



TECHNOLOGY SERVICES:

Set up MFA (Multi-Factor Authentication) in Microsoft Authenticator

Microsoft Authenticator is the MFA (Multi-Factor Authentication) resource supported by FHSU. This document explains how to set up the different MFA methods in Microsoft Authenticator.

For assistance using these procedures, contact TigerTech by calling (785) 628-3478 or visiting www.fhsu.edu/tigertech.

TABLE OF CONTENTS:

- A. [Install the Microsoft Authenticator app on a mobile smart device.](#)
- B. [Set up your MFA \(Multi-Factor Authentication\) options in Microsoft Authenticator:](#)
 - [Method 1: Passkey \(passwordless sign-in\)](#)
 - [Method 2: Push notifications or one-time codes using Microsoft Authenticator App](#)
 - [Method 3: Text or call authentication using a phone number](#)

A. Install the Microsoft Authenticator app on a mobile smart device.

1. Open the **App Store** on your mobile smart device.
2. Search for **Microsoft Authenticator** in the app store.
3. **Download** the *Microsoft Authenticator* app.



B. Set up your MFA (Multi-Factor Authentication) options in Microsoft Authenticator:

Method 1: Passkey (passwordless sign-in)

NOTE: To use **Method 1**, your device's operating system must have **Android 14 or iOS 17 or later**. If your device is older and cannot be updated to these versions, you will need to use Method 2 or 3.

1. [Install and open](#) the Microsoft Authenticator app on your mobile smart device.
2. If asked if you would like to *receive notifications*, tap **Allow**.
3. If prompted, **decide** whether to *share additional data*. This does not affect the MFA process. After deciding, tap **Continue**.



TECHNOLOGY SERVICES:

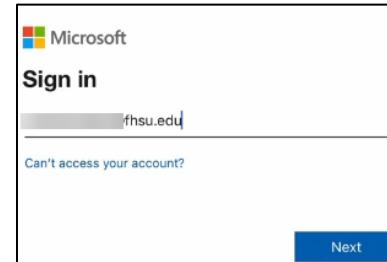
Set up MFA (Multi-Factor Authentication) in Microsoft Authenticator

4. If this is your first time using Microsoft Authenticator, tap the **Add work or school account** button. **If the button is not visible:**

Add work or school account

- a. Tap the “+” icon in the top right corner of the screen.
- b. Tap **Work or school account**.
- c. Tap **Sign in**.

5. In the *Microsoft Sign in* window, type your **university email address**, and then tap **Next**.



6. In the *FHSU Sign in* window, enter your **TigerNetID username** and **password**, and then tap **Sign in**.

7. On the next screen, click **Continue** to set up your Passkey.

8. You should receive a *permission request* depending on your device's capabilities. For example, if your device can perform a face scan, your device may ask you to *allow "Authenticator" to use your Face ID*.



- a. **If you would like to use this feature** for your Passkey, choose **Allow**.
 - i. **Microsoft Authenticator** will walk you through the process of **validating** the **Passkey** using this feature.
 - b. **If you do NOT want to use this feature** for your Passkey, choose **Don't Allow**.
 - i. **Microsoft Authenticator** will ask you to enter your device's unlock passcode, PIN, or combination to set up the Passkey.

9. **If successful**, the screen will display *Account added*.

10. Tap **Done**.

11. You will now see your **university email address** listed on the app's home screen.



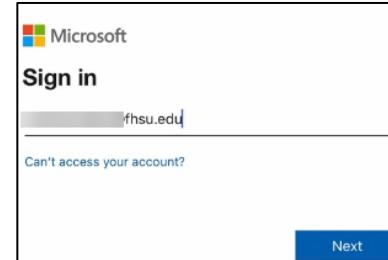


TECHNOLOGY SERVICES:

Set up MFA (Multi-Factor Authentication) in Microsoft Authenticator

Method 2: Push notifications or one-time codes using Microsoft Authenticator App

1. On a computer, open a browser and visit myaccount.microsoft.com.
2. In the *Microsoft Sign in* window, type your **university email address**, and then tap **Next**.
3. In the *FHSU Sign in* window, enter your **TigerNetID username** and **password**, and then tap **Sign in**.
4. In the *Security info* pane, click **UPDATE INFO**.
5. On the next screen, click **Add sign-in method**.
6. In the pop-up window, select **Microsoft Authenticator** from the list.
7. On your mobile device, install and open the Microsoft Authenticator app.



8. If prompted, **decide** whether to *share additional data*. This does not affect the MFA process. After deciding, tap **Continue**.
9. If this is your first time using Microsoft Authenticator, tap the **Scan QR code** button. **If the button is not visible:**
 - a. Tap the “+” icon  in the top right corner of the screen.
 - b. Tap **Work or school account**.
 - c. Tap **Scan QR code**.



10. If you receive a prompt saying “Authenticator” would like to access the Camera, click **Allow**.



11. Go back to your computer and click **Next** until a QR code is displayed.

12. Use your mobile device to **scan the QR code** on the computer screen.

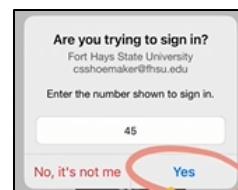
13. On your computer, click **Next**.

14. **Type the number** that appears on the computer screen into the **pop-up window** on your mobile device.

15. Once entered, tap **Yes** to confirm.

16. **If successful**, a confirmation message will appear on the computer screen. Click **Done**.

17. On the *Security info* page, **Microsoft Authenticator** will now be listed as a sign-in method.





TECHNOLOGY SERVICES:

Set up MFA (Multi-Factor Authentication) in Microsoft Authenticator

Method 3: Text or call authentication using a phone number

1. On a computer, **open a browser** and visit myaccount.microsoft.com.
2. In the *Microsoft Sign in* window, type your **university email address**, and then tap **Next**.
3. In the *FHSU Sign in* window, enter your **TigerNetID username** and **password**, and then tap **Sign in**.
4. In the *Security info* pane, click **UPDATE INFO**.
5. On the next screen, click **Add sign-in method**.
6. In the pop-up window, **select the phone method** you prefer:
 - **Phone** – Receive a **text or call** to sign in (best for mobile devices)
 - **Alternate phone** – Receive a call to sign in.
 - **Office phone** – Receive a call to sign in.
7. In the next window, fill out the requested fields:
 - a. **Country code**: Select from the dropdown. It will likely default to “United States (+1).”
 - b. **Phone number**: Enter the phone number to receive the verification.
 - c. If you selected **Phone** in the previous window, under *Choose how to verify*, choose either **Text a code** or **Call**.
8. Click **Next**.
9. Complete the setup by using your selected method:
 - a. If you selected **Text a code**:
 - i. Microsoft will text a verification code to the mobile device.
 - ii. **Enter the code** from the text message **into the pop-up window** on the computer.
 - iii. Click **Next**.
 - b. If you selected **Call**:
 - i. You will receive an **automated call from TigerTech** (785-628-3478).
 - ii. Answer the call.
 - iii. The automated call will say it is Microsoft and provide instructions.
 - iv. **Tap the pound “#” key** on your phone, then end the call.
10. **If successful**, a confirmation message will appear on the computer screen. Click **Done**.
11. On the *Security info* page, the **selected phone method** will now be listed as a sign-in method.

