UNIVERSITY OF MIAMI
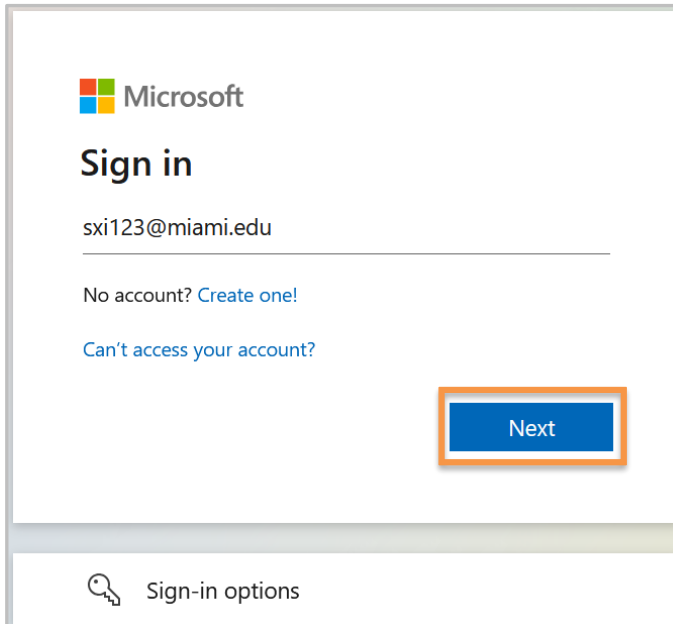**DEPARTMENT of INFORMATION TECHNOLOGY**

Microsoft Authenticator Enrollment Guide:
Existing Duo Users Transitioning to Microsoft Authenticator

Quick Links – Access to Enrollment Instructions to:
Enroll in Microsoft Authenticator – **Add a New Device**

Instructions to
Enroll in Microsoft Authenticator

1. To start the self-enrollment process, visit it.miami.edu/enroll-authenticator and enter your University of Miami Login ID*, then click "**Next**."

   Note: If you don't know your Login ID, visit CaneID Self-Service at caneid.miami.edu and click the "Login ID" banner to easily view your Login ID information.
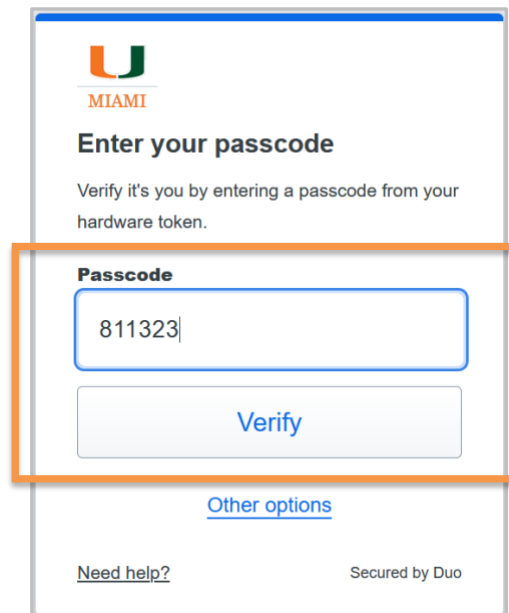
■■ Microsoft

Sign in

sxi123@miami.edu

No account? Create one!

Can't access your account?

Next

⌕ Sign-in options

UNIVERSITY OF MIAMI
DEPARTMENT
of INFORMATION
TECHNOLOGY

2. Once you are redirected to University of Miami Single Sign-On (UM SSO), enter your password and then click "**Sign in**."
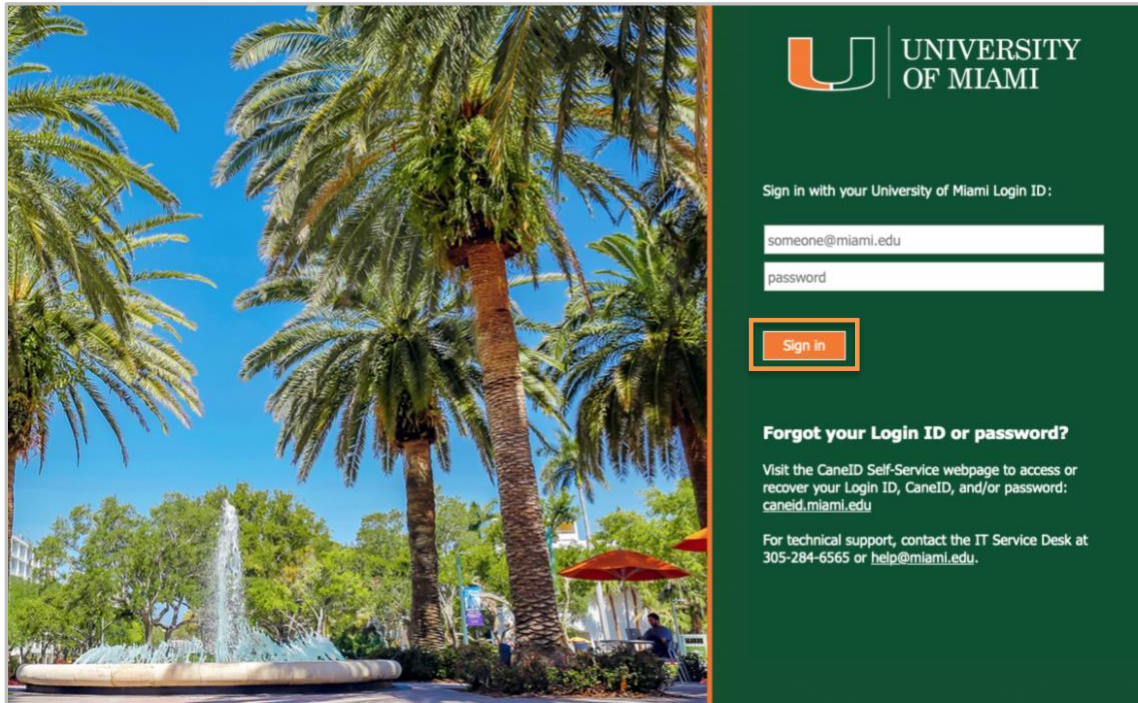
3. Follow the prompts to authenticate with Duo.
   Note: The passcode below is an example only.

UNIVERSITY OF MIAMI
DEPARTMENT
of INFORMATION
TECHNOLOGY

4. Select "**Add sign-in method**."
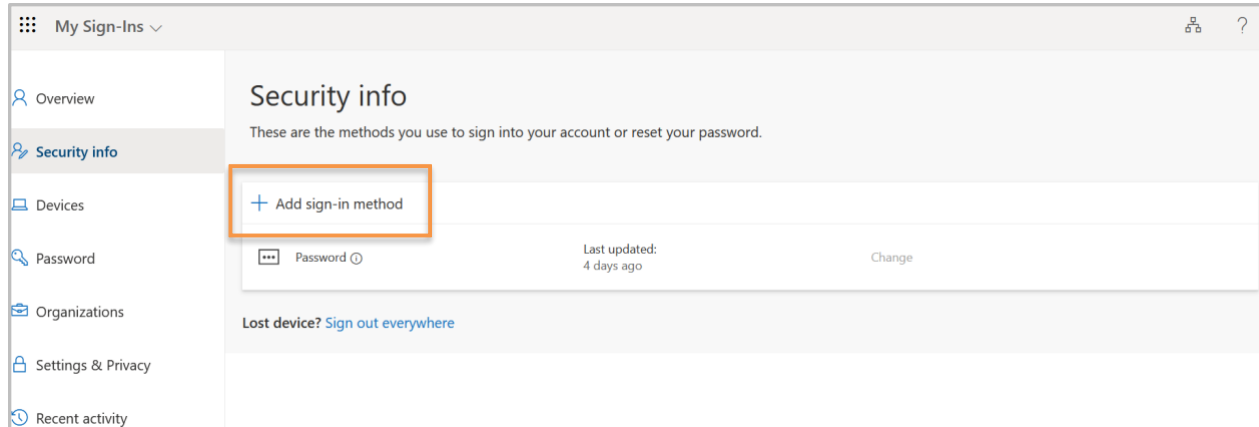
5. In the *Add a Method* pop-up window, **(A)** select "**Authenticator app**" from the drop-down menu and then **(B)** click "**Add**."
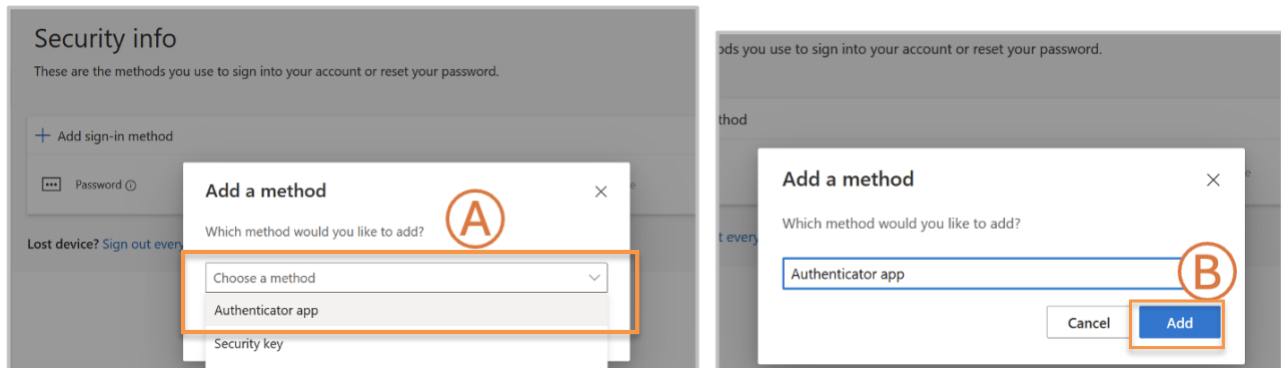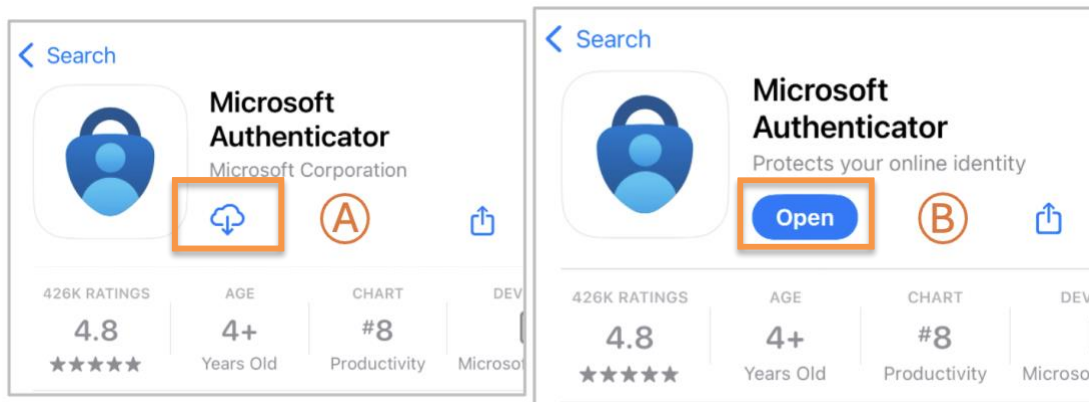

6. Search for "*Microsoft Authenticator*" in your mobile app store, **(A)** click the download button to install it, then **(B)** click "**Open**" to launch the app.
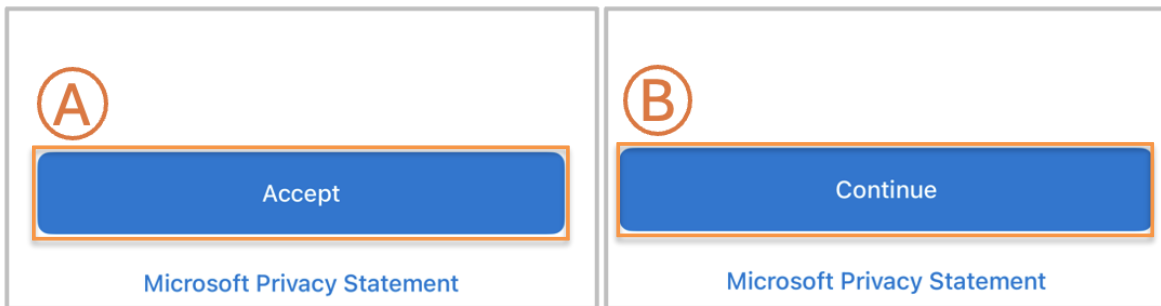
UNIVERSITY OF MIAMI
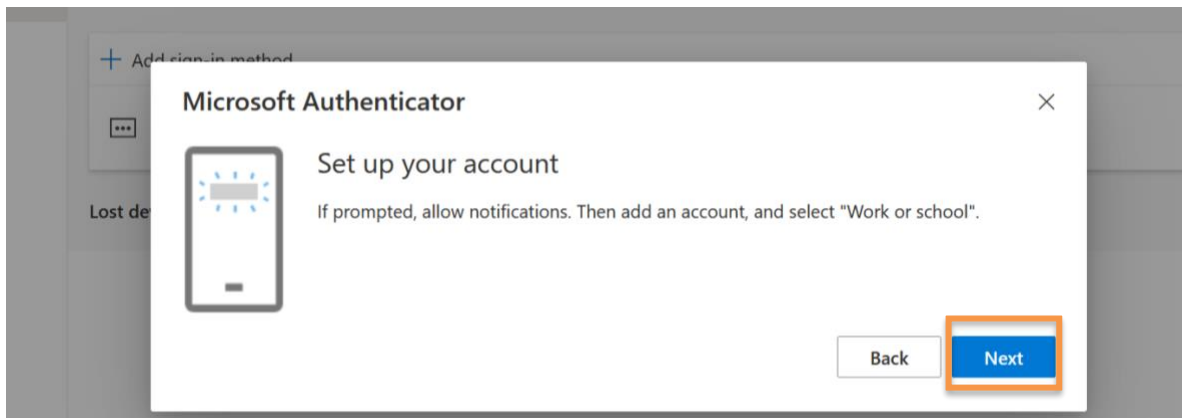**DEPARTMENT of INFORMATION TECHNOLOGY**

7. Once the *Microsoft Authenticator* app has been downloaded on your mobile device, click "**Next**" on your desktop computer.

8. *Microsoft Authenticator* app will prompt you to **(A)** select "**Accept**" to allow diagnostic data collection. When done, **(B)** click "**Continue**."
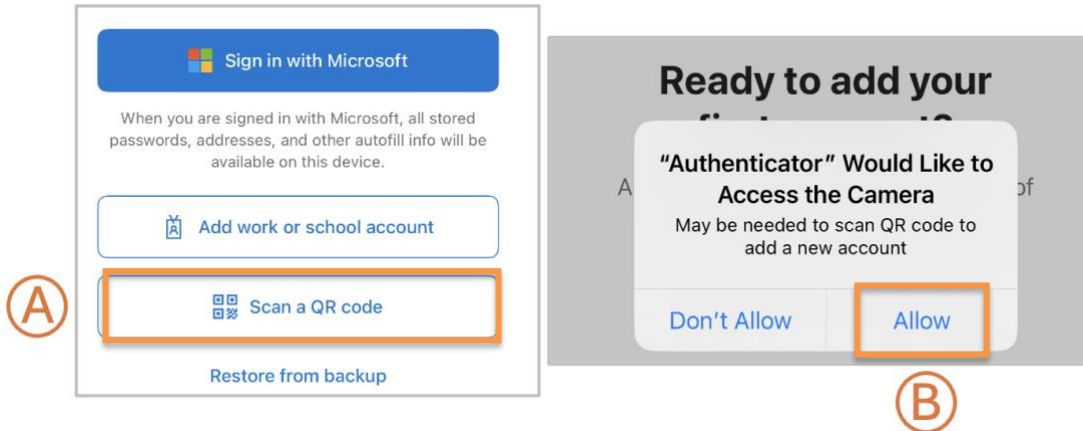

9. Follow the prompts on your mobile device to configure your Microsoft Authenticator app settings, then click "**Next**" on your desktop computer.

UNIVERSITY OF MIAMI
DEPARTMENT
of INFORMATION
TECHNOLOGY

10. From the Microsoft Authenticator app, select "**Scan a QR code**" and then select "**Allow**".

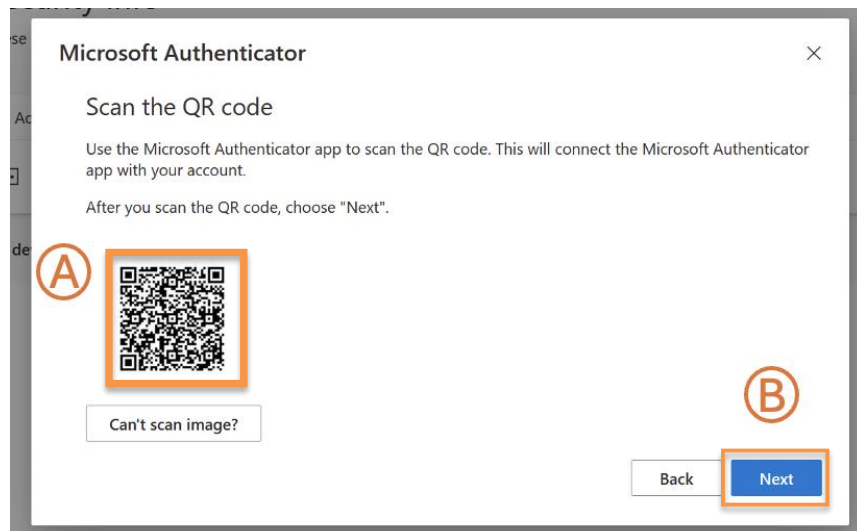**11.** Within the app, select "**Allow**" to ensure you can receive authentication prompts, then proceed with scanning the QR code.
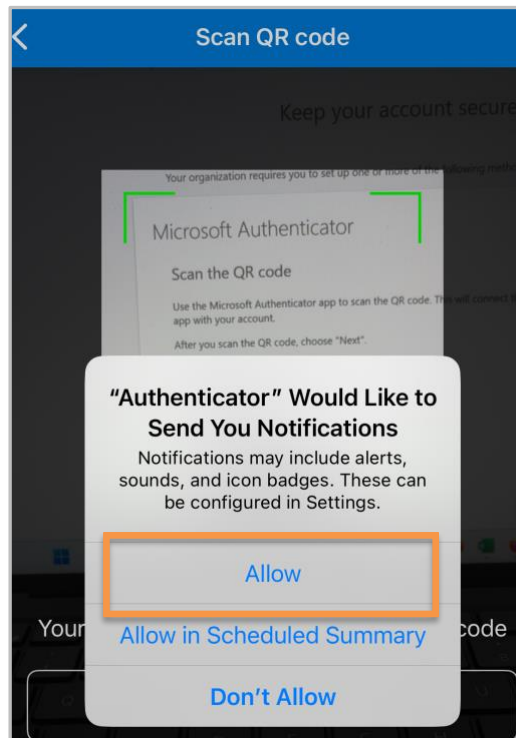
**UNIVERSITY OF MIAMI
DEPARTMENT
of INFORMATION
TECHNOLOGY**

12. From the *Microsoft Authenticator* app **(A) scan the desktop QR code with the app's built-in scanner** and once complete, **(B)** click "**Next**."
Note: The QR code below is an example only.

13. (A) Enter **the number shown on your desktop computer screen** into the **(B)** *Microsoft Authenticator app* on your mobile device and **(C)** select "**Yes**."
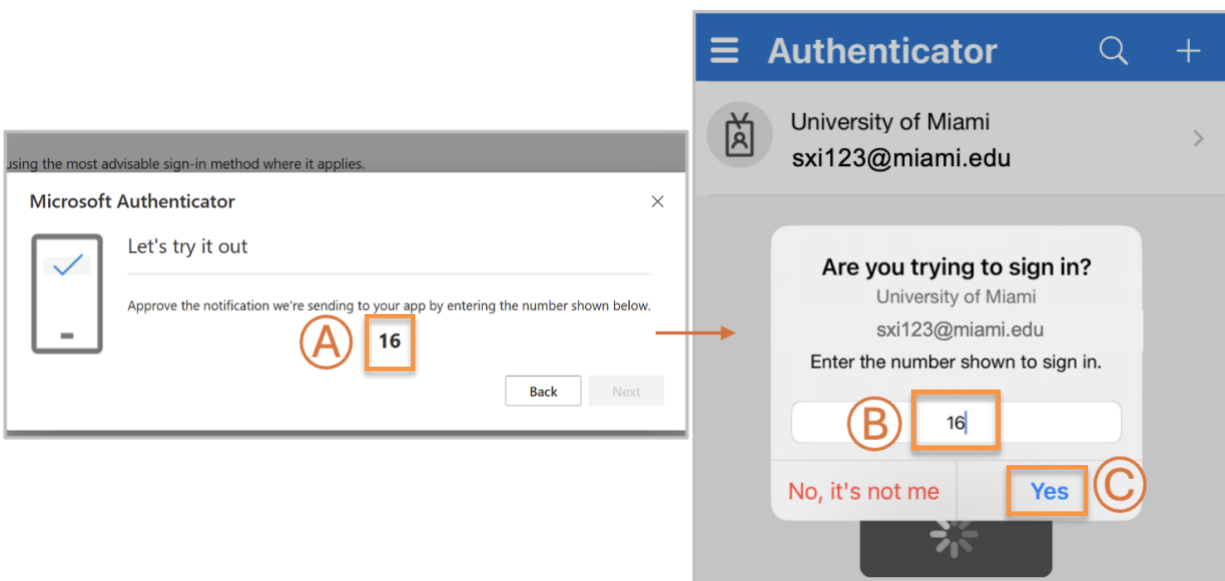
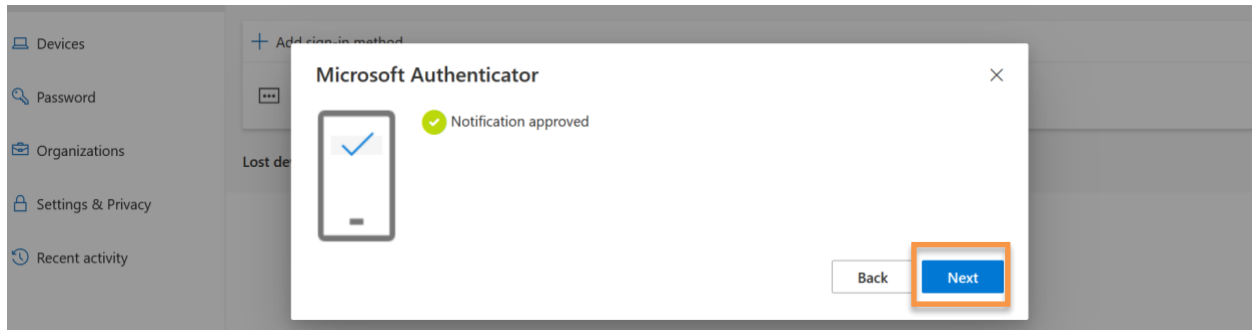**14.** After the notification is successfully approved, click "**Next**" on your desktop computer.

Note: It may take up to 48 hours for your Microsoft Authenticator device enrollment to be completed. In the meantime, you can continue to authenticate using Duo. Once the enrollment process is complete, you can log in to University of Miami systems and applications using Microsoft Authenticator.

Instructions to
Add a New Device

If you would like to add a hardware token as an additional authentication method, please visit one of the convenient locations listed below and an IT specialist will enroll the hardware token in your Microsoft Authenticator account:

Coral Gables campus: Student Technology Help Desk (STHD)
- Open Monday-Friday, 9 a.m.-5 p.m.
- Location: Richter Library, 3rd Floor, Room 325
- Email: sthd@miami.edu
- Call: 305-284-8887

Marine campus: RSMAES Computing Facility
- Open Monday-Friday, 9 a.m.-5 p.m.
- Email: rcf-support@earth.miami.edu
- Call: 305-421-4028

Medical/UHealth campus: 1501 Building
- Open Monday-Friday, 8 a.m.- 5 p.m.
- Location: 1501 NW 9 Ave, Suite 101G, Miami, FL 33136