



# Multi-Factor Authentication (MFA) Set Up Guide

Updated Summer 2023

Information Technology Services

[helpdesk@clarku.edu](mailto:helpdesk@clarku.edu)

# What is multi-factor authentication?

To learn more about MFA, please [click here to view a short video](#).

## What are my MFA options?

**ITS strongly recommends using Microsoft Authenticator**, an app available for download on mobile devices such as smartphones. Once set up, this method will send you a notification on your phone when it needs to verify account access. This method ensures you will be able to access your account anywhere with an internet connection, and it also provides a higher level of security.

If you do not have a smartphone, you can set up MFA through SMS authentication using your cell phone. This method sends a one-time code through SMS (text) messaging when it needs to verify account access, which you then enter into your computer. The code will be different each time and should not be shared with anyone, including members of ITS.

If you do not have a smartphone or a phone capable of receiving text messages, please contact [helpdesk@clarku.edu](mailto:helpdesk@clarku.edu).

## What do I need?

If you're using the Microsoft Authenticator app, you'll need:

- Your smartphone
- Internet access

If you're using SMS authentication, you'll need:

- Your cell phone
- A computer with internet access

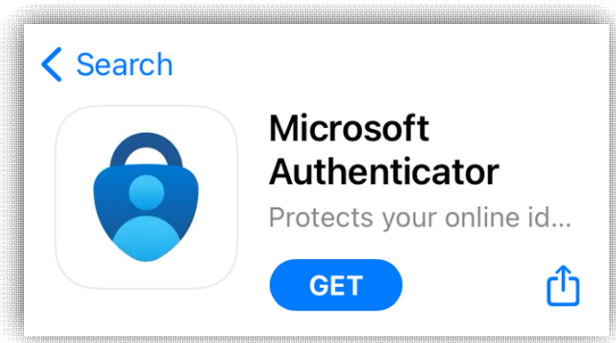
## Table of Contents

[Set up MFA with the Microsoft Authenticator App](#)

[Set up MFA with SMS Authentication](#)

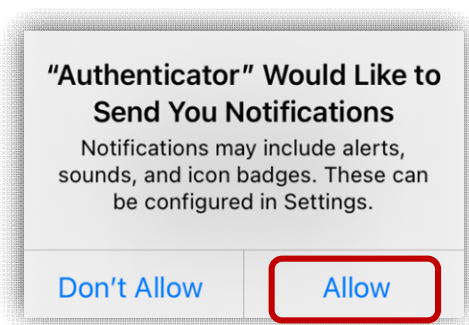
# Microsoft Authenticator App

1. Download the Microsoft Authenticator app to your smartphone using either the [Play Store](#) (for Android devices) or the [App Store](#) (for iOS devices).

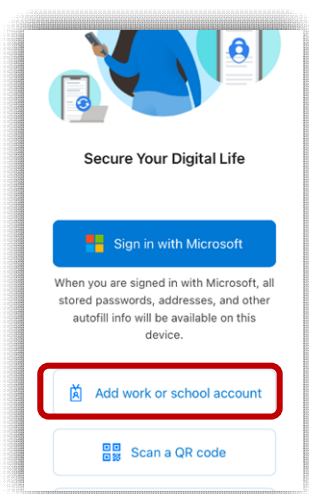


Check that the app you download was published by Microsoft corporation.

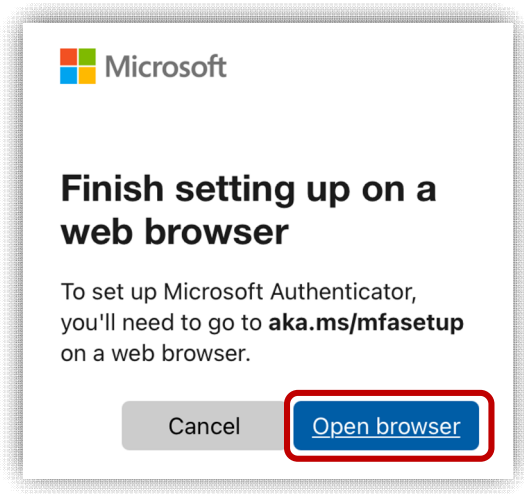
2. Once the Authenticator app is downloaded to your smartphone, tap the app to open it.
3. The app will ask to send you notifications: these notifications will help you authenticate your account moving forward. Tap **Allow**.



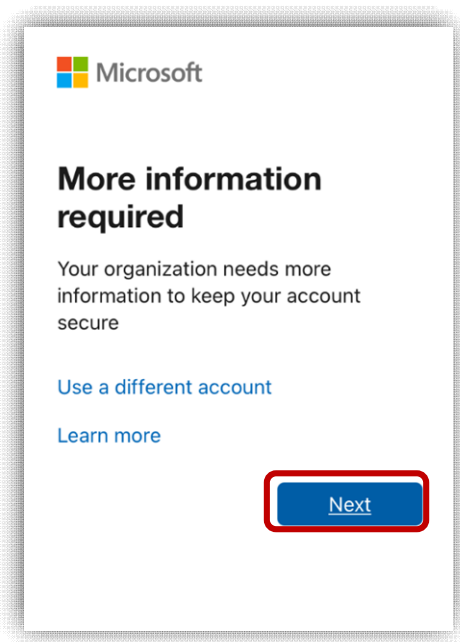
4. Tap **Accept**, then tap **Continue**.
5. Tap **Add work or school account**, then tap **Sign in**.



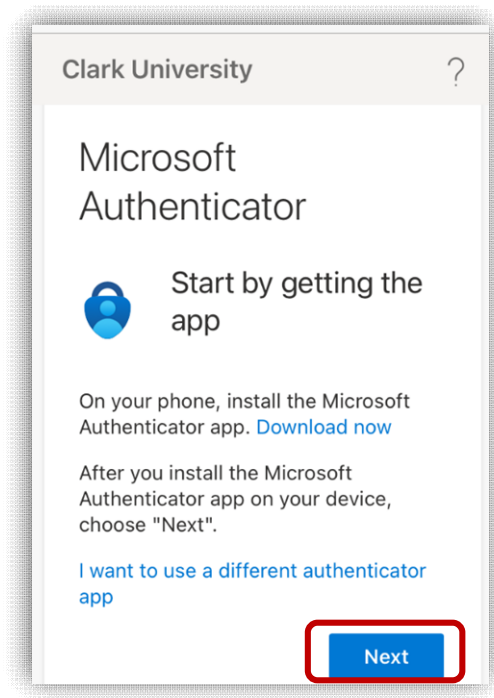
6. Log in using your Clark University email address and password.
7. When prompted to finish setting up on a web browser, tap ***Open browser***.



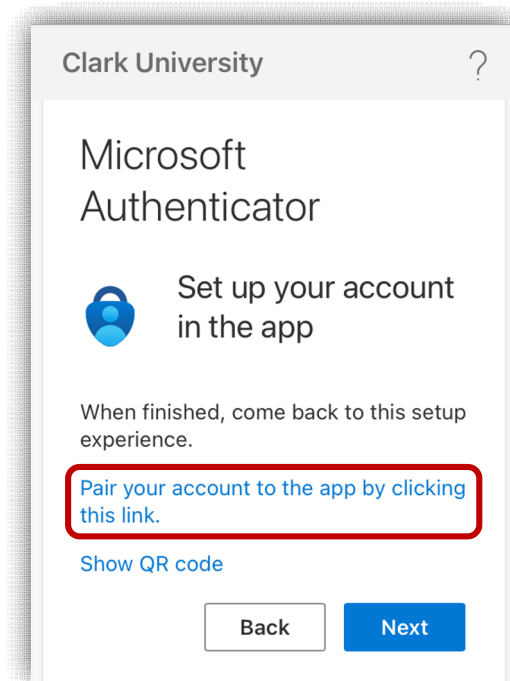
8. Microsoft will alert you that more information is required. Tap ***Next*** and enter your Clark account credentials.



9. Next, you'll see a screen instructing you to get the Microsoft Authenticator app. Since you have already downloaded it to your smartphone, tap *Next*.



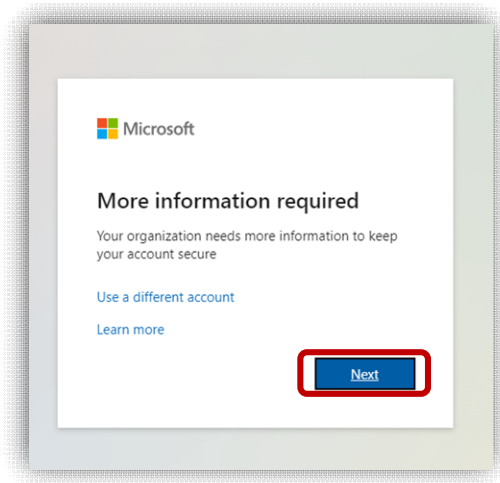
10. The following screen will prompt you to set up your account in the Microsoft Authenticator app. Tap *Pair your account to the app by clicking this link*, and then tap *Open*.



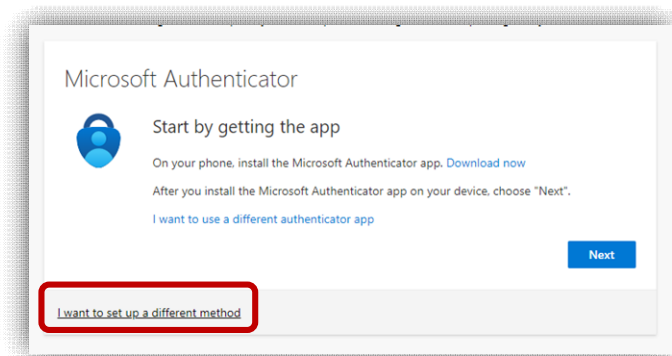
11. Microsoft Authenticator will likely enable App lock, meaning that you will need to enter your TouchID or phone passcode in order to access the app. You can change this in settings if you'd like. When prompted, tap **OK**.
12. You're all set! The next time Microsoft needs to authenticate your account access, you'll receive a notification on your phone. You can manage MFA options by visiting <https://mysignins.microsoft.com/>.
  - a. *Please note that you will not be prompted for MFA while on campus or when connected to the VPN.*

# SMS Authentication

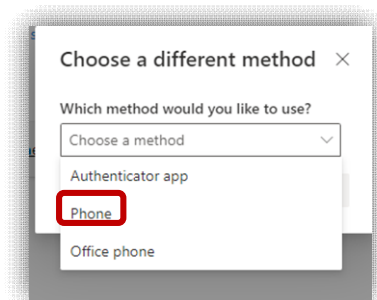
1. On your computer, navigate to <https://outlook.com/clarku.edu> using your internet browser. Log in with your Clark University username and password.
2. Microsoft will alert you that more information is required. Click **Next**.



3. Since Authenticator is recommended by both Microsoft and Clark's ITS department, you will see the app suggestion on your screen. Click ***I want to set up a different method*** at the bottom.



4. In the pop-up window, select **Phone**, then click **Confirm**.



4. Enter your cell phone number and select ***Text me a code***. Then click ***Next***.

Remember:  
Microsoft will text this number a new code each time it needs to verify your account access. Never share any of the codes you receive.

5. Once you input your cell phone number, Microsoft will text you a code. Enter the code when prompted and click ***Next***.

6. Once your phone is registered successfully, you'll see a green check mark. Click ***Next***, then click ***Done***.
7. You're all set! The next time Microsoft needs to authenticate your account access, you'll receive a code via text message on your phone. You can manage MFA options by visiting <https://mysignins.microsoft.com/>.
- Please note that you will not be prompted for MFA while on campus or when connected to the VPN.*