

Multi-Factor Authentication (MFA) at MCC

Strong passwords are essential, but they are not enough. Phishing attacks and data breaches put your account at risk. Multi-factor authentication (MFA) provides extra security for your MCC Network Account and will be required when accessing some college resources. You may also see the terms two-step authentication (2FA), two-step verification, or login verification.

With MFA, anyone trying to access your account must provide two forms of identification:

- Something you know: such as your password.
- Something you have: such as a phone or a mobile app.

Microsoft Authenticator is a free multi-factor authentication app that MCC encourages you to use for MFA since it will give you ‘push’ notifications that you simply accept to confirm and proceed.

How to Start

1. Download and install Microsoft Authenticator on one mobile device by scanning a QR code below.

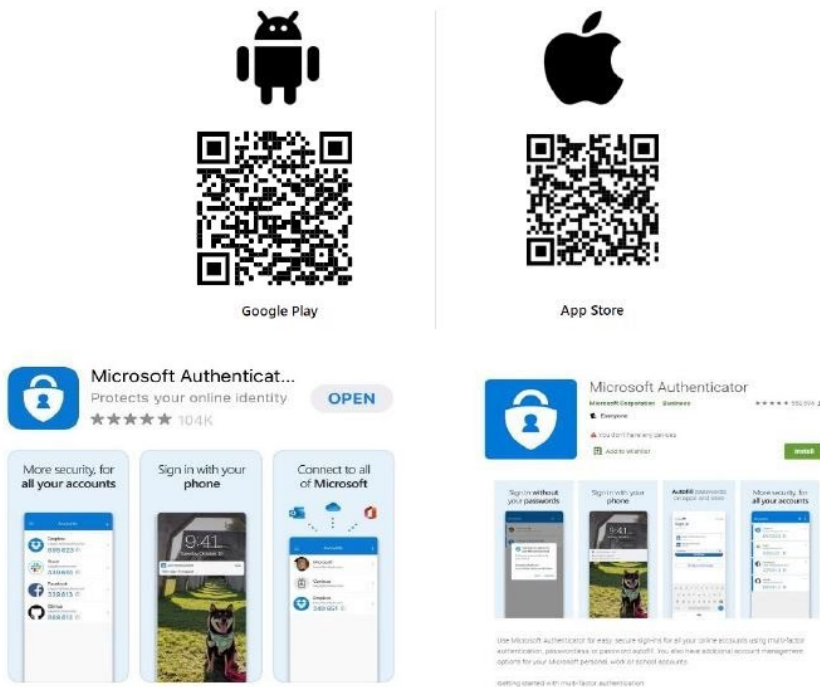


Figure 1 - QR codes for app stores

2. Setup/enroll in MFA for Microsoft 365 following the steps below.

Multi-Factor Authentication Initial Enrollment – Microsoft 365

1. Open browser to <https://myaccount.microsoft.com>. Login using your full MCC network user account (include @student.monroecc.edu for students; @monroecc.edu for faculty/staff).

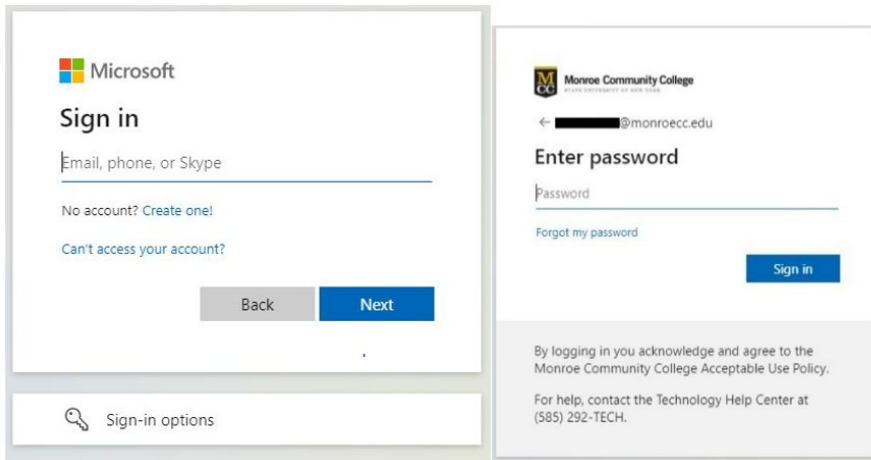


Figure 2 - MS Office login screenshots

2. After signing in, click Security Info from left-hand navigation.

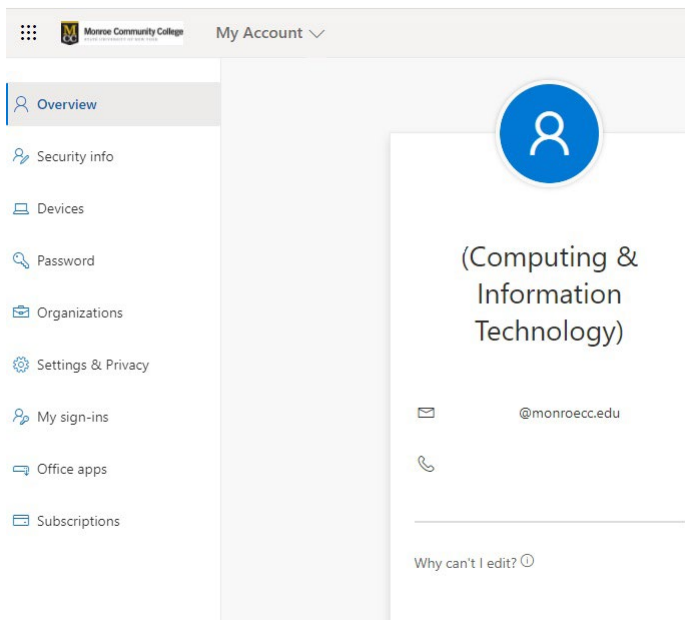


Figure 3 - MS account navigation screenshot

3. Click on + Add Method, select Authenticator app from the drop-down, then click on the Add button (**be sure that you have downloaded the authentication app on your mobile device first**). MCC recommends the Microsoft Authenticator app for the best experience. Microsoft Authenticator has set a time limit so it may time out and you will have to start over again.

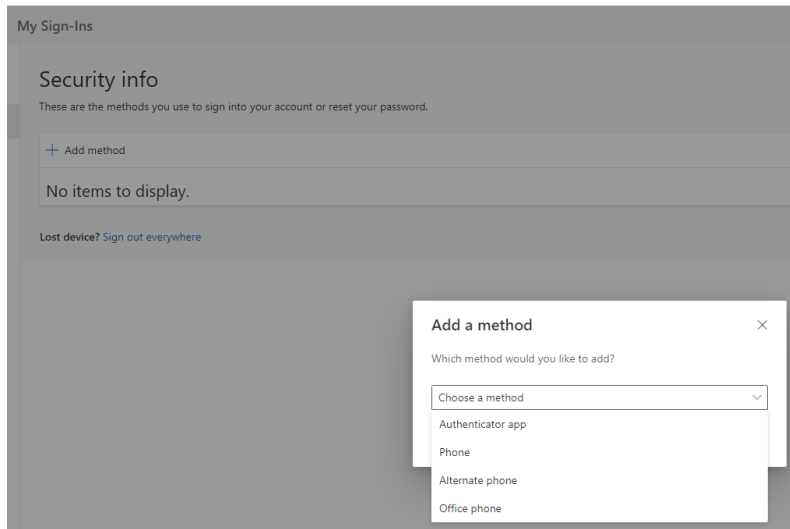


Figure 4 - Add method screenshot

4. Click on Next button in the popup after you have the Microsoft Authenticator app on your mobile device. The next step will be on your mobile device.
5. **On Your Mobile Device:** After obtaining the Microsoft Authenticator app on their mobile device, users should launch the app, select 'Add work or school account' and select "Scan QR code". Be sure to allow Authenticator app access to your camera, then scan the presented QR code on your PC screen. Click Allow to allow push notifications.

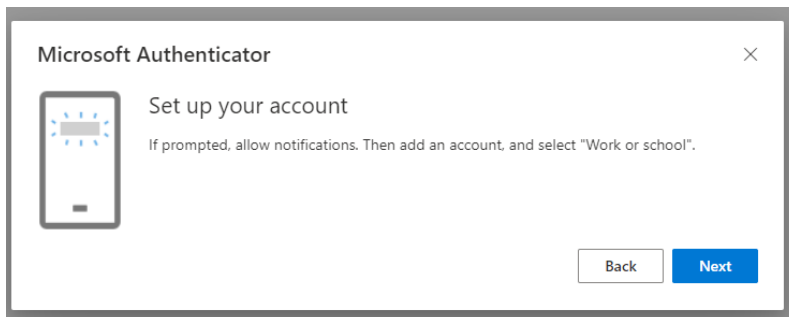


Figure 5 - Microsoft Authenticator app info screenshot

6. When complete within the app, click Next on the webpage to continue.

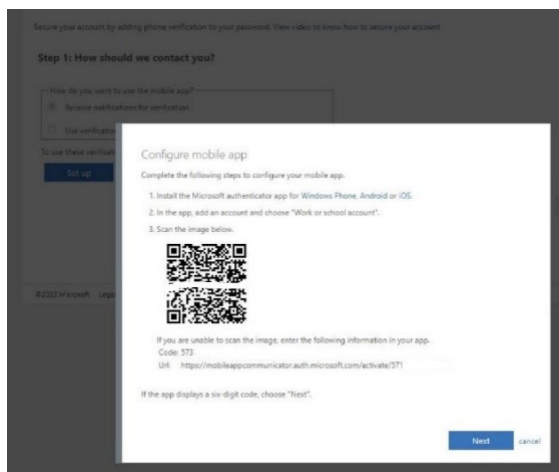


Figure 6 - Mobile app configuration screenshot with enrollment QR code

7. Once the enrollment process detects that the mobile app has been configured, click Next. A multi-factor authentication push request will be sent to your mobile device to verify that everything is working as expected.

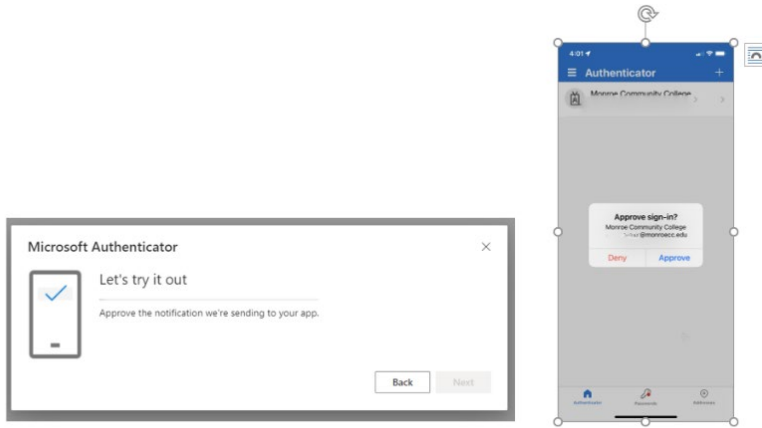


Figure 7 - MFA prompt screenshot and app approval screenshot

8. Once you click to approve the notification on your mobile device, you will see a confirmation on the screen. Click Next to continue.

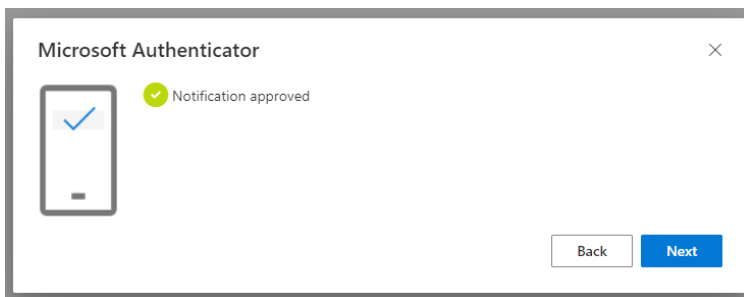


Figure 8 - MFA enrollment completion screenshot

9. Setup a backup with your mobile phone number in case your Microsoft Authenticator app is removed or you lose or replace your mobile device. You will repeat Step #3 but select Phone as the method. Enter your mobile phone number, then click on Next.

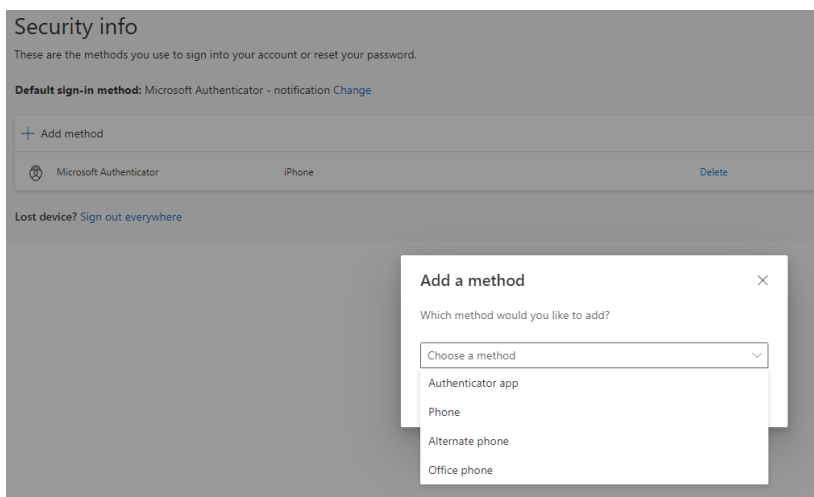
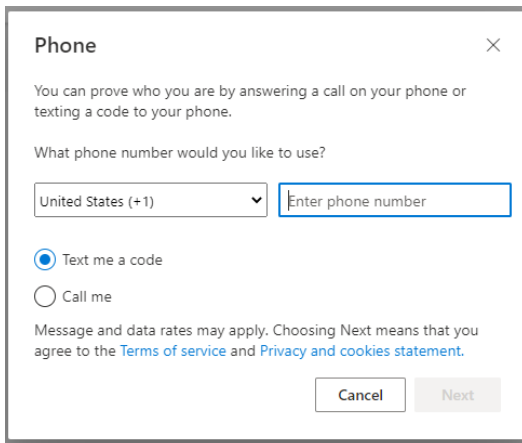


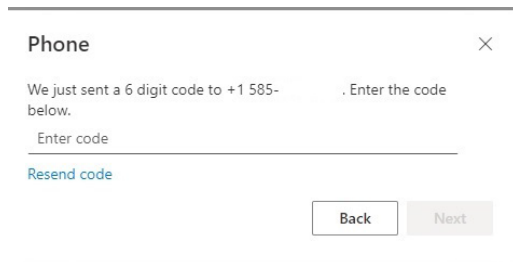
Figure 9 - Add method screenshot

10. Select with text me a code (SMS message) or Call me (phone). [*Note: Message and data rates will apply according to your mobile device plan.*] This establishes a communication to your mobile phone number (which rarely changes as devices are replaced) as a back-up Multi-Factor Authentication option.



The screenshot shows a dialog box titled "Phone" with a close button (X) in the top right corner. The text inside reads: "You can prove who you are by answering a call on your phone or texting a code to your phone." Below this, it asks "What phone number would you like to use?". There is a dropdown menu currently set to "United States (+1)" and a text input field labeled "Enter phone number". Underneath, there are two radio button options: "Text me a code" (which is selected) and "Call me". A small note states: "Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#)." At the bottom, there are "Cancel" and "Next" buttons.

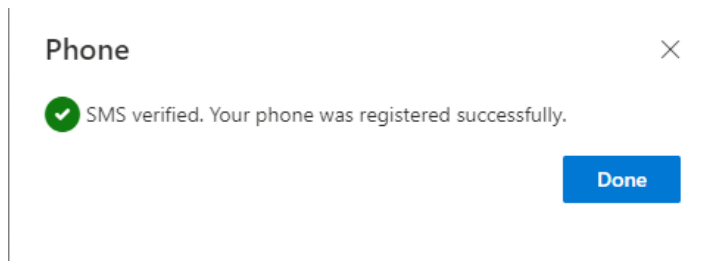
Figure 10 - Phone options screenshot



The screenshot shows a dialog box titled "Phone" with a close button (X) in the top right corner. The text inside reads: "We just sent a 6 digit code to +1 585- . Enter the code below." Below this, there is a text input field labeled "Enter code" and a blue link labeled "Resend code". At the bottom, there are "Back" and "Next" buttons.

Figure 11 - Mobile phone text authentication test

11. Enter the code then click next.



The screenshot shows a dialog box titled "Phone" with a close button (X) in the top right corner. It features a green checkmark icon followed by the text: "SMS verified. Your phone was registered successfully." A blue button labeled "Done" is positioned at the bottom right of the dialog.

Figure 12 - Backup mobile phone verification screenshot

12. Next time you sign-in to office.com, you will be prompted to open your Microsoft Authenticator app on your phone to approve the sign in request.

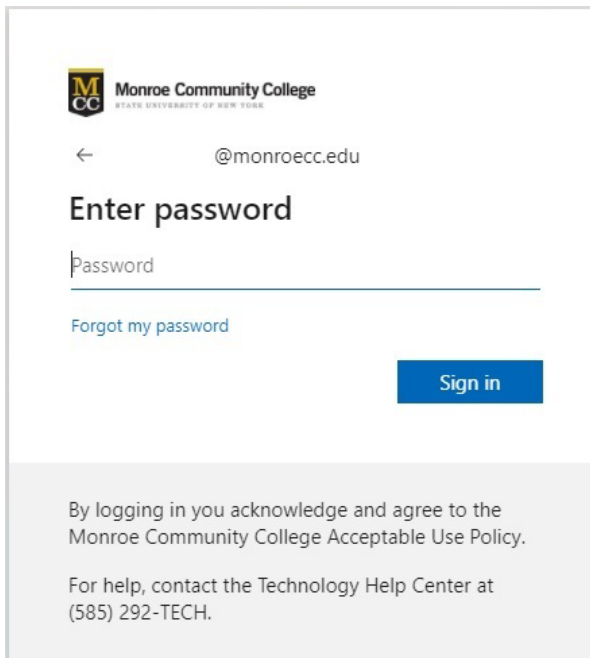


Figure 13 - MFA approval request screenshot

MCC employees should repeat Step #9 to add their *dedicated college-provided office phone* number by selecting Office Phone on the pop-up as a backup authentication method.