UNIVERSITY OF MIAMI
DEPARTMENT
of INFORMATION
TECHNOLOGY

Multi-Factor Authentication (MFA):
Frequently Asked Questions

What is MFA?

- Multi-factor authentication (MFA) adds a step to the login process and requires you to prove your identity after entering a University of Miami username and password by responding to a prompt to enter a passcode using a mobile device, tablet, or hardware token. MFA is required for all University of Miami users, including students, faculty, and staff. **The University of Miami uses Microsoft Authenticator for MFA services**. You can enroll *up to two devices* for MFA services, e.g., a phone and a tablet.

Which app do I download from the Apple App Store or the Google Play Store?

- **Make sure you download the *official* Microsoft Authenticator app** on your mobile device from the Apple App Store and/or Google Play Store. The Microsoft Authenticator app is free to use.

After I enroll, how do I login?

- When you reach the University-branded login page, **enter your University of Miami Login ID* and password**. You will then be prompted to **authenticate with multi-factor authentication (MFA)**.
  - **Your Login ID provides unified access to the majority of University of Miami applications and systems, and is sometimes referred to as your User Principal Name (UPN). Your Login ID is usually formatted like your CaneID; however, the Login ID has @miami.edu or @umiami.edu appended to the end of the ID. (The @miami.edu or @umiami.edu at the end of the Login ID indicates that you are associated to the University of Miami organization.) If you don't know your Login ID, visit CaneID Self-Service at caneid.miami.edu and click the "Login ID" banner to view your information. You can use your CaneID to log in and access this information on the CaneID Self-Service page.*
  - Keep in mind: your CaneID is your unique identifier within University systems, and you will use your CaneID for a variety of reasons—including when connecting to wireless networks at the University of Miami or systems that do not use the University's branded login screen (palm trees/flying ibis). Keep in mind that some University applications/systems may require a different ID to log in, and will prompt you accordingly.

How do I manage my MFA account, e.g., add a new device, delete a device, etc.?

- For instructions on how to manage your University of Miami Microsoft Authenticator account—including adding a new device and deleting a device—review the following tip sheet: How to Manage Your MFA Account/Device(s)

Can I change my default authentication method, e.g., either get a notification on the mobile app or input a six digit code?

- Yes. To change which authentication method you are automatically prompted for, visit it.miami.edu/manage-mfa, log in, and then select "**Change**." In the pop-up, **select your preferred method** and then click "**Confirm**" when complete:
  - If you select "**App based authentication - notification**," you will receive a notification within your Microsoft Authenticator app to input a two-digit code visible on the sign-in screen into the mobile app.
  - If you select "**App based authentication or hardware token - code**," you will need to open the Microsoft Authenticator mobile app to find a six digit code and then enter the code into the sign-in screen.
- For step-by-step instructions on how to changing your default authentication method with your University of Miami Microsoft Authenticator account, review the following tip sheet: How to Manage Your MFA Account/Device(s)

UNIVERSITY OF MIAMI
DEPARTMENT of INFORMATION TECHNOLOGY

Why do I see a map when I open Microsoft Authenticator? Is my phone's location being tracked?

- The map you see in Microsoft Authenticator shows the *IP address location* of the device trying to sign in—not your phone's location. This feature helps you verify if a login attempt is legitimate.
- If the location on the map looks unfamiliar or suspicious, do <u>not</u> approve the request; instead, tap "No, it's not me" to deny the sign-in.

I noticed a sign-in pop-up within the Microsoft Edge browser when I'm logged in with my profile. What do I do to make the pop-up go away?

- This is a known issue within the Microsoft Edge browser on Mac (Apple) devices when signed in with your profile and Copilot is enabled; *Microsoft is currently working on a fix*. (For reference of what the pop-up looks like, see sample below.)
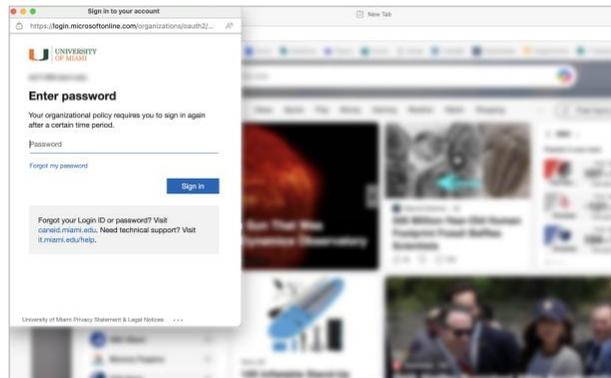
- In the meantime, to disable the sign-in pop-up, follow the steps below:
    - On the top-right of the Microsoft Edge browser, click the **ellipses (...)** and then select **Settings**.
    - Within the *Settings* panel, select **Sidebar** and then select **Copilot**.
    - Disable Copilot within the browser by **toggling off** the option to "show Copilot button on the toolbar" and "allow Copilot to use page content." Your selection is automatically saved.

Who do I contact if I run into issues?

- The IT Service Desk is available 24/7 to provide technical support. Contact the IT Service Desk at 305-284-6565 or help@miami.edu.