Microsoft Authenticator on iOS Devices

# Summary

This document outlines the steps for setting up the Microsoft Authenticator App on iOS Devices such as an iPhone or iPad for use with Multi-Factor Authentication (MFA) at Fullerton College. The same general process can be used to install and configure the Microsoft Authenticator Application on Android Devices.  
 **Last Updated:** November 13th, 2020

## Pre-Requisites

* You have a working Fullerton College FCNet and have confirmed that you can Sign-In at <https://o365.fullcoll.edu>
* You have MFA enabled already enabled and successfully working with either SMS Text Messages or automated Phone Calls
* You will need an iPhone or iOS device with iOS version 14.x or newer installed
  + The application and the instructions to setup the device may work on older iOS versions, but only is only officially support by Fullerton College on newer devices.

## Notes

Some of the screens pictured below may be slightly different depending on your device, screen size, OS version, or browsers that you use.

|  |  |
| --- | --- |
| 1. Navigate to <https://o365.fullcoll.edu> and Sign-In with your FCNet credentials |  |
| 1. Click on your account icon located at the top-right, and select “View Account |  |
| 1. Click on Security Info -> Update Info |  |
| 1. You will be prompted for your existing Multi-Factor Authentication method. Complete the prompts as usual |  |
| 1. On the Security info screen, click Add method |  |
| 1. Select Authenticator app from the drop down  Click Add |  |
| 1. Click Next |  |
| 1. Stop on this screen.  **DO NOT CLICK NEXT** |  |
| 1. On your mobile device, open the Apple Store, search for, and download the Microsoft Authenticator App |  |
| 1. Graphical user interface, text, application     Description automatically generatedWhen the Microsoft Authenticator App opens, click on Scan QR code | Graphical user interface, text, application  Description automatically generated |
| 1. A picture containing diagram     Description automatically generatedIf prompted, you will need to give the application permission to access your Camera. | A picture containing diagram  Description automatically generated |
| 1. Graphical user interface, text, application, chat or text message     Description automatically generatedYou may receive a privacy disclaimer, click OK  If you would like to turn off data collection, you may follow the steps shown after completing the setup of the App. | Graphical user interface, text, application, chat or text message  Description automatically generated |
| 1. Graphical user interface, text, application     Description automatically generatedThe Authenticator Notifications are the easiest way to use the Microsoft Authenticator application, we highly recommend you Allow them.  Click Allow | Graphical user interface, text, application  Description automatically generated |
| 1. Your mobile device should now be ready to scan the QR code from the website. Return to your computer and click next. |  |
| 1. With your mobile device center the QR code within the view finder. |  |
| 1. The app should automatically scan it, and then display the account. |  |
| 1. Return to your computer and click Next. The system should then send a request to the app to test it. |  |
| 1. Your device should now display a pop-up notification with options to Allow or Deny. Tap Allow.  On your computer it should show the Notification approved.  Click Next |  |
| 1. You now need to to switch from Phone to the Authenticator App as your default MFA method  Click Change |  |
| 1. Select Microsoft Authenticator – notification from the drop down  Click Confirm. |  |

## Optional Configuration

Graphical user interface, text, application, chat or text message

Description automatically generatedDepending on your mobile device, the application may enable “App lock” by default. App lock secures the application by requiring your fingerprint, face unlock, or PIN before being able to use the application. If you frequently leave you mobile device unattended, or allow other people or children to use your mobile device, we recommend you leave this feature enabled. If you always keep your device on your person, and do not allow others to use your device you may disable App lock by following these steps:

|  |  |
| --- | --- |
| 1. Open the application on your device and proceed to the configuration screen by clicking on the 3 dots or bars at the top of the application. Depending on your mobile device these may appear on the top left or top right of the application window. |  |
| 1. Graphical user interface, text, application     Description automatically generatedScroll down and locate the App Lock option, then toggle it off. | Graphical user interface, text, application  Description automatically generated |

# Additional Information

Microsoft provides additional documentation on this process at:

<https://docs.microsoft.com/en-us/azure/active-directory/user-help/security-info-setup-auth-app>

# Support

If you encountered any difficulties while following these instruction, if you have any questions, or would like additional information about using your account please visit the FCNet website at <https://fcnet.fullcoll.edu> or contact the Academic Computing Technologies (ACT) Help Desk via email at [helpdesk@fullcoll.edu](mailto:helpdesk@fullcoll.edu) or by calling 714-992-7111