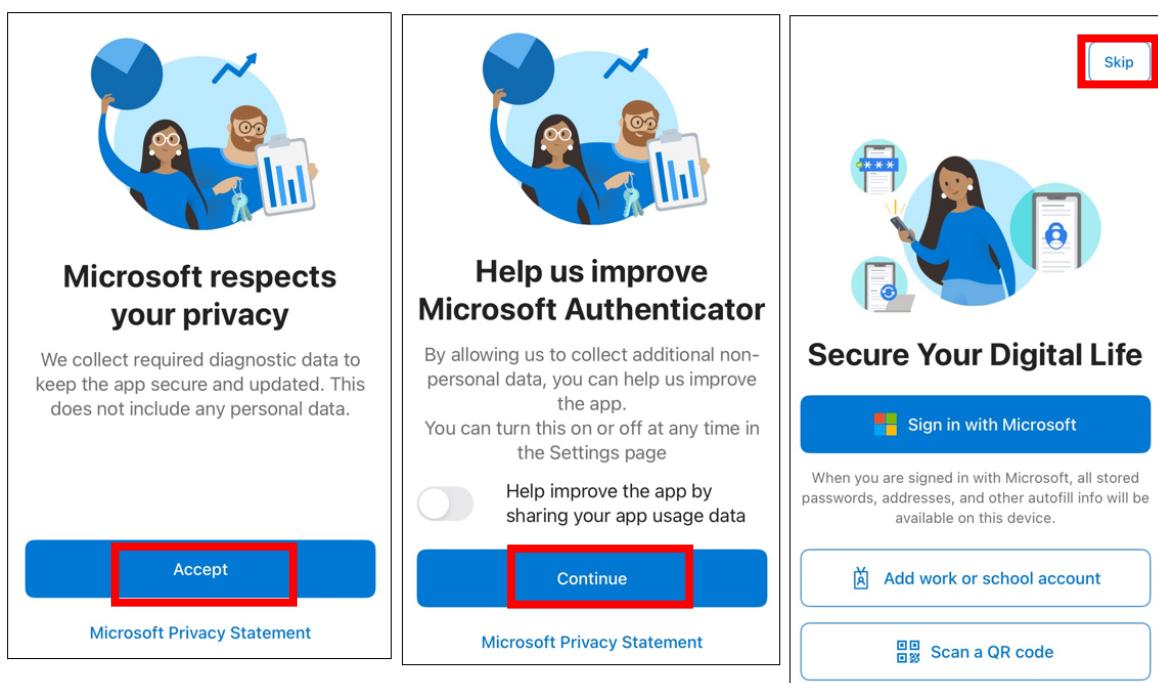


Operating on a smartphone

⑥ Open Microsoft Authenticator, tap [Add account] > [Work or school account] > [Scan QR code] and scan the QR code on the screen in step ⑤.



ⓘ If the following screen is displayed when you start up for the first time, tap [Accept], [Continue], and [Skip] until the [Add Account] button appears.



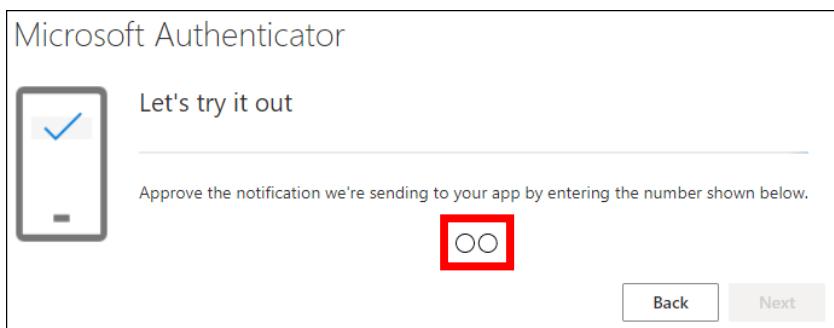
ⓘ In order to use the Microsoft Authenticator, permission is required for notifications from the app and access to the camera from the app.

7 Verify that your APU account has been automatically added to Microsoft Authenticator.



Operating on a computer

8 Click [Next] on the [Scan the QR code] box, and the [Let's try it out] box will appear. Verify that a 2-digit number is displayed.



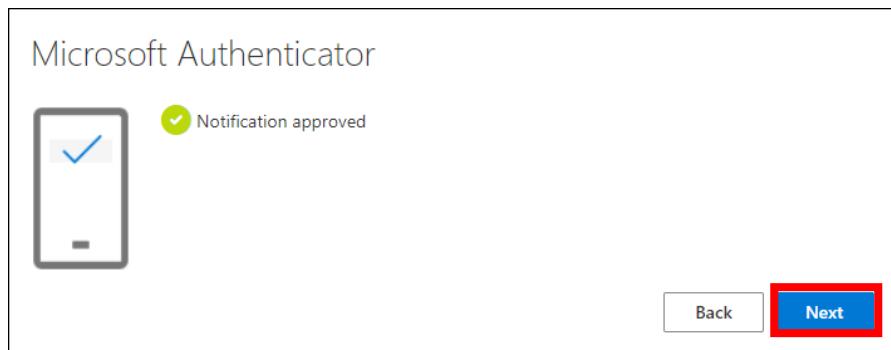
Operating on a smartphone

9 When [Are you trying to sign in?] appears on Microsoft Authenticator, enter the number on the screen in 8 and tap [Yes].

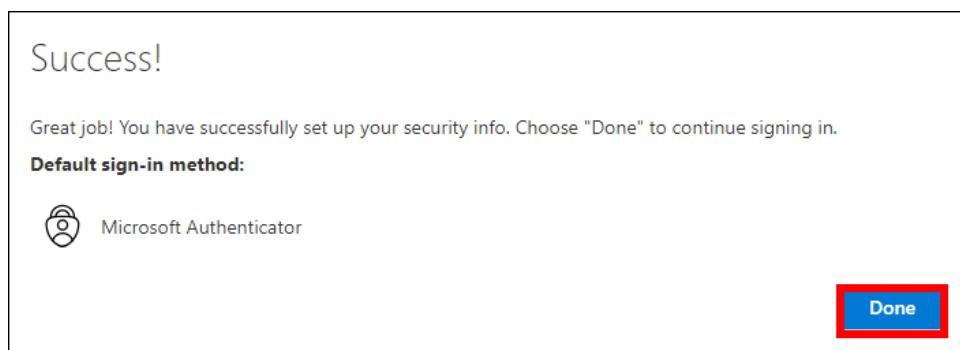


Operating on a computer

⑩ Click [Next] on the [Let's try it out] box, and when [Notification approved] is displayed, click [Next].



⑪ When the [Success!] box shows up, click [Done].



⑫ If Microsoft Authenticator is added as a sign-in method on the [Security Info] screen, the setup is complete.

The screenshot shows the 'Security info' screen in the Microsoft account settings. The left sidebar has options: Overview, **Security info** (which is selected and highlighted with a red box), Devices, Password, Organizations, Settings & Privacy, and Recent activity. The main area is titled 'Security info' and says 'These are the methods you use to sign into your account or reset your password.' It shows the 'Default sign-in method: Microsoft Authenticator - notification' with a 'Change' link. Below that is a table for 'Add sign-in method'. The table has one row with a 'Password' method, last updated 6 months ago, with a 'Change' link. The 'Microsoft Authenticator' method is listed below it, highlighted with a red box. It shows 'Push multi-factor authentication (MFA)' and has a 'Delete' link. At the bottom, it says 'Lost device? [Sign out everywhere](#)'.

⑬ Click [X] to close your web browser.

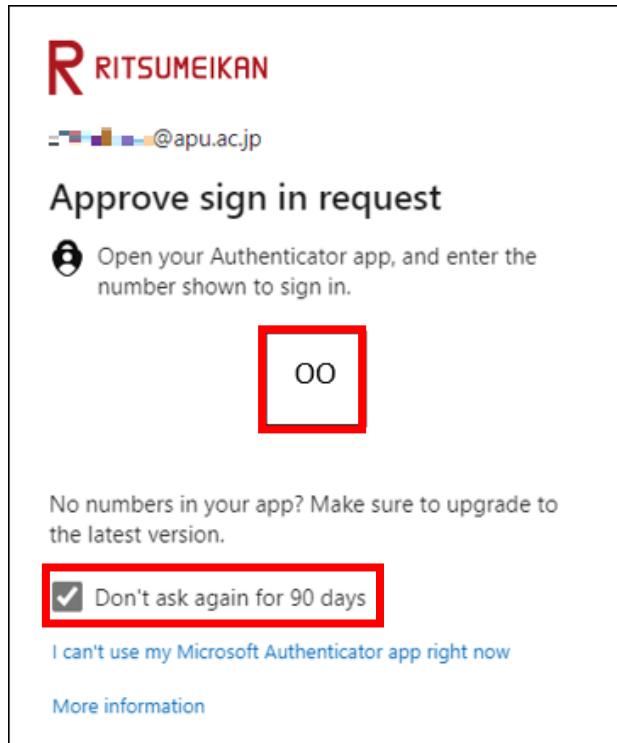
STEP 3: Signing in using MFA

After completing the tasks in STEP 2, MFA will be required by the following day.

If MFA is requested, please follow the steps below.

- ① Enter your ID and password on the university's authentication screen, and click [Sign in].
- ② A two-digit number will be displayed on the [Approve sign in request] screen.

Enter the number into the Microsoft Authenticator of the device you set up, and then tap [Yes].



① You can save Multi-factor Authentication information as follows.

- Web browser: 90 days if you check the box for “Don’t ask again for 90 days” when signing in.
- Desktop application: One-time authentication for a long period of time regardless of the above.

*Some desktop applications behave the same as web browsers